ISSN No:-2456-2165

An Outline of the Problems and Potential Solutions for Cloud Computing Security

Md. Afroz[1]
Department of Computer Science & IT Research Branch,
YBN University, Ranchi, Jharkhand, India

Birendra Goswami[2]
Professor and Dean Department of Computer Science & IT,
YBN University, Ranchi, Jharkhand, India

Abstract:- The security issues and solutions related to cloud computing are a strongly debated academic topic at the moment. Even though there have been many studies on cloud security, there is still some uncertainty about how to link issues with solutions. It is challenging to both generalize the idea and investigate its particular needs since there is no established framework for cloud security. Some polls focus on access control systems, while others discuss virtualization issues and solutions. A survey's suggested countermeasures must also specifically state the issue they are meant to solve. All of these factors have been taken into account while writing this survey paper, which includes a discussion of many open questions in the subject and covers all pertinent themes with appropriate links between them.

Keywords:- *Cloud Computing,Virtualization,Information Security, Data Security, , Security Challenges, Trust*

I. INTRODUCTION

Cloud computing is a highly scalable and cost-effective infrastructure for running High Performance Computing, enterprise and Web applications. Businesses are increasingly substituting cloud-based for internal resources to capture benefits like faster scale-up/scale-down of capacity, pay-as-you-go pricing, and access to cloud-based applications and services without buying and managing on-premises infrastructure. A remarkable positive change can be noticed in IT capital costs, labor cost and enhancement of productivity by using cloud-based computing [1]

A service level agreement must be established between the cloud provider and the consumer (or broker) before the cloud provider may offer a service to that customer (SLA). The SLA is an agreement that outlines the quality of service (QoS) between a service provider and service user. It often also contains the cost of the service, with the cost of the service adjusting the degree of QoS [2].

This cloud-customer relationship, which reflects the concept of a distributed system made up of a number of virtual machines that may be dynamically provided to fit a customer's changing resource demands, is underwritten by the SLA. Service Level Agreement (SLA) Simple on-demand network access to a pool of reconfigurable computing resources, such as network, storage, hardware, and applications, is made possible by the concept of cloud computing that can be instantly assigned, scaled, and released with minimum administration effort or service provider participation. [3].

Using the cloud immediately reduces overall expenses and enhances system performance since the user no longer needs to worry about installing and maintaining her system physically. When cloud-based services are used, a layer of abstraction is built between the user whose data or services are being handled in the cloud and the actual servers or storage. The cloud user, who may also be the service or data owner, is now forced to depend only on the cloud service provider (CSP) for the security and privacy of her data. Mutual trust may be achieved to some degree by negotiating the SLA, but several security vulnerabilities unique to the cloud eventually occur and must be handled by either the CSP or the user.

Data is the top concern for IT security, regardless of the infrastructure being utilized. This also holds true for cloud computing, whose dispersed architecture and multi-tenant design highlight new security concerns. The data life cycle encompasses the creation, archival, use, diffusion, and disposal of data. For each of these data life cycle stages, each CSP should provide the necessary security procedures [4].

If the online application (shared application) is constructed insecurely, a client might, for example, employ a SQL injection [5] to get unauthorized access to another customer's data and delete or edit it. To avoid this, the appropriate security measures must be implemented. Data deletion is an issue in the cloud once again, and as a result, the CSP must take extra care to ensure that data is permanently and totally wiped at the request of the customer. The customers should also be able to see and verify the data backups utilized to avoid data losses (scope, saving intervals, saving timings, storage length, etc.). All of these issues, in addition to a number of others, must be taken care of while using a cloud service.

Virtualization, which provides the requisite levels of flexibility, security, isolation, and manageability for delivering IT services on demand, is another essential component of cloud computing. IaaS is based on the concept of hardware virtualization, while PaaS solutions (covered in the next section) gain from programming level virtualization.

Server consolidation, which enables several applications or services to utilise a single physical server's resources concurrently without interfering with one another or even exposing this information to the client apps, is a concept that

ISSN No:-2456-2165

comes with virtualization. Given the aforementioned, it is very clear that Virtual Machines construct the whole back-end for Cloud-based services. It also increases certain hazards for the Cloud, however. It allows for a novel, unexpected kind of phishing. Malicious programs' ability to completely transparently imitate a host might lead to the theft of private information from the visitor. Additionally, Live Migration [6] and Virtual Machine Image [6] concepts concurrently meet customer demands while creating certain security flaws that the CSP must fix.

As a consequence, while considering cloud security, it should include more than simply data security and should also consider the security of the associated virtual machines (VMs).

It is challenging to distinguish between and categorize the many aspects of cloud security due to the cloud's comprehensive design and how it varies from a conventional on-premises system. Studying viable solutions and putting Cloud security into the proper categories are this paper's main goals.

II. CLOUD MODELS AND THEIR SPECIFICATIONS

➢ *Model of cloud services*

The NIST categorization of Cloud includes three service types [2] that provide services at different levels of a business model.

- Software as a Service (SaaS): This phrase describes a cloud service that enables users to connect online to software applications that are hosted on a cloud infrastructure. SaaS automates all the updates and doesn't need any setup or ongoing infrastructure maintenance expenditures. SaaS provides the least level of client security control since the user cannot access the execution platform and supporting infrastructure.

- Platform as a Service (PaaS) is a cloud-based computing platform that is integrated and abstracted and makes it easier to create, run, and manage applications.

IaaS, or infrastructure as a service, is the virtual supply of hardware, networking, and storage services for use with computer resources. The operating system, deployed services, and selected network segments are all at the client's control under this paradigm. The infrastructure is solely under the control of the CSP. IaaS gives customers greater security control over their data than older models did as a consequence.

B. Cloud Deployment Model

Based on the user's appropriateness and specific purpose, NIST again separates the cloud into four deployment options.

- Public Cloud: The cloud is kept on the end of the service provider and made accessible to regular individuals or large corporations. The public cloud guarantees scalability and reliability, but it also introduces a variety of issues that end up costing customers money. Customers are still in the dark about the CSP's storage strategy, where their data is kept, and whose data is kept nearby (i.e. certain issues of multi-tenancy). Enterprises must make certain security compromises in order to go to the public cloud.

- Private Cloud: Only one organization may use cloud services, and the cloud is either owned by the organization or a third party, either on-site or off-site. Private clouds reduce the security risks associated with public clouds, but they also come with additional costs for provisioning, storage management, and capacity monitoring.

- Community Cloud: The Cloud is offered just for a community of organizations with a common interest, and it may be controlled by the organizations or by a third party, situated on or off premises (e.g., mission, security requirements, policy, or compliance issues). This paradigm has a number of unsolved challenges, including issues with data being dispersed across many organizations and domains[7], contractual repercussions, and security ramifications.

- Hybrid Cloud: This type of cloud infrastructure consists of two or more distinct cloud infrastructures (private, community, or public), each of which is still a distinct legal entity, but which are linked by standardized or proprietary technology that enables the portability of data and applications (such as cloud bursting for load balancing between clouds) [6]. While simultaneously taking care of the security and control of private clouds, hybrid clouds provide the benefits of cost and scalability comparable to those of public clouds.

Data privacy and integrity issues emerge when data is transferred from the public to the private environment or vice versa since the privacy regulations in the public cloud environment are quite different from those in the private cloud[6].

In the section that follows, we go through the many security issues that arise often in cloud environments.

III. CLOUD SECURITY PROBLEMS AND REQUIREMENTS

The degree to which a user trusts the Cloud Service Provider (CSP) and the services they provide is one of the key determinants of whether they choose to utilize a cloud system or a traditional one. Trust is determined by assessing whether a provider has taken all necessary precautions, including those relating to data security, virtual machine security, and other legal and regulatory requirements. For this assessment of the security of the Cloud system, confidentiality, integrity, and availability are the three factors that have been taken into consideration (CIA). The primary goal of this part is to generalize the security needs of an existing Cloud system within the CIA domain, which is a widely accepted norm for defining the security issues with a conventional information system.

ISSN No:-2456-2165

A. Security of information

Confidentiality refers to the safeguarding of a specific company asset against disclosure to unauthorized users. These users in a cloud system can be clients who want to get unauthorized access to information that the CSP has kept in the same database as their own information. Additionally, the CSP could employ some dishonest or inquisitive workers who might look over or even tamper with the client's private and crucial data. The virtual machine network, virtual machine image, and other items must adhere to confidentiality rules in addition to client information.

This article has addressed the following categories under the different cloud system confidentiality criteria:

(1) Data Integrity

Unencrypted data is regularly processed and kept at the CSP end. As a consequence, CSP (SaaS) is in charge of safeguarding customer data during the whole course of its operation. Some issues with the confidentiality of data particular to clouds include:

Several cloud storage businesses enable shared access to online folders that contain user data. This can result in a potential loss of data confidentiality. Even if a file is shared in a group using a cloud storage service, the owner of the file must get frequent updates on any group modifications. The CSP must essentially explicitly manage the separation of client data from other data (competitor, unauthorised user).

The actual physical location of the user's data is another factor that affects its confidentiality. Since the data might be transported by CSP from one data center to another, the regulations that apply to it (if it crosses international boundaries) are constantly changed [8]. The exact rules that must be followed when a user analyzes data in the UK, stores it on servers in the US, and transfers it through France are difficult to nail down. Naturally, this compromises the confidentiality of the user's data [8].

Customers who requested service deactivation or whose membership time may have expired may have issues if the CSP improperly or insufficiently erases their data. The confidentiality of these users may be in danger due to the remnants of the erased data.

On rare occasions, CSP enlists outside help to provide data backup services. Such questionable outside service providers run the risk of using the client's private information improperly, which eventually jeopardizes the privacy of her information.

Cloud customers usually ask for more monitoring or log data for their own convenience and security. Log data contains the service provider's proprietary infrastructure information, which the cloud should once again not compromise.

As a consequence, the CSP and the users must have several talks about the details of log data that should be shared with clients without endangering the anonymity of the CSP.

Cloud service providers who forbid data owners from encrypting their own data or information before putting it on the cloud pose a severe danger to the security of user data. Sensitive data, such as medical or health information, government or defense data, should not be kept in the cloud if encryption options are not available.

In certain cases, it is assumed that cloud service providers are skeptics who are also trustworthy. They are more interested in learning about user access rights and the information included in user data files. In order to avoid such situations, the owners should set up suitable access control procedures.

(2) Security of Virtualization

IaaS runs user applications on virtual machines that CSP hosts. The deployed service that is contained in each VM may be seen or modified by anybody with privileged access to the host in a cloud system. As a result, users are unable to protect VM secrecy on their own. As a consequence, when considering security problems related to the Cloud, the entire virtualization layer exposes several security weaknesses that cause serious concerns. Here are a few of those topics:

Someone acting as the system administrator of the CSP is able to remotely access any existing PC with root access.

The system administrator may then change this VM to another one under her control that is outside the IaaS security perimeter [6]. Such internal assaults can invariably harm the application or the privacy of consumer data.

VM migration, particularly live migration, is the rapid function of cloud computing systems for load balancing, elastic scalability, fault tolerance, and hardware maintenance [6]. During and after the live migration, the CSP must take the necessary precautions to preserve the privacy of the virtual machine instances and their information.

In the virtualized context of a cloud system, several workloads [9] share the same hardware environment, creating difficulties with workload isolation [9], which is essential for diverse departments or domains that wish to keep their data private and distinct from one another. Therefore, the proper principles should be followed for allocating resources among all of the workloads in a datacenter.

The VMM, a piece of simple software, is used to oversee and manage virtual machines (Virtual Machine Manager or Hypervisor). It may have security flaws that jeopardize the privacy of user data, just like any other kind of software. The risk of security vulnerabilities is reduced when the VMM is as brief and uncomplicated as feasible since it makes faults easier to see and fix.

Virtual Machine Images (VMI) are created by the user or the supplier utilizing a variety of settings.

The hazardous VMIs that intruders upload might infect other legitimate users (for instance, a VMI that contains a Trojan horse that a valid user downloads and uses could harm

ISSN No:-2456-2165

that user's computer). These malicious programs might have been used to exploit the user's personal information.

Another issue with Virtual Machine Images (VMIs) or Templates (VMTs) is the potential for information from previous owners to be preserved and exploited maliciously by another user. Therefore, before providing VMIs to another user, the CSP should properly clean them.

In other words, VM access to the local area network should be managed and carried out using the necessary processes in order to avoid unauthorized data flow over virtual networks, or VLANs.

Additionally, it is possible to sniff or spoof such virtual networks at any time [10].

B. Dependability

A security element known as integrity verifies that an asset has not been changed by individuals from a third party who are not authorized to carry out such an activity. This characteristic ensures that an asset's correctness and validity with respect to its owner. The integrity of an asset is often assumed to be altered by append, remove, and edit operations. All web-based attacks—which may alter the contents of user files, databases, virtual machine information, or even WSDL files—are particularly frequent in cloud settings since users access cloud-based services via web browsers.

Under the different integrity standards of the cloud system, the following categories have been addressed here:

(1) Integrity of the Data

Massive refers to Tera Bytes (TB) or even Peta Bytes (PB) of data, and the Cloud system handles a sizable number of processes with huge data needs that are strongly reliant on data. Because of this, platform as a service, software as a service, and data as a service data integrity concerns must be managed correctly. The following problems with data integrity only pertain to clouds:

Data outsourcing at the CSP end clearly poses a danger to the integrity of the data. A client would never be able to demonstrate that CSP destroyed some valid tuples linked to their data [11]. Without the client's knowledge, CSP may provide even partial data sets to the client.

The SQL injection attack, which takes advantage of web servers' vulnerabilities to introduce malicious code into the system and alter the data in user databases, is one of the well-known web-based attacks.

Cross scripting attacks are another kind of malware injection attack in which cybercriminals insert malicious scripts (like JavaScript, VBScript, ActiveX, HTML, etc.) into vulnerable dynamic web pages so that the malicious code is executed on the client's browser and gives them access to the user's account and jeopardizes the security of her data and information.

The metadata spoofing attack modifies the contents of the WSDL (Web Service description document) files to do certain operations for which she may not have authorisation. One of two variations exist for this: In WSDL spoofing, changing the WSDL file's parameters is the primary objective. ii) Reducing the proposed web service's security requirements by altering the WSDL file

[11]. An example of a WSDL spoofing attack is as follows: An example of how a hacker may change a service's WSDL is to make a call to the deleteUser operation syntactically similar to a call to the setAdminRights operation.

The wrapping attack is another frequent attack on web-based services, and it becomes more likely for cloud systems. At the TLS (Transport Layer Service) layer, the content and signature of SOAP messages are duplicated during translation and sent to the server as an authentic user. In order to stop the cloud servers from functioning properly, the attacker may interfere in the cloud and execute malicious malware [12].

(2) Virtualization Integrity

In addition to confidentiality, consideration must be given to the integrity of the Virtual Machines and the VMIs since, as was already established, the virtualization layer itself presents significant security problems that go beyond only secrecy.

Since the assigned VMs on the backend are completely accessible to the CSP administrators, adequate security measures should be made to protect their integrity from insider attacks.

Another method the cloud system might be exploited is if an incursion introduces its own malicious service instance or virtual machine instance. A malicious service instance that infects the whole system may be automatically selected by the CSP to accept user requests as they come in. The system is then tricked into considering the instance as genuine by the attacker. It is crucial to verify the integrity of the 350 services or virtual machine instances that were impacted.

Replication of virtual machines (VMs) is another important component that, if managed incorrectly, might cause data loss. It is suggested that the user appropriately pauses/temporarily deactivates the virtual machines when replicating in order to preserve data integrity. Appropriate controls should be put into place to limit the replication of sensitive VMs and control the migration of VMs into and out of a controlled infrastructure [12].

A cloud computing phenomena known as VM rollback may reestablish certain integrity problems in the VM. Reverting virtual machines may enable passwords or accounts that had been deactivated or restore security weaknesses that had previously been addressed. Therefore, it is necessary to preserve VM snapshots [13].

ISSN No:-2456-2165

The process of VM live migration must be managed, as previously said, and the CSP should be in charge of both protecting the integrity of the protected contents and the maintenance metadata [13].

The lifecycles and state changes of the VMs as they move around the environment must be examined by the CSP. VMs may be suspended, inactive, or active. Additionally, VMs without a state or allotted space in storage are possible. For virtual machines (VMs) that are off, stopped, or without any resources allocated, it's critical to frequently assess their vulnerabilities and install security updates [13].

Virtual machines allow CSP to transfer them across datacenters as required to gain greater processing power or CPU capabilities, which is one of its key advantages. However, security rules and baseline records are necessary for such VMs to work. A VM travels without its security policy, rendering it vulnerable to certain attacks [13].

On cloud security, VM hopping and VM escape both have negative implications. In the first case, the attacker's malware takes advantage of environment vulnerabilities to access the host or hypervisor where the VM is running. VM hopping, on the other hand, describes the malware attacker rotating between VMs that are concurrently running on the same host or under the same hypervisor [13].

C. Accessibility

Availability is one of the most important security elements that a CSP must maintain. The availability of the services must be guaranteed by various commercial organizations that utilize cloud-based services to offer for their consumers since even the slightest downtime may result in a significant financial loss that is irrecoverable. In a typical service-level agreement, the provider commits to fulfill the promised availability and response times. The service level could specify, for example, that resources will be accessible 99.999 percent of the time and that more resources will be made available upon request if more than 80 percent of any given resource is being used. The next section discusses issues with data and VM availability:

(1) Availability of data and services

A denial of service attack is one of the primary causes of service or data unavailability in the Cloud system. A target service is often inundated by the attacker with a huge number of unclear requests. When the cloud computing operating system notices the high demand on the overloaded service, it begins to provide more processing capacity (more service instances). On the one hand, CSP is fighting the attacker (by continuously giving computing resources), but it may equally be argued that CSP is helping the attacker by enabling it to prevent authorized users from accessing the intended service.

An indirect denial of service attack on a cloud system is also possible, and other services operating on the same server as a flooded service may also suffer service outages. Once the server's hardware resources have been exhausted from processing the flooding attack requests, the other service instances operating on the same physical machine may abruptly cease to function. The adverse effect might worsen if the cloud system notices the lack of availability and tries to "evacuate" the affected service instances to other servers. The flooding assault extends to other service types and finally impacts the whole Cloud System as a result of the increased load on those other servers.

Other cloud users may be impacted by some client penetration testing, which might result in the temporary suspension or reduction of certain services [14].

It is conceivable for third-party WAN providers to temporarily disrupt services. It is also feasible for software flaws to impact several copies of cloud data at once and make them inaccessible to their original owners.

Natural disasters like fire, flood, etc. are likely to have an effect on both the main and redundant copies of data in a data center. Again, this puts availability at risk, thus the issue has to be handled properly.

(2) The availability of virtualization

As we've seen, sustaining high availability requires considering a variety of elements, such as network vulnerability, multisite redundancy, and storage failure. But before thinking about cloud availability, virtualization should be paired with it as it is one of the fundamental elements of the Cloud system.

One of the most significant challenges is IP failover [15]. The need to safeguard a production-grade IT system or service application against the failure of any node has been addressed by several software technologies. The bulk of public cloud providers often fall short of providing the minimum standards, and many cloud services don't completely support these software products.

As a consequence, clients end up being reliant on highly available solutions that are not cloud-based. To ensure that the failure of one instance (IP in particular) may be immediately made up for by another instance using some efficient mechanism, it is thus required to safeguard virtual machine instances against such failures [15].

The host system, or more specifically the Hypervisor or VMM (for example, the ESX/ESXi host), may crash or fail at any time, affecting all the virtual machines (VMs) operating on it. In order to avoid such a disaster, the CSP must configure an alternate host machine for all the VMs that were previously operating on the failed VMM.

The aforementioned subjects address some of the most crucial aspects of cloud security. The section that follows has information on a few of the upcoming projects in the field of cloud security.

ISSN No:-2456-2165

IV. PROPOSED SOLUTIONS OR APPROACHES

Some of the remarkable and beneficial methods that have been developed and implemented are included below under the distinct topics of Confidentiality, Integrity, and Availability. The different security criteria of the Cloud System have been explored and implemented to meet them.

A. The confidentiality of data

The two primary issues of data confidentiality in the cloud that have previously been highlighted in the preceding section are the protection of user data from attackers and the assurance that CSP is oblivious of the data it is storing and calculating. These confidentiality issues have been solved using the several encryption methods indicated in Table 1.

Proposed Layout	Implemented algorithms	Required Keys	Implemented encryption type	Complexity	Idea
1.Onion Encryption (OE)	1.Data Encryption algorithm 2.Query execution Algorithm	Randomized (RND) Encryption key, Deterministic, (DET) Encryption KeyOrder Preserving (OPE) Encryption Key, Homomorphic (HOM) Encryption Key	1.RNDprovides Indistinguishability under an adaptive Chosen-plaintext attack. 2. For queries that choose on equality to a specified value, DET offers secured execution. 3. OPE offers secured execution for queries including comparison-based selection 4.HOM is used to run queries that compute server-side aggregates.	O (T1.T2) where T1 = Time spent for rewriting queries, T2 = Time required for encrypting and decrypting payloads. Experiments have shown that the use of this scheme induces an overall drop of throughput by 22.5%.	To enable SQL queries to be executed on encrypted data, including ordering operations, aggregates, and joins, Curinoet al. (2011) [18] introduced an approach of adjustable security with different layers of encryption (like an onion) protecting each value of a tuple. The query processing is done entirely at the CSP side while maintaining the confidentiality of the user data since decryption only occurs at the client side. The only thing to worry about in this situation is keeping distinct encryption levels for each column and decrypting each one to the right level needed for the given query.
2.Fully Homomorphic Encryption (FHE)	1.Key generation Algorithm 2.Encryption Algorithm 3.Evaluation Algorithm	Pk= Public key used for encryption of data. Evk= Key used for evaluation of circuits Sk= Private key used for data decryption	Asymmetric Encryption. 1.Additive Homomorphissm~exponentiation function 2.Multiplicative Homomorphism~RS A[15]	O(λ3.5) per gate for ciphertext refreshing [15] λ=Security Parameter	Homomorphic encryption, as described by Tebbaet al. (2012)[16], would enable clients to encrypt their specific data before saving it at the CSP end. The trick is buried in the fact that the CSP may do the necessary computations on the

ISSN No:-2456-2165

					client data without decrypting it. The secrecy of client data is thus maintained without impairing data calculation thanks to the use of homomorphic encryption.
4.Attribute based encryption for secure scalable fine grained access control (ABE)	1.Setup algorithm 2. Encryption Algorithm 3.Key generation algorithm 4. Decryption Algorithm 5. Proxy Reencryption Algorithm	PK- System public key MK- System master key S -Root secret key PKa- Initial public key of attribute a Ska- Initial secret key of attribute a PKTa Time-based public key of attribute a. PKu -User public key SKu -User identity secret key (UIK) 9. SKTuu,a - Time-based user attribute secret key (UAK)	1. Hierarchical attribute-based encryption (HABE). 2. Proxy reencryption (Time based)	User revocation Cost incurred by data owner= 0 Cost incurred by CSP= O(6N), where N is the number of conjunctive clauses in an access structure.	When fine-grained access control [19] is required, the aforementioned systems use cryptographic techniques to safeguard sensitive user data, but they also place additional burdens on the client or data owner in terms of key distribution and management as well as data management. In addition to addressing user data confidentiality, Yu et al. (2010) transferred the majority of the computational workload associated with the data access control scheme to cloud servers without revealing the underlying data contents. They also introduced a fine-grained access control scheme for cloud environments.
4.Searchable Encryption (SE)	1.Data Encryption Algorithm 2.non-numeric file search Algorithm	Secret number xj, and coefficients cj1, cj2in [- N, N] are used for encrypting the segmented user data where N is a self-defined integer.	1. Secret sharing Encryption Algorithm for numeric data 2. Non-numeric segment Encryption algorithm for text-based data (Uses secret sharing algorithm internally)	O(s*n) per encryption and decryption process. Where s= no of segments into which each alphabet could be split. n= Limited length of each word Detailed cost analysis could be found in [16].	By combining the ideas of searchable encryption and secret sharing, Jyun-Yao Huang and I-En Liao (2012) [17] suggested a method by which a user could search the encrypted tuples (both numeric and non-numeric) from cloud databases and file storages without disclosing the content to CSP.

Table 1:- Analysis of Cloud Data Confidentiality Systems

ISSN No:-2456-2165

Proposed Scheme	Algorithms used	Required Keys	Hypervisor	Agents Involved	Idea
1.TVDc	1. VMM Authorization Algorithm 2.Inter VMcommunication Algorithm 3.Resource Access Algorithm 4.Network Isolation and Infrastructure Integrity algorithms	No keys are used here. But security policies (MAC) exist Comprising of 1) Labels, defining Security classifications of resources,VMs and VMM. 2) Anti-collocation rules containing conflict sets for VMs	Xen	i)Trusted Platform Module (TPM)[8] ii) Virtual TPM iii)IBM hypervisor security architecture (sHype) iv) Management VM or Dom0 v) Access Mediation Hooks (2 sets) vi) Access Control Module (ACM), present inside the core hypervisor	By establishing MAC policy rules throughout the whole Datacenter of the CSP and introducing the idea of workloads, IBM Trusted Virtual Datacenter (TVDc) technology developed a methodology in 2008 that prevented each VM from accessing any other random VM or resource of its choice [9]. The protection provided by this method prevents the leaking of sensitive information and the transfer of harmful software from one workload to another.
2.TCCP	1. Node Registration Algorithm 2. VM launch Algorithm	vii) EkpTC/N= Endorsement private key of TC or N [5] ii)EKPN = Public Endorsement key of N iii) EKPTC= Public Endorsement key of. iv)TKpN/TKpTC = Private trusted keys of Node N and TC v) TKPN/ TKPTC =Public trusted keys of N and TC respectively. vi) KVM = Session key of VM	Xen	i)Trusted Platform Module (TPM) ii)External Trusted Entity (ETE) iii) Cloud Manager (CM) iv) Trusted Node N v) Trusted Coordinator TC (part of TPM) vi) Trusted Virtual Machine Monitor TVMM (part of TPM)	(Santos, Gummadi, and Rodrigues. 2009) [6] created the Trusted Cloud Computing Platform (TCCP) with the goal of maintaining the confidentiality of virtual machines, i.e., to stop CSP (more specifically, sysadmins with root privileges) from carrying out attacks by moving the targeted VM to a domain outside the IAAS's security perimeter.
3. SSC	1. Create_Udom0 2.Create_Userdomain 3. Create_MTSD 4. Grant_Privilege 5. Bootstrapping_SSL	i)AIK =vTPM,s [20] public key ii)freshSym= Client Symmetric key iii)SSLpiv= SSL Private Key	Xen (v3.4.0)	i)TPM [20] ii)vTPM[20] iii)TCB[20] iv)Sdom0 v)Domain builder domB vi)Udom0 vii)User Domain UdomU viii) Service Domain SD i.e. the Security Service ix)MTSD for Regulatory Compliance	A self-service cloud computing system was presented by Ganapathy V (2015) in an effort to address the problems of continuous CSP access to the client CPU, registers, and memory. The key issues that have been highlighted in this study are the attack on Dom0 [20], the involvement of hostile Cloud administrators, as well as client dependence on CSP for enabling or disabling each and every innovative service like VM introspection, migration, and check pointing.

ISSN No:-2456-2165

4.PALM	1. Migration Data Protection Algorithm 2. Metadata Migration Protection Algorithm	vii). Global Migration session Key/ Per page Random key used for encrypting and decrypting secured memory pages before migration. ii) Private platform key issued for encrypting the hash values of the protected pages along with the session keys. iii) Public Platform key used to decrypt hash values of the protected pages along with the session keys on the target machine	Xen	i)Migration Data Protection Module ii)Metadata Management Module [20] iii)SecurityGuard iv) Migration Manager v) Control VM or Dom0 vi)Hypervisor (part of TCB [20]) vii)Hardware (part of TCB [20])	A prototype system called PALM was created by Zhang et al. in 2008 [20] and was intended to ensure security (confidentiality and integrity) of protected user data as well as protection metadata (encryption keys and hashes, process identities, process CPU contexts, process group info, system call info, and opened file info) during and after VM live migration [20].

Table 2:- Comparison between Cloud Virtualization Confidentiality Schemes

Proposed Scheme	**Algorithms used**	**Required Keys**	**Utilised signature/encryption scheme**	**Complexity**	**Idea**
1.Dynamic Provable Data Possession [25]	i)PrepareUpdate(F, info) ii)PerformUpdate(Fi-1,Mi-1, e(F), e(M)). iii)VerifyUpdate(F, info, Mc, Mc′, PMc′) iv) Challenge(n) v)Prove(Fi, Mi, c) vi) Verify(Mc, c, P)	No keys are directly involved in thus scheme. Instead a rank value (r(v)) is associated with each node (v) of the skip list denoting the number of nodes at the bottom level that can be reached from that particular node.	Rank-based authenticated skip lists	O(logn)	A system based on the idea of dynamic provable data possession (DPDP) and using a rank-based authenticated dictionary constructed over a skip list was proposed by Erway et al. in 2009 [25]. This system provides client-verified cloud data integrity as well as dynamic data. Block-less verification is further assisted by the concept of tag, which stands in for each block b.
2.Public Verifiability and Data Dynamics scheme	i)KeyGen(1k) ii)SigGen(sk, F) iii)GenProof(F,Φ, chal) iv)VerifyProof(pk, chal, P). v)ExecUpdate(F,Φ, update) vi)VerifyUpdate(pk, sigsk(H(R)),update, Pupdate)	i)Secret key sk=α.α← Zp [24]. ii)Public key pk=v.v=gα [24]	BLS signature [24].	Verification cost is O(logn). Communication cost is O(logn)	A Public Verifiability and Data Dynamics strategy for ensuring the integrity of Cloud data storage was proposed by Wanget al in 2009. The paradigm allows for dynamic data operations (Modification, Insertion, and Deletion) while maintaining an equivalent level of integrity check, as well as blockless [24] and stateless [24]

ISSN No:-2456-2165

					verification. It also gives TPA control over Cloud data integrity verification. The issue of data privacy has not been taken into account in this plan, in contrast to the prior one.
3.Privacy-Preserving Public Auditing scheme	i) KeyGen(1k) ii)SigGen(sk, F) iii)GenProof(F,Φ, chal,pk) iv)VerifyProof(pk, chal,P)	i)kprp= Random permutation key ii)fkprf=Randomly chosen PRF key iii) MACkey= Key used for generating the MAC.	Public key based homomorphic authenticator with random masking [23]	The total communication cost = O(n/∈) [23].With an extra constant time factor R added for guaranteeing privacy preservation.	A privacy-preserving public auditing approach for ensuring the accuracy and integrity of the data stored in cloud storage was put forth by Wang et al. in 2010. CSP is viewed as an unreliable/unfaithful party since it may delete blocks that the client rarely or never accesses in order to conceal data loss or even free storage. In order to prevent such integrity breaches, the model offers a proper data verification mechanism [23].
4MHT	i) Multi-Join [22] ii) Single-Join[22] iii) Zero-Join[22] iv)Range Condition[22]	No specific keys used. Radix path Identifiers[22] are used.	Tree Signature scheme[22]	Transmission cost is O(log2n) where n= Total no. of data blocks involved (if normal MHT used) Transmission cost is O(n) if RPI based is MHT used.	A Merkle's Signature Scheme was proposed by Niaz M.S. and Saake Gin in 2015 [22] as a way to guarantee user data integrity in cloud storage without the hassle of keeping a (data+signature) table at the data owner end or the danger that CSP could delete some valid tuples or send some incomplete information without the user being able to confirm the fact. As the author noted, the plan may be improved by adding support for multi-user environments and NoSQL databases.

Table 3:- Analysis of Cloud Data Integrity Systems

ISSN No:-2456-2165

Proposed Scheme	Algorithms used	Keys Involved	Hypervisor	Involved Agents
SSC	Create_UDom0(BACKEND_ID, NONCE,ENC_PARAMS,SIGCLIENT) This algorithm is used by Sdom0 to create client meta-domains.	AIK =vTPM,s [21] public key and private key.	Xen	TPM [21], vTPM[20], TCB[20], SDom0, Domain builder domB,UDom0
MIRAGE	Access Control (VMI, Owner), Image Transformation(VMI, Type of filter), Provenance Tracking(VMI, operation), Image Maintenance(Cloud repository)	No specific keys, but Filters [26] are used in this scheme	VMware	Retriever, publisher, Repository administrator [26]
PALM [20]	Migration Data Protection Algorithm, Metadata Migration Protection Algorithm (Already explained above)	Private and Public platform key of TPM	Xen	Retriever, publisher, Repository administrator [26]
ACPS[27]	Activity Checking, Activity logging, Checksum/Hash Calculation, Alert Generation, Security Response Generation	No Keys Used.	KVM	Interceptor, Warning recorder, Evaluator, Warning pool, Security management layer, Hasher

Table 4:- Cloud Virtualization Integrity Schemes Comparison

B. Discretion in Virtualization

Along with data confidentiality concerns, CSPs and cloud customers should be concerned about the confidential execution of VMs operating on the cloud platform. As a consequence, several strategies have been proposed to address these issues; a few of them are examined in Table II.

C. Data Reliability

The integrity of client data stored in the cloud is another key part of cloud security that should be handled by the CSP using the proper methods. The data owner initiated a recurrent practice called data audits to assess the correctness,

value, and integrity of her data. Because it goes against the concept of cloud storage as a whole, downloading all or part of the data from the CSP end and comparing it to the owner copy is a fairly unrealistic auditing strategy. As a consequence, many methods—some of which are listed in Table III—have been developed for ensuring the accuracy of cloud data.

D. Integrity of Virtualization

The term "virtualization integrity" refers to problems with the integrity of the whole virtualization layer, including Virtual Machine data and Hypervisor issues. Various strategies have been proposed to address these problems; some of them are included in Table IV.

E. Data Accessibility

As was previously discussed in earlier parts, one of the major concerns affecting the accessibility of cloud data is DDoS assaults. Numerous DDoS kinds may be realized in the cloud environment.

In 2012, Kumar M.N. suggested an EDoS (Economic Denial of Sustainability [28]) mitigation service called Scrubber Service. It is built on cryptographic conundrums.

Mousa M (2013) [29] created a method for DDoS attack detection in a cloud environment based on measurements of Kolmogorov Complexity.

Somani et al. (2015) [30] created a DDoS mitigation technique using the concept of DDoS Aware Resource Allocation in Cloud. (DARAC). Again, this approach concentrates on EDoS and protects against having an impact on the customer's financial security by controlling the Cloud's auto-scaling capabilities (distinguishing between legitimate traffic and malicious traffic). The mitigation strategy used here is based on an examination of behavioral patterns in people (the number of page requests made from a specific source IP in a minute).

F. Availability of virtual machines

Additionally, it has been advised to deploy intrusion detection systems in addition to virtualized DDoS attack mitigation approaches. The availability of the VMs themselves in the cloud is a significant concern as well. Another aspect of cloud service availability is "IP failover."

IBM SmartCloud business proposed the idea of virtual IP addresses in order to provide High Availability of the Cloud service with reference to IP failover [15].

V. AREAS OF CLOUD SECURITY THAT HAVE BEEN LEAST EXPLORED

Despite the fact that the location of cloud data has long been a contentious issue, no useful research has been done in this area. As indicated in section 3.1.1, a customer who is storing her important data or hosting her applications on the Cloud is ignorant of its original location, thus it is still necessary to design appropriate location-based access control models for addressing such issues. Additionally, a lot of study has to be done before adequate access control methods can be implemented for cross-domain or multidomain [31] of Cloud. Another crucial problem that is integrally tied to cloud security is mutual trust between the CSP and the Client. Although the works of (Hwang, Li, 2010 [32]) based on Reputation systems (for CSP trust evaluation) and (Li-qin Chuang, Yang, 2010 [33]) for user trust evaluation are some of the few in this domain, it is anticipated that a thorough investigation and research in this area will be done in the near future. Data or service compliance is another hard aspect of cloud computing. Since the security and privacy of the data handled by the CSP on behalf of the organizations eventually comes under their purview, it is crucial that the CSP adhere to a specific jurisdiction and establish SLA rules that are acceptable for that jurisdiction. The inability of cloud users and CSPs to work together to identify and address security vulnerabilities is another critical component of cloud security that has to be properly investigated.

VI. CONCLUSION

The study highlights both the critical security flaws and the need for security in an existing Cloud infrastructure. A broad overview of these concerns has been provided here to highlight the need of understanding the security issues in the Cloud computing architecture and providing workable solutions for them. The discussion has concluded with a framework for comparing different cloud security approaches. The general objective of the article is to provide a comprehensive overview of cloud security now and its possibilities for the future.

REFERENCES

[1]. Md. Afroz, Birendra Goswami., “Energy-Efficient Green Technology Cloud Computing”, Proceedings of 2nd International E-Conference in Emerging Trends in Computer Science, Govt. Vijay Bhushan SinghDeo Girls PG College Jashpur Nagar, Jashpur Chhattisgarh, India: pp. 225–228, 2022

[2]. Son, Seokho & Jung, Gihun & Jun, Sung. (2013). An SLA-based cloud computing that facilitates resource allocation in the distributed data centers of a cloud provider. The Journal of Supercomputing. 64. 10.1007/s11227-012-0861-z.

[3]. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[4]. Chen D and Zhao H, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, 2012, pp. 647-651.

[5]. Chou TS. Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology. 2013 Jun 1;5(3):79.

[6]. Santos N, Gummadi KP, Rodrigues R. Towards Trusted Cloud Computing. HotCloud. 2009 Jun 15;9(9):3. [6] Goyal S. (2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. International Journal of Computer Network and Information Security.

[7]. Goyal S. (2014). Public vs Private vs Hybrid vs Community – Cloud Computing: A Critical Review. International Journal of Computer Network and Information Security. 6. 20-29.10.5815/ijcnis.2014.03.03

[8]. Jansen W and Grance T, “Guidelines on Security and Privacy in Public Cloud Computing”, NIST Special Publication 800-144, pp. 5, 2011 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[9]. Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, and Srinivasan D. 2008. TVDc: managing security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev. 42, 1 (January 2008), 40-47.

[10]. Wu H, Ding Y, Winer C and Yao L, "Network security for virtual machine in cloud computing," 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, 2010, pp. 18-21.

[11]. Wang Q, Wang C, Li J, Ren K, and Lou W. 2009. Enabling public verifiability and data dynamics for storage security in cloud computing. In Proceedings of the 14th European conference on Research in computer security (ESORICS'09), Michael Backes and Peng Ning (Eds.). Springer-Verlag, Berlin, Heidelberg, 355-370.

[12]. Kazi Z & S.V V. (2017). Security Attacks and Solutions in Clouds.

[13]. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), 1-13.

[14]. Sen J, "Security and privacy issues in cloud computing", Architectures and Protocols for Secure Information Technology Infrastructures, pp.1- 45, 2013.

[15]. Security and high availability in cloud computing environments in IBM Global Technology Services Technical White Paper (2011).

[16]. Tebaa M, El Hajji S, El Ghazi A. Homomorphic encryption applied to the cloud computing security. InProceedings of the World Congress on Engineering 2012 Jul 4 (Vol. 1, pp. 4-6).

[17]. Huang JY, Liao IE. A searchable encryption scheme for outsourcing cloud storage. InCommunication, Networks and Satellite (ComNetSat),2012 IEEE International Conference on 2012 Jul 12 (pp. 142-146). IEEE.

[18]. Curino C, Jones E, Popa R, Malviya N, Wu E, Madden S, Balakrishnan H, and Zeldovich N. Relational Cloud: A Database Service for the Cloud. In CIDR, pages 235–240, 2011.
[19]. Yu S, Wang C, Ren K, and Lou W. 2010. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" In INFOCOM, 2010 Proceedings IEEE , 1 - 9. San Diego: IEEE.
[20]. Zhang F, Huang Y, Wang H, Chen H, Zang B: PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia-Pacific. Washington, DC, USA: IEEE Computer Society; 2008:9–18
[21]. Ganapathy V. (2015) Reflections on the Self-service Cloud Computing Project. In: Jajoda S., Mazumdar C. (eds) Information Systems Security. ICISS 2015. Lecture Notes in Computer Science, vol 9478. Springer, Cham
[22]. Niaz M..S, Saake G, "Merkle hash tree based techniques for data integrity of outsourced data", GvD, pp. 66-71, 2015
[23]. Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. InInfocom, 2010 proceedings ieee 2010 Mar 14 (pp. 1-9). Ieee.
[24]. Wang Q, Wang C, Li J, Ren K, Lou W. Enabling public verifiability and data dynamics for storage security in cloud computing. Computer Security–ESORICS 2009. 2009:355-70.
[25]. Erway C, Küpçü A, Papamanthou C, and Tamassia R. 2009. Dynamic provable data possession. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). ACM, New York, NY, USA, 213-222.
[26]. Wei J, Zhang X, Ammons G, Bala V, Ning P: Managing Security of virtual machine images in a Cloud environment. In Proceedings of the 2009 ACM workshop on Cloud Computing Security. NY, USA: ACM New York; 2009:91–96.
[27]. Lombardi F, Pietro R.D, Secure virtualization for cloud computing, In Journal of Network and Computer Applications, Volume 34, Issue 4, 2011, Pages 1113-1122, ISSN 1084-8045.
[28]. Kumar MN, Sujatha P, Kalva V, Nagori R, Katukojwala AK, Kumar M. Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. InComputational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 2012 Nov 3 (pp. 535-539). IEEE.
[29]. Prangishvili AR, Shonia OT, Rodonaia IR, Rodonaia VA. Formal security modeling in autonomic cloud computing environment. InWSEAS/NAUN International Conferences, Valencia, Spain 2013.
[30]. Somani G., Johri A., Taneja M., Pyne U., Gaur M.S., Sanghi D. (2015) DARAC: DDoS Mitigation Using DDoS Aware Resource Allocation in Cloud. In: Jajoda S., Mazumdar C. (eds) Information Systems Security. ICISS 2015. Lecture Notes in Computer Science, vol 9478. Springer, Cham
[31]. Xiong D., Zou P., Cai J., He J. (2015) A Dynamic Multi-domain Access Control Model in Cloud Computing. In: Abawajy J., Mukherjea S., Thampi S., Ruiz-Martínez A. (eds) Security in Computing and Communications. SSCC 2015. Communications in Computer and Information Science, vol 536. Springer, Cham
[32]. Hwang K, Li D. Trusted cloud computing with secure resources and data coloring. IEEE Internet Computing. 2010 Sep;14(5):14-22.
[33]. Tian L.Q, Lin C and Ni Y, "Evaluation of user behavior trust in cloud computing," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Taiyuan, 2010, pp. V7-567-V7-572.