Cloud Computing Security Challenges & Solutions-A Survey

Srijita Basu
Department of Computer Science & Engineering. IEM
Institute of Engg. & Management
Kolkata, India
srijita.basu202@gmail.com

Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar
Department of Computer Science & Engg & IT
Institute of Engg. & Management
Kolkata, India
{bardhan.arjun, koyal.gupta1107}@gmail.com

***Abstract*— Cloud Computing and its' related security issues as well as countermeasures are one of the highly debated topics in today's research field. Though, various surveys regarding Cloud security are already prevalent, there remains a certain gap between the proper mapping of these issues to their corresponding solutions. Some surveys present the Virtualization issues and solutions while other deal with the access control mechanisms, but what lacks is a common framework that would at the same time generalize the concept of cloud security as well as intricately analyze its' specific requirements. Moreover, countermeasures that are provided in a survey must clearly depict the issue that it is handling. Keeping all these factors in mind this survey paper has been designed so as to cover the necessary areas with a proper interconnection between them and lastly discuss a set of open problems in this domain.**

Keywords—: Cloud computing, Virtualization, Data security

I. INTRODUCTION

Cloud reflects the concept of a distributed system comprising of a group of virtual machines that can be dynamically provisioned to meet the varying resource requirements of a customer [1] and the entire base of this Cloud-Customer relationship is governed by the SLA (Service Level Agreement). The National Institute of Standards and Technology (NIST) defines Cloud as a model that enables convenient on-demand network access to a shared pool of configurable computing resource e.g. network, storage, hardware, applications, etc. that can be rapidly allocated, scaled as well as released with minimum management effort or service provider intervention[2].

Cloud relieves the user of the overhead of physical installation and maintenance of her system, which automatically reduces the overall cost and enhances the system efficiency. Embracement of Cloud based services results in introduction of an abstraction layer between the physical storage or servers and the user whose data or services are being processed in the Cloud. The present scenario is such that the Cloud consumer who can be the data or service owner has to rely completely on the Cloud Service Provider (CSP) for the privacy and security of her information. The notion of mutual trust is achieved to some extent by negotiating the SLA but still a good number of cloud specific security issues become inevitable that need to be handled by either the CSP or the user itself.

Data holds the topmost position when it comes to IT security concerns, irrespective of the infrastructure being used. Cloud Computing is no exception to this, moreover it focuses on added security concerns because of its distributed nature and multi-tenant architecture. The data life cycle comprises its generation, storage, usage, distribution and destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms [3]. For example, if the web application (shared application) is insecurely programmed, a customer could possibly use an SQL injection [4] to gain unauthorized access to another customer's data, and delete or manipulate it. To prevent this, appropriate security measures must be implemented. The phenomenon of data deletion is again somewhat crucial in the cloud and therefore should be handled carefully by the CSP to ensure permanent and complete destruction of data on a client's request. Moreover, the data backups (scope, saving intervals, saving times, storage duration, etc.) used to avoid data losses should be transparent and auditable for the customers. All these issues and several others need to be taken care of while using a cloud service

Virtualization plays another important role in cloud computing since it allows for the appropriate degree of customization, security, isolation, and manageability that are fundamental for delivering IT services on demand. IaaS (discussed in later section) is based on the concept of hardware virtualization whereas programming level virtualization contributes for the PaaS (discussed in later section) offerings. With virtualization, comes the concept of Server Consolidation, which enables sharing of resources of a single physical server by a number of applications or services simultaneously without interfering, or even revealing it to the client applications. Thus, it is quite clear from the discussions so far that Virtual Machines construct the entire back-end for Cloud based services. At the same time it induces certain threats for the Cloud. It opens the door to a new and unexpected form of phishing. The capability of emulating a host in a completely transparent manner may led to extraction of sensitive information from the guest by malicious programs.

Moreover, the concepts of Virtual Machine Image [5], and Live Migration [5] at the same time acts useful for the consumers as well as introduces certain security flaws that need to be handled by the CSP.

Therefore while security in Cloud is considered, it should not be constrained within the limits of data security but the corresponding Virtual Machine (VM) security should also be considered equally.

The entire Cloud architecture and its variation from the traditional on-premise system makes identification and segregation of the various aspects of cloud security, a challenging task. Therefore, the main focus of this paper is to categorize the Cloud security into suitable domains and explore the proposed solutions.

The rest of the paper is organized as follows. Section 2 gives a brief overview of the Cloud Service and Deployment models. Section 3 presents a detailed study on the essential Cloud security issues. Section 4 surveys some of the proposed solutions. Section 5 summarizes the unexplored/least explored areas of Cloud security. Finally, Section 6 concludes the paper.

II. CLOUD PROPERTIES AND MODELS

A. Cloud Service Model

NIST classified Cloud into three service models [2] that provide services at different layers of a business model.

- **Software as a Service (SaaS)**: It describes a cloud service where consumers are able to access software applications running on a cloud infrastructure, over the internet. *SaaS* not only incurs no initial setup cost or underlying infrastructure maintenance cost but also automates all the updates. *SaaS* has the minimum customer control on security as the underlying infrastructure as well as execution platform lies outside the range of the user.
- **Platform as a Service (PaaS)**: *Platform as a Service (PaaS)* is an abstracted and integrated cloud-based computing environment that supports the development, running, and management of applications. It is a delivery of a computing platform over the web. Control on the underlying cloud infrastructure including network, servers, operating systems, or storage, lies within the hands of the CSP whereas consumers are allowed to have certain controls over the deployed applications and possibly configuration settings for the application-hosting environment. *PaaS* model offers greater extensibility and greater customer control on security than *SaaS* but less than that of *IaaS*.
- **Infrastructure as a Service (IaaS)**: *IaaS* is the virtual delivery of computing resources in the form of hardware, networking, and storage services. In this model customer control spans the spheres of operating system, deployed services, and selected parts of the network. The infrastructure is managed wholly by the CSP. *IaaS* thus provides an increased amount of security control in the client's court as compared to the previous models.

B. Cloud Deployment Model

Depending upon the suitability and exact purpose of the user Cloud is again divided into four deployment models by NIST.

- Public Cloud: Cloud services are provided to general users or large business enterprises and the Cloud resides at the service provider end. Public Cloud ensures scalability and reliability but at the same time introduces several issues that turn out to be disadvantageous for customers. Customers remain ignorant about the type of storage used by the CSP, the geographical location of their data, the organization whose data is stored with its data (i.e. certain issues of multi-tenancy). Thus, organizations have to compromise with certain security aspects while it moves to public cloud.
- Private Cloud: Cloud services are provided exclusively for a single organization and the Cloud is owned by either the organization or by a third-party, located on or off premises. Private Cloud solves the security issues of Public Cloud but at same time introduce overheads of storage management, capacity watching and provisioning etc.
- Community Cloud: Cloud services are provided exclusively for a community of organizations that have a common interest (e.g., mission, security requirements, policy, or compliance considerations) and the Cloud is owned by either the organizations or by a third-party, located on or off premises. The drawback of this model lies in the fact that there are still a number of unanswered questions regarding service outages, contractual and security implications i.e. issues regarding data being spread across multiple organizations and multiple domains[6].
- Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [6]. Hybrid cloud offers the benefit of cost and scaling like public clouds, while the security and control of private clouds are also taken care of. The issues which poses threat on the hybrid cloud includes the data privacy and integrity concerns while data flows from public to private environment or vice versa since privacy controls in the public cloud environment vary significantly from the private cloud[6].

In the next section we detail the various security issues prevalent in a Cloud environment.

III. CLOUD SECURITY ISSUES/REQUIREMENTS

Trusting the Cloud Service Provider (CSP) and their offerings is one of the strongest driving forces behind the decision of a user to move into a cloud system or continue with the legacy system. Trust is based on the assessment as to whether a provider has covered all the risks, including areas of data security, VM security as well as other government and compliance issues. The three factors that have been considered here for the evaluation of the Cloud system security are **Confidentiality**, **Integrity**, and **Availability (CIA)**. As the CIA, domain is a widely used convention for determining the security concerns of a traditional information system, the main focus of this section is to generalize the security requirements in an existing Cloud system under this domain. Further sub-categorization and fine grained classification of security issues have been presented here which would ease the understandability, mapping and evaluation of the cloud specific attacks and proposed solutions presented in the later sections.

A. Confidentiality

Confidentiality refers to the protection of some enterprise asset from disclosure to unauthorized users. In a Cloud System such users may be clients who might want to get unauthorized access to the data of some other individual which is stored in the same table as that of the intruder's data by the CSP. It may also be the case that the CSP itself contains some dishonest or inquisitive members who could view or even tamper with the client's private and valuable data. Other than client's data the Virtual Machine network, Virtual machine image, etc has inevitable confidentiality requirements.

Under the various confidentiality requirements of the cloud system the following categories have been discussed here:

1) Data Confidentiality

Data residing at the CSP end is often stored and processed in plaintext. Thus CSP (*SaaS*) is held responsible for maintaining the confidentiality of client data during it's entire life cycle. Some cloud specific data confidentiality issues include:

A number of Cloud Storage providers allow shared access to online folders that store the user data. This may result is potential loss of data confidentiality. Even when a file is shared in a group using a Cloud storage service the owner must get periodic updates about any changes regarding the group. In short, client **data segregation** from other data (competitor, unauthorized user) must be handled explicitly by the CSP.

The actual **geographical location of the user's data** is another factor that affects the data confidentiality. CSP can actually move the data from one data centre to another which in many cases changes the entire set of legal rules enforced (if the data crosses the boundary of a country) [7].If user processes data in the UK, store it on servers in the US and send it via France, then it becomes difficult to determine the exact laws that should be obeyed and naturally poses a threat to the confidentiality of the user data [7].

Improper or **incomplete data deletion** by the CSP can be dangerous for the consumers who requested for service removal, or whose subscription period might have ended. The remnants of the deleted data might cause a confidentiality breach of such users.

In some cases, CSP may use third-party assistance for **data-backup services**. Such un-trusted third-party service providers may utilize the personal data of the client in some unfair means which naturally hampers the confidentiality of her data.

Cloud consumers may often request for more **monitoring or log data** for their own convenience and safety. Log data contains sensitive infrastructure data of the service provider which should again not be compromised by the Cloud. Therefore, several negotiations need to be made between the CSP and the users regarding the particulars of log data that should be shared with the clients without compromising with the CSP's confidentiality.

Cloud service providers that do not allow data owners to **encrypt** their own data or information before deploying them on the cloud, poses a serious threat to the user data confidentiality. Sensitive information such as medical or health records, government or defense data should not be stored in Cloud if encryption options are not available.

Cloud service providers in some cases are assumed to be honest but curious. They are more interested in knowing the contents of the user data files as well as the **user access privilege information**. Suitable access control policies should be devised by the owners in order to avoid such situations.

2) Virtualization Confidentiality

In *IaaS,* CSP hosts virtual machines where the user applications are executed. In a Cloud system, anyone with privileged access to the host can read or manipulate the deployed service that resides in each VM. Therefore, users cannot protect the confidentiality of VMs on their own. Thus, the total virtualization layer induces certain security loopholes that appear to be a serious matter of concern when considering Cloud security issues. Few of those are discussed as following:

An individual acting as the system admin of the CSP may login remotely to any existing machine with **root privileges**. The system admin could then divert this VM to some other VM which is under her control and outside the *IaaS* security perimeters [5]. Such internal attacks can necessarily cause a breach in confidentiality of the customer data or application.

VM migration, especially live migration [5], is an expedient feature of Cloud Computing systems for load balancing, elastic scaling, fault tolerance, and hardware maintenance. The CSP should adopt necessary means to preserve the confidentiality of the VM instances as well as VM metadata during and after the live migration.

In the virtualized environment of a Cloud system, multiple workloads [8] share the same hardware environment and this gives rise to issues of **workload isolation** [8] which is highly required by different departments or domains who want to keep their data separate and secure from each other. Thus, appropriate rules should be applied to govern the sharing of resources among all the workloads in a datacenter.

The **VMM** (Virtual Machine Manager or Hypervisor) is low level software that controls and monitors its virtual machines. Similar to any traditional software it may also encounter security flaws which may lead to certain compromises with user data confidentiality. Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it becomes easier to find and fix any error.

Virtual Machine Images (VMI) are either created by the provider or by the user itself with different configurations. Malicious VMIs uploaded by certain intruders could infect the other legitimate customers (e.g. A VMI having malicious code containing Trojan horse could possibly be downloaded and used by some valid user thus ruining his system). Such malicious codes could be designed in such a way so as to exploit certain confidential information of the user.

Another issue related to Virtual Machine Images or **Templates** is that VMIs may retain previous owner information which may be misused by some other user. Hence VMIs should be cleaned properly by the CSP before assigning it to some other user.

Virtual Networks or **VLAN**s should also be isolated in order to avoid unauthorized flow of data through them or in other words VM access to the Local area network should be controlled and implemented using suitable methodologies. Moreover, chances always exist for sniffing or spoofing such virtual networks [9].

B. Intergrity

Integrity refers to the security property of an asset that guarantees that it has not been modified by some third-party personnel who is not authorized for such an activity. Thus accuracy and correctness of an asset with respect to it's owner is ensured by the this property. Usually, append, delete or edit operations are believed to change the integrity of any asset. Since Cloud based services are accessed by users via web browsers, therefore all the web based attacks are highly prevalent in a Cloud environment that can modify the contents of user files, Databases, Virtual Machine metadata or even WSDL files.

Under the various integrity requirements of the cloud system the following categories have been discussed here:

1) Data Integrity

The Cloud system deals with a good number of data-centric operations with massive data requirements where massive refers to Tera Bytes (TB) and even Peta Bytes (PB) of data. Thus data integrity challenges associated with Data as a Services, Software as a Service, Platform as a Service, etc. needs to be addressed carefully. Some cloud specific data integrity issues are as follows:

Data outsourcing at the CSP end poses an obvious threat on its integrity. CSP could delete some valid tuples related to a client's data and the client would never be able to establish this fact [10].CSP could even send an incomplete data set to the client which would again remain undetected by the client.

SQL injection attack is one of the remarkable web-based attacks that could modify the contents of the Customer databases by exploiting the vulnerabilities of web servers and injecting malicious codes into the system.

Cross scripting attacks are another form of malware injection attacks where hackers could insert malicious scripts (JavaScript, VBScript, ActiveX, HTML, etc.) into vulnerable dynamic web pages such that the malicious code gets executed on the client's browser to get unauthorized access on the users account and compromise the integrity of her data and information.

Metadata Spoofing attack is one of the attacks which modify the contents of the WSDL (Web Service description document) files in order to execute special tasks for which she may not be authorized. This can be of two types- i) WSDL Spoofing: The WSDL file is modified mainly with the intention of tampering with it's parameters. ii) WS Security Policy Spoofing: The WSDL file is manipulated to lessen the security requirements of the intended web service [11]. An example of WSDL Spoofing attack may be cited as follows: An intruder might manipulate a service's WSDL in such a way, that call to a *deleteUser* operation syntactically looks like a call to another operation, e.g. *setAdminRights*. As the modified WSDL document is presented to the user, each of his *deleteUser* operation invocations results in SOAP messages that at the server-side is interpreted as *setAdminRights* operation. At the end, an adversary could manage to create several user logins that were supposed to be deleted by the application's semantics, but in reality still exists, and additionally are provided with administrator level access rights [11]. An example of WS Security Policy Spoofing can be -The information that certain message should been encrypted is removed by the attacker, resulting in an unencrypted communication between web services, enabling the attacker to read the message content.

Wrapping attack is again another common attack for web based services and naturally becomes highly probable for cloud systems. During the translation of SOAP messages at the TLS(Transport Layer service) layer it's content as well as the signature is duplicated and sent to the server as an authentic user. Thus, the adversary is able to interfere in the cloud and run malicious codes to interrupt the usual functioning of the cloud servers [11].

2) Virtualization Integrity

As discussed earlier, the virtualization layer itself induces certain security issues which are not confined within the bounds of confidentiality alone i.e. along with confidentiality the integrity of the Virtual Machines as well as the VMIs needs to be taken care of.

The **CSP administrators** have full access at the backend to the allocated VMs and thus proper security measures should be taken to protect the integrity of the VMs from insider attacks.

Another possible attack in the cloud system is when an intruder launches its own malicious service instance or **virtual machine instanc**e into the Cloud System. Next the adversary tricks the system to treat the instance as a valid one and naturally when a user request is encountered the CSP may forward it to some malicious service instance which when executed contaminates the whole system. Thus the integrity of

the service or VM instances are compromised here and thus should be checked.

VM replication is another important factor which may cause unwanted data leakage if not handled properly. It is therefore suggested that the user properly pauses/temporarily deactivates the virtual machines while replicating to ensure data integrity. Proper policies should be enforced to limit replication of sensitive VMs and control movement of VMs in and out of a managed infrastructure [12].

VM rollback is a phenomenon in Cloud computing that may again introduce certain integrity problems in the VM. Rolling back virtual machines can re-create security vulnerabilities that were fixed or re-enable previously disabled accounts or passwords. VM snapshots need to be maintained for this purpose [12].

As has already been mentioned the process of **VM live migration** needs to be taken care of and preservation of the integrity of the protected contents as well as the maintenance metadata both should be handled by the CSP [12].

The lifecycle of the VMs and their changes in states, need to be analyzed by the CSP as they move through the environment. VMs can be on, off, or suspended. VMs can also be unallocated in storage, with no state associated with them. It is important to constantly assess a VM's vulnerabilities and apply updated security patches to VMs that are off, suspended or unallocated [12].

One of the primary advantages of VMs is that CSP can move them around different datacenters as required, to obtain additional processor or compute resources. But such VMs need **security policies** and baseline histories to move along. When a VM moves, without its security policy, it becomes vulnerable to certain attacks [12].

VM escape and **VM hopping** both have serious impacts on the Cloud security. In the first case the attacker's malware escapes the VM to the host or hypervisor on which the VM is running by exploiting the vulnerabilities in the environment. On the other hand VM hopping implies hopping of the malware's attacker from a VM to another peer VM co-resident on the same host or within the control of a common hypervisor [12].

C. Availabilty

Availability is one of the most important aspects of security that needs to be maintained by a CSP. Different business enterprises who use cloud based services to serve their clients must assure the availability of these services as a slightest downtime can result into a large monetary loss which is irrecoverable. A typical service-level agreement states what the provider has agreed to deliver in terms of availability and response to demand. The service level might, for example, specify that the resources will be available 99.999% of the time and that more resources will be provided dynamically if greater than 80% of any given resource is being used. Both data and VM availability issues have been addressed in the following section:

1) Data/Service Availability

Denial of Service attack in the Cloud system is one of the major causes of service or data unavailability. The attacker generally sends huge amount of vague requests to a certain service. When the Cloud Computing operating system notices the high workload on the flooded service, it starts providing more computational power (more service instances) to handle the additional workload. On one hand CSP is fighting against the attacker (by supplying continuous computational resources) and again on the other hand it can also be said that the CSP is supporting the attacker by letting it exploit it's resources and thus making the intended service unavailable for legitimate users.

Indirect Denial of Service attack is also possible in a Cloud system where other services running with a flooded service on the same server may also become unavailable. Once the server's hardware resources are exhausted after processing the flooding attack requests, the other service instances on the same hardware machine may automatically fail to perform their intended tasks. The side-effect may worsen if the Cloud system notices the lack of availability, and tries to "evacuate" the affected service instances to other servers. This would result in additional workload for those other servers, and thus the flooding attack moves on to other service types, and spreads throughout the whole Cloud System.

Certain **customer penetration testing** could impact other cloud customers i.e. such testing could halt certain services for a specific period of time thus affecting the availability [13].

Disruption of service by **third party WAN providers** could lead to temporary service outages or even certain software bugs could affect multiple copies of cloud data at the same time thus making it unavailable to it's original owners.

Natural disasters like fire, flood etc. in a data center are likely to affect both the primary and redundant copies of data. Therefore availability is once more threatened here and effective measures should be taken to cope up with these situations.

2) Virtualization Availability

As we have already seen, ensuring high availability covers a number of areas that need to be considered, such as network vulnerability, multisite redundancy and storage failure. But since virtualization is one of the most important aspects of the Cloud system, availability in Cloud should be considered after combining the essence of virtualization with it.

One of the most important issues here is of IP failover [14].The need to defend a production-grade IT system or service-application against a failure of any node is not a new issue, and has been addressed in many software products. But these software products are to some extent incompatible with many of the cloud offerings, and most of the public cloud providers generally fail to provide the required functionality. This results into clients being dependent on high availability constructs that exist outside the cloud. Therefore virtual machine instances need to be taken care of against such failure such that the failure of one instance (IP specifically) can be compensated immediately by an alternative instance by some efficient means [14].

The host machine or more specifically the Hypervisor or VMM (e.g. ESX/ESXi host) may fail/crash due to some reason causing all the VMs running on it to fail. Such a situation must be avoided by the CSP by arranging an alternative host machine for all the VMs which were previously running on the failed VMM.

The above stated issues span some of the most critical areas of Cloud security. In the following section some of the proposed works in Cloud security domain have been discussed.

IV. PROPOSED SOLUTIONS OR METHODOLOGIES

Some of the remarkable and beneficial methodologies that have been designed and implemented in order to address the varied security requirements of the Cloud System have been discussed here in a tabular format under the seperate heads of Confidentiality, Integrity, and Availability.

A. Data Confidentiality

The main concerns of data confidentiality in Cloud which have already been discussed in the previous section, implies protection of user data from adversaries and the assurance that CSP remains oblivious to data it is storing and computing. Such confidentiality issues have been confronted using various encryption methodologies that have been presented in Table I.

TABLE I. COMPARISON BETWEEN CLOUD DATA CONFIDENTIALITY SCHEMES

Proposed Scheme	Algorithms used	Required Keys	Type of Encryption used	Complexity	Idea
1.Fully Homomorphic Encryption (FHE)	1.Key generation Algorithm 2.Encryption Algorithm 3.Evaluation Algorithm	$\mathbf{P}_k$= Public key used for encryption of data. $\mathbf{Ev}_k$= Key used for evaluation of circuits $\mathbf{S}_k$= Private key used for data decryption	**Asymmetric Encryption.** 1.Additive Homomorphism~**exponentiation function** 2.Multiplicative Homomorphism~**RSA**[15]	$O(\lambda^{3-5})$ per gate for ciphertext refreshing [15] λ=Security Parameter	Tebbaet.al. (2012) proposed the application of homomorphic encryption [15] in a Cloud based system which would allow clients to encrypt their respective data before storing them at the CSP end and the trick is hidden in the fact that the CSP can carry out necessary computations on the client data without decrypting it. As a result of using homomorphic encryption the confidentiality of client data is thus preserved without affecting the data computation.
2.Searchable Encryption (SE)	1.Data Encryption Algorithm 2.Non-numeric file search Algorithm	**Secret number** $\mathbf{x}_j$, and **coefficients** $\mathbf{c}_{j1}$, $\mathbf{c}_{j2}$in [-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].	Jyun-Yao Huang and I-En Liao (2012) [16] proposed a technique by applying the concept of secret sharing and searchable encryption by which a user could search the encrypted tuples (numeric as well as non-numeric) from cloud databases and file storages without revealing the content to CSP.
3.Onion Encryption (OE)	1.Data Encryption algorithm 2.Query execution Algorithm	Randomized **(RND)** Encryption key, Deterministic, **(DET)** Encryption Key Order Preserving **(OPE)** Encryption Key, Homomorphic **(HOM)** Encryption Key	**1.RND** provides Indistinguisha-bility under an adaptive Chosen-plaintext attack. **2.DET** provides secured execution for queries that involves selection on equality to a given value **3.OPE** provides secured execution for queries that involves selection based on Comparison. **4**.**HOM** is used for executing queries that involves calculation of server side aggregates.	O (T_1.T_2) where T_1 = Time spend for rewriting queries, T_2 = 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%.	Curinoet. Al. (2011) [17] introduced an approach of adjustable security with different layers of encryption (like an onion) protecting each value of a tuple such that SQL queries could be executed on encrypted data, including ordering operations, aggregates, and joins and the query processing is done completely at the CSP side while maintaining the confidentiality of the user data since decryption takes place only at the client side. The only matter of concern here is maintaining different levels of encryption for each column and decrypting each of it to the appropriate level that is required for the requested query.
4.Attribute based encryption for secure scalable	1.Setup algorithm 2.Encryption Algorithm	**PK**- System public key **MK**- System master	1. Hierarchical attribute-based encryption (**HABE**).	User revocation Cost incurred by data owner= 0	The above mentioned approaches protect sensitive user data by using cryptographic techniques but at the same time induce

fine grained access control (ABE)	3.Key generation algorithm 4.Decryption Algorithm 5.Proxy Re-encryption Algorithm	key **S** -Root secret key **PKa**- Initial public key of attribute a **Ska-** Initial secret key of attribute a PK^{T}_{a} Time-based public key of attribute a. $\mathbf{PK_u}$ -User public key $\mathbf{SK_u}$ -User identity secret key (UIK) 9. $\mathbf{SK^{Tu}_{u,a}}$ -Time-based user attribute secret key (UAK)	2. **Proxy re-encryption** (Time based)	Cost incurred by CSP= O(6N), where N is the number of conjunctive clauses in an access structure.	overheads of key distribution and management as well as data management on the Client or data owner when fine grained access control [18] is required. Yu et. al. (2010) introduced a fine-grained access control scheme for cloud environment which at the same time addressed confidentiality of user data, and transferred most of the computational workload involved in the data access control scheme to cloud servers without disclosing the underlying data contents.

TABLE II. COMPARISON BETWEEN CLOUD VIRTUALIZATION CONFIDENTIALITY SCHEMES

Proposed Scheme	Algorithms used	Required Keys	Hypervisor	Agents Involved	Idea
1.TCCP	1. Node Registration Algorithm 2. VM launch Algorithm	i) $EK^{P}_{TC}/N_{=}$ Endorsement private key of TC or N [5] ii)$EK^{P}_{N=}$ Public Endorsement key of N iii) $EK^{P}_{TC=}$ Public Endorsement key of. iv)$TK^{P}_{N}/TK^{P}_{TC=}$ Private trusted keys of Node N and TC v) TK^{P}_{N}/ TK^{P}_{TC} =Public trusted keys of N and TC respectively. vi) K_{VM} = 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) [5] designed a Trusted Cloud Computing Platform (TCCP) with the target of preserving confidential execution of VMs i.e. to prevent CSP (more specifically sysadmins with root privileges) from performing attacks by moving the intended VM to a domain that lies outside the IAAS's security perimeter
2.PALM	1. Migration Data Protection Algorithm 2 Metadata Migration Protection Algorithm	i) 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 [19] iii)Security Guard iv) Migration Manager v) Control VM or Dom0 vi)Hypervisor (part of TCB [19]) vii)Hardware(part of TCB [19])	Zhang et.al.(2008) [19] designed a prototype system called PALM (Protection Aegis for Live Migration of VMs) which ensured security (confidentiality as well as 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[19] for VMM enforced process protection systems [19].
3.TVDc	1. VMM Authorization Algorithm 2. Inter VM-communication 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	IBM Trusted Virtual Datacenter (TVDc) technology in 2008 proposed a methodology which restricted each VM from accessing any other random VM or resource of it's choice, by implementing MAC policy rules throughout the entire Datacenter of the CSP and introducing the concept of workloads [8]. Thus this scheme ensures protection from unwanted data leakage and spreading of malicious software from one workload to another.
4. SSC	1. Create_UDom0 2.Create_Userdomain 3. Create_MTSD 4. Grant_Privilege	i)AIK =vTPM,s [20] public key ii)freshSym= Client Symmetric key	Xen (v3.4.0)	i)TPM [20] ii)vTPM[20] iii)TCB[20] iv)SDom0	Ganapathy V (2015) introduced a Self Service Cloud Computing scheme which tried to solve the issues of uninterrupted CSP access on the contents of client CPU, registers and memory. Attack on Dom0 [20],

	5. Bootstrapping_SSL	iii)SSLpiv= SSL Private Key		v)Domain builder domB vi)UDom0 vii)User Domain UDomU viii) Service Domain SD i.e. the Security Service ix)MTSD for Regulatory Compliance	intervention of malicious Cloud administrators, as well as dependency of client on CSP for enabling or disabling each and every novel service like VM introspection, migration, and check pointing are the main issues that have been highlighted in this work.

TABLE III. COMPARISON BETWEEN CLOUD DATA INTEGRITY SCHEMES

Proposed Scheme	Algorithms used	Keys used	Signature/Encryption scheme used	Complexity	Idea
1.MHT	i) Multi-Join [21] ii) Single-Join[21] iii) Zero-Join[21] iv)Range Condition[21]	No specific keys used. Radix path Identifiers[21] are used.	Tree Signature scheme[21]	Transmission cost is $O(\log_2 n)$ where n= Total no. of data blocks involved(if normal MHT used) Transmission cost is O(n) if RPI based is MHT used.	Niaz M.S, Saake Gin 2015 [21] proposed a Merkle's Signature Scheme for ensuring user data integrity in Cloud storage without the overhead of maintaining a (data+signature) table at the data owner end or the risk of CSP being able to delete some valid tuples or send some incomplete information without the user being able to establish the fact. The scheme could be improvised as pointed out by the author by including support for multi-user environment and NoSQL databases.
2.Privacy-Preserving Public Auditing scheme	i) KeyGen(1^k) ii)SigGen(sk, F) iii)GenProof(F,Φ, chal,pk) iv)VerifyProof(pk, chal,P)	i)k_{prp}= Random permutation key ii) f_{kprf} = Randomly chosen PRF key iii)MAC_{key}= Key used for generating the MAC.	Public key based homomorphic authenticator with random masking [22]	The total communication cost = $O(n/\epsilon)$ [22].With an extra constant time factor R added for guaranteeing privacy preservation.	Wang et. al in 2010 proposed a Privacy-Preserving Public Auditing scheme meant for assuring data integrity/correctness of the Cloud Storage. CSP is considered to be an untrusted/unfaithful party which may hide data losses or even free storage by deleting the blocks that are rarely or are not at all accessed by the client. Therefore, the model provides a suitable data verification methodology to prevent such integrity breaches [22].
3.Public Verifiability and Data Dynamics scheme	i)KeyGen(1^k) ii)SigGen(sk, F) iii)GenProof(F,Φ, chal) iv)VerifyProof(pk, chal, P). v)ExecUpdate(F,Φ, update) vi)VerifyUpdate(pk, $sig_{sk}(H(R))$,update, P_{update})	i)Secret key sk=α.α← Zp [23]. ii)Public key pk=v.v=g^{α}[23]	BLS signature [23].	Verification cost is O(logn). Communication cost is O(logn)	Wanget. al in 2009 proposed a Public Verifiability and Data Dynamics scheme for providing Cloud data storage integrity. The model extends the control of Cloud data integrity verification to the hands of TPA, avails dynamic data operations (Modification, Insertion, Deletion) while maintaining equal degree of integrity check, and Blockless [23] as well as stateless[23] verification. Unlike the previous scheme, the issue of data privacy has not been considered here.
4.Dynamic Provable Data Possession [24]	i)PrepareUpdate(F, info) ii) PerformUpdate (F_{i-1}, M_{i-1}, e(F), e(M)). iii) VerifyUpdate(F, info, M_c, M_c', P_{Mc}') iv) Challenge(n) v)Prove(F_i, M_i, c) vi) Verify(M_c, 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)	Erway et. al. in 2009 proposed a scheme based on the concept of dynamic provable data possession (DPDP) using rank-based authenticated dictionary built over a skip list [24]. This scheme supports data dynamicity along with cloud data integrity verification by the client. Moreover, block-less verification is supported by including the concept of tag, that represents each block b.

TABLE IV. COMPARISON BETWEEN CLOUD VIRTUALIZATION INTEGRITY SCHEMES

Proposed Scheme	Algorithm used	Keys/labels involved	Agents involved	Hypervisor used

SSC	**Create_UDom0**(BACKEND_ID, NONCE,ENC_PARAMS,SIGCLIENT) This algorithm is used by Sdom0 to create client meta-domains.	AIK =vTPM,s [20] public key and private key.	TPM [20], vTPM[20], TCB[20], SDom0, Domain builder domB,UDom0	Xen
MIRAGE	Access Control (VMI, Owner), Image Transformation(VMI, Type of filter), Provenance Tracking(VMI, operation), Image Maintenance(Cloud repository)	No specific keys, but Filters [25] are used in this scheme.	Retriever, publisher, Repository administrator [25]	VMware
PALM [19]	Migration Data Protection Algorithm, Metadata Migration Protection Algorithm (Already explained above)	Private and Public platform key of TPM	Same as Table II	Xen
ACPS[26]	Activity Checking, Activity logging, Checksum/Hash Calculation, Alert Generation, Security Response Generation	No keys used.	Interceptor, Warning recorder, Evaluator, Warning pool, Security management layer, Hasher	KVM

B. Virtualization Confidentiality

Along with Data Confidentiality issues the CSP and Cloud user should also be concerned about the confidential execution of VMs residing in the Cloud platform. Therefore various schemes have been proposed to address such issues, a few of which has be surveyed in Table II.

C. Data Integrity

Protecting the integrity of the client data stored in cloud is another vital part of Cloud security that should be handled by the CSP using proper methodologies. Data auditing is a periodic phenomenon initiated by the data owner to assess the quality, utility and integrity of her data. Downloading the entire or a part of the data from the CSP end and comparing it with the owner copy is quite an infeasible procedure of auditing since it contradicts the concept of cloud storage on a whole. Therefore, various schemes have been proposed for assuring the integrity of Cloud data which has been summarized in Table III.

D. Virtualization Integrity

Virtualization Integrity includes the integrity issues of the entire virtualization layer ranging from Virtual Machine metadata to Hypervisor. Various schemes have been proposed to address such issues, few of which has been noted in Table IV.

E. Data Availbilityy

As already discussed in previous sections one of the main threats affecting Cloud data availability is DDoS attack. Different flavors of DDoS are realized in the Cloud environment.

Kumar M.N (2012) proposed an EDoS (Economic Denial of Sustainability [27]) mitigation service termed as Scrubber Service based on cryptographic puzzles.

Mousa M (2013) [28] introduced a scheme based on Kolmogorov Complexity metrics for detecting DDoS attack in a Cloud environment.

Somani et.al. (2015) [29] introduced a DDoS mitigation scheme using the concept of DDoS Aware Resource Allocation in Cloud (DARAC). Once again this scheme concentrates on EDoS and prevents the consumer's monetary strength from being affected by controlling the auto-scaling features of the Cloud (differentiating a legitimate traffic from a malicious one). The mitigation procedure used here is based on human behavior analysis (No of page requests from a particular source IP in a minute).

F. Virtual Machine Availability

Virtualized methodologies for mitigating DDoS attacks (using intrusion detection sensors) have also been proposed. Besides the availability of the VMs, it-self is a vital concern of Cloud availability. Another aspect of Cloud service availability is "IP failover". IBM SmartCloud enterprise brought forward the concept of virtual IP addresses for ensuring High availability of the Cloud service with respect to IP failover [14].

V. LEAST EXPLORED AREAS OF CLOUD SECURITY

Though, Cloud data location had always been a highly debated issue, no fruitful research has yet been conducted in this field. A client who is storing her valuable data or hosting her applications on the Cloud, remains unaware of it's original location as already discussed in section 3.1.1. Suitable location based access control models are yet to be designed for overcoming such problems. Moreover, ample research for introducing proper access control methodologies suitable for the cross-domain or multi-domain [30] of Cloud is yet to be done. Again mutual trust between the CSP and the Client is another vital issue that is inevitably related to cloud security. Though the works of (Hwang, Li, 2010 [31]) based on Reputation systems (for CSP trust evaluation) and that of (Li-qin Chuang, Yang, 2010 [32]) for user trust evaluation are some of the few in this domain, a rigorous study and research in this area is expected to be done in the near future. Data or service compliance is another complicated issue when it comes to Cloud computing. Since, ultimately the organizations are responsible for the security and privacy of data held by the

CSP on their behalf, proper construction of the SLA policies and following a specific jurisdiction by the CSP becomes neccessary. Lack of collaborative work between the cloud user and the CSP in identifying and reacting to security incidents is another vital area of cloud security that need to be explored in-depth.

VI. CONCLUSION

The paper covers the essential security loop holes as well as security requirements of an existing Cloud system. A generalized view of these issues have been presented here to enhance the importance of understanding the security flaws of the Cloud computing framework and devising suitable countermeasures for them. Finally, various cloud security schemes have been discussed on a comparative framework. On a whole, the paper aims at constructing a proper snapshot of the present scenario and future prospects of Cloud security.

REFERENCES

[1] Buyya R, Yeo C.S. , Venugopal S, Broberg J, and Brandic I.2009. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, 25(6): 599-616, doi:10.1016/j.future.2008.12.001

[2] Mell P.M. and Grance.T. 2011. "The NIST Definition of Cloud Computing." In Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800145.Gaithersburg: National Institute of Standards & Technology.

[3] 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.

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

[5] 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. 6. 20-29. 10.5815/ijcnis.2014.03.03.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] Hashizume K, Rosado D.G, Fernández-Medina E, and Fernandez E.B, "An analysis of security issues for cloud computing", J. Int.Serv. App. pp. 1-13, vol. 4(5), 2013.

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

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

[15] 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).

[16] 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.

[17] 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.

[18] 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.

[19] 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

[20] 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

[21] Niaz M..S, Saake G, "Merkle hash tree based techniques for data integrity of outsourced data", GvD, pp. 66-71, 2015

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] Prangishvili AR, Shonia OT, Rodonaia IR, Rodonaia VA. Formal security modeling in autonomic cloud computing environment. InWSEAS/NAUN International Conferences, Valencia, Spain 2013.

[29] 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

[30] 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

[31] Hwang K, Li D. Trusted cloud computing with secure resources and data coloring. IEEE Internet Computing. 2010 Sep;14(5):14-22.

[32] 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.