Hussain *et al. (IJECI)* 2023

IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701125

Research Article

Vol. 7 issue 1 Year 2023

Security Issues and challenges in Cloud Computing

Hussain Akbar, Muhammad Zubair and Muhammad Shairoze Malik

Department of Information Technology, Superior University Lahore Pakistan

Corresponding author: msisw-f21-003@superior.edu.pk

Received: November 20, 2022; **Accepted:** January 20, 2023; **Published:** March 03, 2023

Abstract:

A cloud computing model allows customers to use a pool of shared computer resources on-demand or pay-per-use basis. In terms of capital investment and operational cost reductions, cloud-based computing offers users and organizations many benefits. Despite these advantages, several challenges still limit the adoption of cloud computing. A crucial concern that is usually taken into account is security. Without this vital component, the computing model has a negative influence, which causes suffering on the human, ethical, and economic levels. This essay will look at the security issues that cloud entities must deal with. This group includes Cloud Service Provider, the Data Owner, and the Cloud User—concentrating on the communication, computation, and service level agreements that make up the crypto-cloud. It will offer the required updates by evaluating the origins and consequences of different cyberattacks.

Key words: Cloud computing, security, high performance, challenges, quality.

1. Introduction

Users are given a network-based environment perception through cloud computing, which makes it possible to share calculations and resources anywhere in the world. Cloud computing is described by the National Institute of Standards and Technology (NIST) as "a template for delivering the appropriate and when required internet access to a shared pool of quickly manipulable programmable grids, servers, amenities, storage, and software." [1]. On-demand self-service, High-performance network access, Accelerated Elasticity, High Scalability, and Defined Performance are the processing type traits shown in Fig. 1. Four deployment types are also offered, including Community, Private, Hybrid, and Public Clouds. Hybrid, community, private, and public clouds. The three service

models—PAAS (Platform as a Service), IAAS (Infrastructure as a Service), and SAAS (Software as a Service)—are then connected with this model. The NIST definition of cloud computing provides the necessary framework, illustrating commonalities, including Geographic Distribution, Homogeneity, Virtualization, and Service Orientation.

Security concerns must be considered when using the cloud service models with all the levels. When the stories are contrasted, the browser's significant dependence puts it at the top. In contrast, the lower levels are more focused on web services. Overall operational costs and investments are reduced, and improved productivity and scalability throughout the levels.

Depending on the customer's needs, hybrid, community, private, and public cloud service models may be used.

Organization: The security issues are highlighted in the following two sections. The problems with security in Service Level Agreement (SLA), computational, data, and communication levels are addressed in Sections 4–7. Lastly, Section 8 concludes with the author's research with other previous studies for comparison.

2. Challenges With Security

Because cloud service providers (CSPs) have data centers in different geographical locations, which presents several security issues and dangers, consumers in cloud computing are oblivious to the precise location of their sensitive data. Due to the quick propagation of threats in virtualized environments, conventional security measures like host-based antivirus, firewalls, and intrusion detection technologies do not provide sufficient security in server virtualization.

2.1. Cloud computing dangers and threats

Walker [2], on the other hand, highlighted that the Cloud Security Alliance (CSA) had published a list of the top 12 cloud-related risks. Table 1 contains a list of these twelve dangers. Data breaching is the most pressing security concern that requires attention among these threats.

2.2. Security in crypto-cloud

As Kamara [3] explained, there are several upsides to utilizing a public cloud. They also noted several security hazards associated with using public cloud services. Many serious worries center on the possibility of damage to the data's privacy and authenticity. Kamara [3] 2010 presented a crypto-cloud architecture, which is depicted clearly in Fig. 3. There are three primary actors involved: the data's owner (the Data Authority), the data's end user (the consumer), and the storage service provider (the Cloud Storage Service Provider) (CSSP). Customers or users of cloud services are granted authorized access to encrypted files uploaded by the data authority. After those steps, the requested file may be downloaded and decrypted using the proper tokens and credentials. These three groups have unique data protection problems in their communications, computations, and SLAs.

Table 1. CSA'S Top 12 threats

Threat no.	Threat name
1	Violated privacy.
2	Passwords and authentication issues.
3	Broken APIs and hacked user interfaces.
4	Taking advantage of loopholes in the system.
5	Taking someone else's account without permission.
6	Contaminated by malicious insiders.
7	The APT virus, or Advanced Persistent Threat.
8	Inaccessible files are forever gone.
9	Having not done enough research.
10	Misuse of cloud services.
11	Attacks using the denial-of-service (DoS) protocol.
12	Shared technology, shared dangers.

3. Security Issues That Cloud Companies Must Deal

Authentication, integrity, transparency, confidentiality, availability, and audits are a few fundamental security criteria that must be addressed in addition to legal security standards, according to Rebollo [4]. The security tree in Fig. 4 is an example of the value of fundamental security criteria. Just like the root anchors the tree in the ground, the issues identified at the root must be correctly treated. The security tree, figuratively represented as the fruits and leaves on a tree, provides advantages in terms of anything/everything as a Service (XaaS) when these fundamental conditions are duly satisfied. Data is transmitted securely using the protocols (TLS) and (SSL), which stand for Transport Layer Security and Secure Socket Layer, respectively.

4. The Quality Of Communication

Due to attacks on Virtual Machines (VMs), there will surely be communication challenges due to the VMs' shared resources, infrastructure, etc. Bhadauria [5] separates this into three categories: network, host, and application. These three tiers of interaction serve as a basis for detecting attacks.

4.1. Security on the level of the network

Data privacy and security are two of the most important aspects of any network infrastructure. When it comes to safety on a network level, the problems include the following:

- Attacks Made Against Domain Name Servers
- Hijacking of prefixes in the Border Gateway Protocol (BGP).
- Concerns Regarding the Reuse of IP Addresses
- Sniffer Attacks etc.

4.2. The security of the application level

Applications require security to prevent allowing attackers the opportunity to obtain control over them by changing settings that they haven't been permitted to modify.

Their configurations.

- ✓ Cookie Poisoning is one of the problems that must be addressed at this level.
- ✓ DDoS.
- ✓ The manipulation of the hidden field
- ✓ An attack with a dictionary
- ✓ Breaking CAPTCHAs
- ✓ Hacking Google

4.3 Security measures used at the host level

At the level of the operating system, which is the foundation upon which applications run, host risks are handled. Worms, viruses, and Trojan horses are the primary dangers found at the host level.

- Profiling.
- Methods for breaking passwords.
- Footprinting.
- A refusal to provide a service.
- Unauthorized entry or use

5. Computational Level

One of the most challenging problems to solve on a computational level is figuring out how to implement virtualization in the cloud.

5.1. Challenges posed by virtualization

Virtualization may be thought of as the abstraction of physical resources. The terms "desktop virtualization," "application virtualization," "network virtualization," " and "server virtualization "machine virtualization" are examples of some of the most prevalent categories of virtualization.

Multiple instances of Virtual Machines make up the virtual layer, which is made up of these machines. It paints a picture of a virtual and distributed environment that operates on top of the cloud architecture and is managed by a cloud provider. The virtualization layer allows it to simultaneously deploy and operate several virtual machines (VMs) on the same physical host. It is carried out by a particular component or piece of software known as the hypervisor or the Virtual Machine Monitor (VMM), which divides up resources among the several VM instances and ensures that they remain isolated. VMs can communicate with one another over the virtual switch, thanks to the virtual network. Ram, the Central Processing Unit (CPU), and storage are examples of hardware resources included in the physical layer.

5.1.1. Security problems at the virtual machine level (also known as the virtual layer)

The virtual machines go through their unique life cycles, which include a variety of states such as being created, pending, operating, suspended, restarted, powered off, shut down, destroyed, and others.

5.1.1.1. Cloning a virtual machine (VM)

Cloning a virtual machine (VM) means creating a clone of an existing VM with the exact identification (ID), computer name, Internet Protocol (IP), and Media Access Control (MAC) addresses. This process is referred to as VM cloning. The cloned virtual machine (VM) shares its virtual resources with the original virtual machine (VM), referred to as the parent. The cloned virtual machine is unaffected by any modifications made to the original VM after completing the cloning process, and vice versa. Because both virtual machines (VMs) will use the same network, there will be a duplication of IP addresses, which may cause security problems.

5.1.1.2. Isolation of VMs

To guarantee safety and security, the VMs need to be isolated. Virtual machines (VMs) can be kept secure by isolating them from one another, even if another VM running on the same physical host is breached. However, virtual machine isolation is not a foolproof solution when the hypervisor has been breached. The virtual machines' shared usage of IP addresses, which breaks the isolation between them, causes problems that must be fixed as soon as possible. This may bring the whole system's performance down.

5.1.1.3. Migration of Virtual Machines

Virtual Machines may be moved simply from one server to another, which helps improve the efficiency with which resources are used. Automating this procedure to achieve load balancing and energy savings is possible. Because of the dynamic nature of the migration, there is a potential for security issues, not only with the virtual machine being moved but also with the new VM host. Live VM migration and non-live VM migration are the two forms of migration. Compared to non-live migration, the live migration process results in a more difficult task.

5.1.1.4. Virtual Machine Exit

Virtual machines (VMs) often operate in secluded and self-contained settings within the host. Any effort by the virtual machine (VM) to directly interact with the hypervisor by intervening in an isolated environment would result in the VM escaping the environment. Therefore, this problem must be handled carefully to avoid compromising the overall virtual setup.

5.1.1.5. VM rollback

Allows virtual machines to be reset to their previous state at any time. Restoring the afflicted virtual machines to their last state may involve the removal of hazardous viruses and worms. As a result, virtual machines (VMs) might be re-exposed to security flaws when rollbacks are performed. Memory snapshot was protected by Sabahi [7] using per-page encryption in conjunction with hashing. The memory contents were hashed using a Merkle hash tree, with the pages' granularity determining the hash's precision. Maintaining logs for the processes, exceptionally suspend/resume and migration, is the recommended best practice. An in-depth investigation indicates that VM rollback, if not managed safely, might activate even hazardous viruses and worms. This was discovered as a result of an investigation into the matter.

5.1.1.6. VM sprawl

Uncontrolled deployment of virtual machines is known as "VM sprawl," and it's a problem that can be avoided. According to Bose [8], VM sprawling is a scenario in which there is a linear growth in the number of VMs, but most themes are inactive. There is a risk that a significant amount of the host's resources will be wasted. Virtual machine sprawl must be controlled to manage resources with the fewest possible efforts efficiently.

5.1.1.7. Virtual Machine (VM) Hopping and Virtual Machine (VM) Hyper Jumps

Virtual Machine (VM) hopping refers to the process of getting access to another VM by exploiting a flaw in the hypervisor. Because of this vulnerability, remote assaults and malware can infiltrate and eventually take control of the middleware packages running on the underlying host by jumping from virtual machine to virtual machine (VM to VM). The most susceptible virtual machines (VMs) are frequently singled out as the entry point for further assaults on the system.

This problem will need to be addressed at some point in the future. The vulnerability in the hypervisor creates a single point of failure in the system.

5.1.1.8. Virtual machine (VM) poaching

The vulnerabilities in the operating system and applications cause the system to behave unanticipatedly. They use up the system resources, which might fail other virtual machines hosted on the same host. It is recommended that patches be applied to both the guest operating system and the regular application to mitigate VM poaching successfully. The issues posed by virtual machines (VMs) are addressed in the publications listed in Table 2.

The overall study shown in Table 2 displays the many options available to ensure the safety of VMs. A comparison of the many methods that have been suggested eliminates the possibility of an increase in either the amount of time required for the execution or the number of test systems. To keep the integrity of the system intact, it is recommended that virtual machines (VMs) not be subjected to the transmission of packets at a fast pace as well as avoiding the application of false assumptions, which would make the problem more complex, and avoiding the oversight of certain specific assumptions and parameters. The Advanced Cloud Protection System (ACPS) raises the level of security and keeps the integrity intact while degrading performance only a little. Wei [9] came up with the idea for a system that assumes several virtual machines (VMs) belong to the same organization, even if they are hosted on a shared network. The authors have argued that there is a requirement for the provision of a protected system, regardless of the virtual machines (VMs) deployed by various enterprises on the same shared network.

5.1.2. Hypervisor level (Virtualization layer)

Qin [10] mentioned that a hypervisor keeps track of virtual machines as they are created, stopped, restarted, and moved around. The Hypervisor or Virtual Machine Monitor (VMM) is nothing more than a low-level code

that is capable of independent operation regardless of the operating system. The hypervisor facilitates virtualization by pooling available resources and supporting many tenants. The hypervisor-based virtualization technique known as para-virtualization is the one that is used most frequently. Complete virtualization and virtualization aided by hardware According to Sabahi [7], hypervisor-based virtualization is prone to having a single point of failure. The current methods for improving hypervisor security are listed in Table 3. All these methods, in their manner, ensure a safe hypervisor. Based on the comparison results, it is suggested that multi-factor authentication be used to strengthen the hypervisor's security further. Protection against software-related vulnerabilities in virtualization cloud computing infrastructures (VCCI) is achieved by combining physical and virtual measures.

Table 2: Security issues in V.M. compared to similar systems.

S. No	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Schwarzkopf, 2012	The protection of cloud-based virtual machines.	Checker for updates: Find software that has become obsolete (inactive)—free online hacking toolkit: Runs tests on virtual machines (VMs) before releasing them.	Prevents execution of flawed VMs. Handles multiple software repositories from different vendors.	The time required to complete a task will linearity Quantity of test systems has grown. Identifying software defects that cause network disruptions.
2	Bindra, 2012	The Analysis and Risk Management of Virtual Machine Images on the Cloud.	Suggest doing a security review of the virtual machine images.	Assures the safety of the virtual machine image	……
3	Shea, 2013	Experiments and Analysis of Virtual Machine Performance During Distributed Denial of Service Attacks	Strengthening the stability and safety of current virtualization technologies. (Denial of Service) Attacks.	SYN- proxies are now in place. DOS attacks are no match for container-based virtualization.	When sending tiny packets rapidly, issues occur.

4	Qin, 2012	State-of-the-art Safeguarding Virtual Machines in the Cloud.	Separated the problems into several virtualization security categories.	Methods are classified as either "within" or "outside" the V.Ms.	Some of the identified performance factors are ignored. Some plans are overly complicated and based on false assumptions.
5	Lombardi, 2010	Safe and sound virtualization on the cloud.	Highly Efficient Anti-Cloud Systems (ACPS).	Better protection for cloud data. Constant vigilance ensures that no one's honesty is compromised.	Minimal hit to performance.
6	Duncan, 2013	Insider Threats to Migrating Virtual Machines in the Cloud.	Using digital forensics and system administration methods, identify malicious insider activity.	Ethernet tap detection of packet sniffing.	There isn't a simple way to tell if a network is being passively tapped or not.
7	Wu, 2010	Safeguarding Virtual Machine Networks in the Cloud.	Recommended an innovative framework for virtual networks to manage VM-to-VM interaction.	Improve safety by adding a firewall and a routing layer to your secure, shared network. Defeats attempts that attempt to sniff or fake your signal.	Virtual machines (VMs) should only be used within a company's shared network.

5.1.2.1. Threats in virtual networking

The potential dangers of virtual networks are that they are challenging to construct securely and that all the cloud components need to be connected. Brohi [11] has argued that hypervisor-resident VFs (Virtual Firewalls) on the VMM is a need for protecting virtual machines. Threats like as traffic eavesdropping (intercepting network communication), address spoofing (faking an IP address), VLAN hopping (breaking network segregation), etc., have been cataloged by Laniepce [6] and will need to be quickly addressed in the future.

5.1.2.2.VM-to-VM attack

Vvirtual machine (VM) can be attacked by another VM on the same physical host, using

hypervisor vulnerabilities and perhaps a side channel attack to compromise the coveted VM, as described by Laniepce [6]. Zhang [12] has suggested a methodology for systematically identifying and investigating several common but elusive inter-VM assaults. Therefore, action is required to resolve the problem.

5.1.2.3. Security issue with VM introspection

Virtual machine (VM) introspection is a security concern since it allows for monitoring VMs on a physical server. Expanded [13] coverage of VMI tools for the hypervisor. Intruding in private virtual machines is a sure way to get unauthorized access to their contents and running processes. That's why cutting-edge safeguards against intrusion are required.

5.1.2.4. Issues due to virtualized trusted computing (VTC)

Problems with virtual trusted computing (VTC) are an emerging concern since this technology represents the next logical step in virtualization but has the potential to compromise security if it fails. As described by Laniepce [6], Trusted Platform Module (TPM), a dedicated TPM is required for each virtual machine (VM) and hypervisor. However, the hypervisor often controls a single hardware TPM, which might introduce vulnerabilities. Dongxi L [14] mentioned vTPM and certificate and critical administration. Trusted Platform Module (TPM) implementation in software exacerbates existing problems in the TCB and introduces new vulnerabilities.

5.1.2.5. Hyperjacking / hypervisor subversion

When an attacker uses a compromised virtual machine (VM) to access the hypervisor and then uses that access to try to take over the virtualization layer. Miller [15] has described the assaults on dropbox, Linkedin, etc., resulting from hyperjacking. According to Microsoft's latest page on Hyperjacking, "viruses planted in the hardware/BIOS can't be identified by the O.S." These problems cause bottlenecks that must be addressed.

5.1.2.6. Issue due to resource sharing

Sharing shared resources is a source of contention since a malevolent VM might cause the intended VMs to go without essential resources. Seventy-five percent of security issues, according to Wueest [16], are the result of sharing resources. The cloud computing paradigm relies heavily on the pooling of available resources. Therefore, it's crucial to work out the kinks in the system that prevent people from pooling their resources.

5.1.2.7. Challenges to the Security and Isolation of Virtual Machines (VMs) Caused by Hypervisors: The hypervisor controls the degree of separation between virtual machines. There is a risk that guests' secrets will be revealed if the hypervisor's security is not guaranteed. Therefore, the hypervisor needs better techniques for controlling access.

Table 3: Here are a few publications that discuss the difficulties with hypervisor security

S. no.	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Romney, 2013	Hypervisors' Versatility, Adaptability, and Productivity in the Classroom of Engineers.	co-created a Master of Science in Cyber Security and Information Assurance (MS-CSIA) degree program at NU with Efficiency Student access to cutting-edge technology; agility; flexibility; simplicity of cloning;	The use of more than one authentication method improves safety. The bandwidth has been doubled from 50 Mbps to 100 Mbps.	When virtual memory (VM) size grows from 200 to 770, it becomes a crucial concern.
2	Sabahi, 2012	Safeguarding Virtualization in a Cloud Setting Technology based on a hypervisor is used.	Recommended a different approach to virtualization security that relies on a hypervisor.	A safer environment. Identifies an overflow attack. Better use virtualization.	Both VSEM and VREM are essential to the effectiveness of a security system.
3	Turnbull, 2013	Limitations: Examining Possible Entry Points for Hypervisor Attacks.	Four possible attacks in the ESXi5.0 hypervisor were found and examined.	Cloud computing is now safer to eliminate data rerouting and system call hooking.	
4	Brohi, 2013	Security Risks in Virtualized Cloud Computing Environments: Identification and Analysis (VCCI).	The Virtualization Attack Model (VMM) is a technique for virtualizing CCI-style attacks against VCCI.	Protected VCCI by tracing intrusions both from the inside and the outside.	

5	Laniepce, 2013	Intruder Detection and Prevention in IaaS Clouds using Hypervisor-Based Engineering.	advocated for a hypervisor-based method of keeping tabs on things	Perhaps most encouraging, it strengthens end users' virtual machine (VM) security.	That's up to the reliability of your cloud service.
6	Nimgaonkar, 2012	Ctrust is an infrastructure for running applications in the cloud safely and reliably.	The Ctrust framework, a proposed attack model, and a prototype implementation are presented.	Gives people a sense of safety and confidence. Scalable.	The incorporation of hardware design.

The VMM/Hypervisor from both internal and external threats. When an overflow attack occurs, hypervisor-based monitoring immediately alerts the administrator. By safeguarding the hypervisor as a whole, we can eliminate a potential catastrophic failure point (SPoF). If you want to implement the no hypervisor idea, you'll have to upgrade your operating system to include all the capabilities that hypervisors typically provide. However, doing so increases the already high complexity of the OS beneath it. This means that the hypervisor is essential for implementing virtualization.

For cloud computing to work, virtualization must be at its core. The VMM allows for the construction, suspension, restart, activation, and allocation of resources for Virtual Machines (VMs). The cloud computing paradigm suffers from SPoF's performance degradation and must be protected.

Cloud-based virtual machines (VMs) share the hardware layer's central processing unit (CPU), memory, network interface card (NIC), and storage space (among other resources). If a visitor can circumvent DAC and MAC due to a hypervisor flaw, isolated protections are at risk. Hardware security and vulnerability considerations have been brought to light, as Zissis [17] has noted. In the lack of protection to hardware, a variety of dangers, including Distributed Denial of Service (DDOS), hardware disruption, hardware theft, hardware modification, abuse of infrastructure, and so on, are a possible; server placement, firewall upkeep, and hardware health monitoring are all problems at the physical layer, as categorized by Mathisen [18].

In addition to the problems described above, hardware health monitoring is essential, as Turnbull [19] explains. This is necessary for determining the capabilities of the various hardware components and conveying that information to the kernel and the virtualization manager. To reduce the impact of issues in the physical layer, the system should employ a

robust authentication method in the virtual Border to lessen hyperjacking's associated problems.

6. Problems With The Data Itself

Any crypto-cloud system's entities may be considered extensions of the data that serves as its source and beating organ. Table 1 shows that CSA feels data breaches are the most significant security risk. Understanding how many layers of protection the new computing technology offers to the data the author foresees before adopting is crucial since hacking skills are also well-versed. Data Leakage is a problem that arises when data is stored off-site (outside of our control) to support several tenants. Data at every point of its life cycle—from creation to distribution to use to sharing to archiving to deletion, as outlined by Chen [20]—must be safeguarded. Generally, there are two types of data level security: those that apply while the data is in motion and when the information is at rest. Since data transmission is performed using TLS by default, there are no additional security concerns associated with data-in-transit compared to data-at-rest. It's more appealing to a hacker to access data when it's resting in storage.

6.1. Information in transit

During data transfers, entities in the crypto-cloud interact with one another. Instances of the following problems may arise due to the entities' attempts to communicate with one another via a secure communication channel, such as Transport Layer Security.

6.1.1. Data Lineage

There's the concept of "data lineage," which refers to the history of where and from whom specific data has been collected. Data lineage is a concept suggested by Bhadauria and Sanyal [5]. It's useful for auditing. Due to the non-linear structure of the cloud, it is one of the most challenging and time-consuming aspects of tracing.

6.1.2. Data Leakage

The second problem is data leakage, which occurs whenever more than one tenant accesses data. As Sabahi [7] described, one of the concerns is information loss. Security flaws in Google Docs have been known since at least March 2009, when Chen first brought them to light [20]. With such a high risk of compromised information, handling must be done with extreme caution. Leaks of sensitive information can occur through various channels, including instant messaging, email, webmail, blogs/wikis, malicious web pages, the file transfer protocol (FTP), and USB/mass storage devices.

6.2. DATA- IN-REST

Vyas [21] presented a method for ensuring data integrity and performance during cloud storage and retrieval. Improve cloud data security by storing encrypted files, hash files, and meta-data.

Data security in the cloud, using cryptographic mechanisms to protect individual privacy, is a topic that has been extensively reviewed by Chatterjee [22].

6.2.1. Data Recovery

Data recovery is extracting data from damaged or unreadable storage media and restoring it for use. Figure 11 shows the progression through the four stages of data recovery. When a file is deleted, just its information is erased; the data itself is still stored on the disc. Retrieval using "file carving" is possible. Bifragment gap carving, Smart Carving, and Carving memory dumps are a few examples of popular Carving techniques. Problems with the operating system, the disc, or the deletion of files are common obstacles to data recovery. These obstacles must be conquered.

6.2.2. Data Remanence/Sanitization/Removal

All data must be thoroughly and safely wiped after its useful life. One of the most time-honored methods of cleaning data is overwriting. As stated by Chen [20], physical properties allow for the restoration/recovery of lost data, which might lead to the exposure of private information. It is feasible to retrieve information from damaged storage media with the proper knowledge and tools. There has to be consideration given to the persistence of data after deletion.

6.2.3. Data backup

Data loss occurs when data is updated often. In the event of data loss, it is essential to have a recent backup stored in the cloud or on an external server. The 3-2-1 rule, as outlined by Bhargav Vora [23], requires keeping three copies of all critically significant data: one primary copy and two backups. Two separate storage mediums are used to protect against potential threats. Hold one duplicate in a secure location. Replication maintenance compromises data safety.

6.2.4. Data isolation

Information must be kept completely isolated from unauthorized access. Access control and encryption methods should protect sensitive information from prying eyes. A user's identification can provide several fine-grained access control types, such as attribute-based, time-based, etc. Isolation is a very exclusive setting. Carelessness can result in a virtual machine (VM) to VM assault, compromising user privacy.

6.2.5. Data segregation

The separation of data across users in a virtualized cloud environment is known as "data segregation." Data segregation is a concern brought up by multi-tenancy, according to Negi [24]. Data segregation in the cloud should be accomplished with the help of highly protected protocols and encryption methods. SQL injection, unsecured storage, and improper data validation contribute to data segregation issues. In a multi-tenant setting, the difficulty of data segregation can be reduced by catering to tenants' specific needs in the ways outlined.

6.2.6. Data Lock-in

Data lock-in is the most significant barrier to achieving data portability and interoperability, bringing us to point six. Sax [25] warns that, according to a well-documented industry perspective, the possibility of cloud provider lock-in impedes the free flow of data into, throughout, and beyond the cloud. Due to the

lock-in nature, it is challenging to integrate data from many sources. Cloud users should be unaffected by the current situation with one provider.

6.2.7. Data Location

Where the data is physically stored is crucial to the success of any storage as a service model. Users are hesitant to keep sensitive data in the cloud due to the lack of transparency surrounding the data's physical location. It's a typical challenge for businesses. Concerns about data safety, legality, and meeting regulatory standards arise when their whereabouts are unknown. This is a complicated matter because certain cloud storage services can't be relied on.

Problems that arise when data is both in motion and at rest constitute Section 6.3.

1. The first tenet of sound data management ensures that only authorized parties may read and change stored information. Independent verification of data integrity is possible. However, Kaur [26] offered a data correctness system that assured data security through a third-party audit. Static and dynamic data require security measures to prevent accidental or malicious use or disclosure.

2. Integrity and computational correctness are data provenance aspects, referred to as "provenance." Provenance may be defined as (integrity + computational correctness =). However, Muhammad Rizwan Asghar[27] emphasized the significance of provenance in post-incident investigations by explaining how data is created. Martin[28] proposed a risk-based strategy for determining origin. Data provenance presented several difficulties, including computational cost, storage overhead, platform independence, and application independence.

Table 4: The current methods for fixing Data Level Challenges

S. no	Author	Title of the security scheme	Work proposed	Strengths	Weakness
1	Chen, 2012	The challenges of protecting sensitive data and personal privacy in the cloud.	Survey: Data security and privacy at different stages of the data's life cycle were analyzed.	Discussed the data security and privacy studies that will be conducted in the future	
2	Wang, 2012	The move toward safe and reliable cloud storage services.	Saving money on bandwidth and processing by auditing cloud storage.	Accurately pinpointing the source of data problems in a hurry. Dynamic efficiency.	Stores supplemental data structures locally for ease of usage.

3	Liu, 2013	Safe Multi-Owner Cloud Data Sharing for Evolving Communities, or Mona.	With MONA, cloud-based groups may be dynamic and responsive.	100% Safe and Effective. Revoked users incur no additional costs for storage or processing.	
4	Wei, 2014	Protection of personal data during cloud computing storage and processing.	Prevention of privacy breaches and promotion of a trustworthy auditing methodology for computing.	This first protocol audits safe storage and computation—the bare minimum.	Using SecCloud takes a little longer than the original protocol.
5	Dong, 2014	Developing a cloud-based file-sharing service that meets these criteria—efficient, scalable, and protective of user privacy—is a primary goal of modern cloud computing.	A strategy utilizes both CP-ABE and IBE methods.	Data privacy is efficient, scalable, and adaptable. Safe and allowing for granular permissions	
6	Dong, 2015	Cloud-based data collaboration services that prioritize security and scalability, aka SECO.	An identity-based, multi-level encryption system for use in an insecure cloud environment.	Safe online data sharing with granular permissions Efficient Minimal computational, networking, and storing overhead.	Data synchronization and security concerns have not been resolved.
7	Khalid, 2013	Protocol for improved authentication and authorization based on security and privacy, implemented in the cloud.	A method for establishing trust and exchanging information in an untraceable fashion.	Simplicity to implementing Compatible	

8	Sun, 2013	A system for assessing encryption software based on its properties.	The use of properties is recommended to verify the security of encryption software.	Effective. Effectiveness at finding problems is rather good.	The differences between defects that have been mimicked and those that occur in real-time are striking. The Number of Metamorphic Relationships is bounded (Mrs)
9	Liu, 2014	Cloud-based data sharing security protocol that uses time-based proxy re-encryption.	A TimePRE that causes a user's privileges to lapse on their own time.	Accomplishes efficient and granular access control. A safe and helpful option There is no granularity in the time measurements.	The user's total number of keys will increase proportionally. The price of decryption is little.
10	Koo, 2013	Safe and quick decryption of encrypted data. Data on the cloud utilizing attribute-based encryption.	A fast information retrieval system based on ABE.	Optimal for Large Data Archives Controlled entry and rapid searching	
11	Puthal, 2017	The efficient security of large-scale sensing data streams based on a dynamic prime number.	Security verification for massive data streams using dynamic prime numbers (DPBSV).	It cuts down on time spent communicating. Increases verification efficiency. Saves time. Make use of minimum size.	
12	Shaikh, 2015	Cloud computing security is only achievable with properly organized data.	A system for collecting and analyzing data tested with representative data sets.	Strength and safety are greatly enhanced.	

The most fundamental component of a cloud that needs protection is its data. Threats to data security can occur both while information is in transit and while it is stored. Without adding to the cost of storage, transmission, or computing, Table 4 outlines the several security concerns that must be overcome. For instance, the SecCloud method adds negligible time over the currently used, more insecure protocol. Reducing exposure even if doing so causes unexpected financial strain. Combinations of encryption methods that are efficient, scalable, adaptable, secure, and allow for granular control over who has access to data. Research in the future can focus on methods that improve security while requiring less work from administrators.

A system that provides maximum security at a minimum cost in terms of memory, bandwidth and processing power is urgently required. The system must be reliable, extensible, and safe. Security, however, should not be an afterthought; instead, it should permeate the entire system and be built at each step (Computational, Communicational, and Service Level Agreement).

7. Service Level Agreements (Slas)

Providers are responsible for delivering services to customers by agreed-upon SLAs. The obligation of upholding SLAs falls on crypto-fundamental cloud entities' shoulders. Bandwidth, central processing unit, memory, and critical management are just a few factors that might affect resource allocation at any given time. SLAs may be broken down into three distinct tiers: customer-centric, service-centric, and multi-tiered. The amount of money and workforce allocated is crucial and shouldn’t be underestimated.

While privacy concerns motivate the development of service-level agreements, principles of honesty motivate their introduction. Hoehl [29]. Risk reduction and efficient assignment of responsibilities between parties is facilitated by incorporating security metrics within the SLA. Regarding security management, no one SLA standard fits all scenarios. However, measures such as the European Commission's SPECS (Secure Provisioning of Cloud Services) and ENISA's (European Network and Information Security Agency) guarantee security by requiring the upkeep of SLAs. Quality of Service (quality of service) may be improved using SLA. Define, negotiate, monitor, and enforce the terms of a contract using Service Level Agreements. While defining and negotiating a contract, both parties can determine their respective roles and the duration of their separation agreements. The relationship between the supplier and the customer is strengthened using monitoring and enforcement.

Guaranteed service availability was also brought forward by Dash [30]. Depending on the SLA, the provider's capabilities, the efficiency of the users, and the accessibility of the services will vary. To mitigate any adverse outcomes, consider the following information. Loss of bandwidth and operations, business continuity, data location, data appropriation,

data integrity, and data dependability are just a few of the many concerns that must be addressed. The pay-as-you-go business cannot persist without adequate SLAs.

8. Wrapping Up

Questions of data, system and Service Level Agreement security are examined. Security problems with virtualization and data are seen as the most dangerous to a computer system. The benefit of cloud computing is enhanced through virtualization, a core component of the cloud. The problems that can arise at the virtual, virtualization and physical levels are discussed. There are two main types of data security problems: those that occur when the data is at rest and those that occur while it is in transit. Both are investigated, and there's a pressing need to resolve any problems. Numerous chances for hackers to crack the crypto-system exist nowadays due to the proliferation of security threats. However, many studies and polls agree with the author's vote. Cloud computing still appears to be in its infancy regarding protecting user data.

Table 5 shows how our survey stacks up against previous survey papers when comparing the three foundational dimensions. The table reveals that very few reports have comprehensively examined the causes and consequences of problems at the Virtual Machine, Hypervisor, and Hardware levels of computing. Future research on Service Level Agreements has to be deeper and broader. This article paves the way for future research in cloud computing to explore previously uncharted territory.

Table 5: A look at our study in comparison to others from three different vantage points

S. no	Author	Communication level		Computational/Functional level			SLA level	
		Network level	Application level	Virtualization			Data security	
				V.M. level	Hypervisor level	Hardware level		
1	Ali, 2015	X		X	X		X	X
2	Rong, 2013						X	X
3	Zissis, 2012		X	X		X	X	
4	Sun, 2011	X	X				X	
5	Shahzad, 2014	X					X	X
6	Rao, 2015	X					X	
7	Soofi, 2014	X	X				X	
8	Warhade, 2014	X	X				X	
9	Padhy, 2011	X	X	X			X	X
10	Denz, 2013			X	X	X		
11	Ouedraogo, 2015			X	X		X	X
12	Rawat, 2014					X	X	
13	Our survey	X	X	X	X	X	X	X

Table 5: A look at our study in comparison to others from three different vantage points

Security should not be an afterthought for cloud service providers; it should be a primary concern.

9. References

[1] P. Mell and T. Grance. "The NIST definition of cloud computing". National Institute of Standards and Technology; 2009http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] K. Walker. "Cloud security alliance(CSA)". The treacherous 12: cloud computing top threats in 2016. https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/.

[3] S. Kamara and K. Lauter. "Cryptographic cloud storage". Microsoft Research Cryptography Group; January 2010 http://research.microsoft.com/pubs/112576/cryptocloud.pdf.

[4] O. Rebollo, D. Mellado, E. Fernandez-Medina and H. Mouratidis. "Empirical evaluation of a cloud computing information security governance framework". Inf SoftwareTechnol 2015. vol. 58: pp. 44–57www.elsevier.com/locate/infsof.

[5] R. Bhadauria and S. Sanyal. "Survey on security issues in Cloud Computing and Associated Mitigation Techniques". Int J Comput Appl (0975-888). vol. 47, no. 18. June 2012.

[6] S. Laniepce, M. Lacoste, M. Kassi-Lahlou, F. Bignon, K. Lazri and A. Wailly. "Engineering intrusion prevention services for iaas clouds: the way of the hypervisor", 2013.IEEE seventh international symposium on service-oriented system engineering.

[7] F. Sabahi. "Secure virtualization for cloud environment using hypervisor-based technology". Int J Mach Learn Comput. vol. 2, no. 1. February 2012.

[8] R. Bose and D. Sardar. "A Secure Hypervisor-based technology creates a secure cloud environment". Int J Emerg Res Manage Technol. Vol. 4, no. 2. February 2015.

[9] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen and AV Vasilakos. "Security and privacy for storage and computation in cloud computing". Inf Sci;258: pp. 371–386. 2014. www.elsevier.com/locate/ins.

[10] Z. Qin, Q. Zhang, C. Wan and Y. Di. "State-of-the-art virtualization security in cloud computing". J Inf Comput Sci. vol.9, no. 6. 2012.