Cloud Computing – Threats and Challenges

Article · January 2017

CITATIONS
8

READS
1,062

1 author:

Ishrat Ahmad
Cardiff Metropolitan University
2 PUBLICATIONS **16** CITATIONS

SEE PROFILE

Cloud Computing – Threats and Challenges

I. Ahmad, H. Bakht, U. Mohan

Abstract— Recent advances in cloud technologies have gained much eminence in successfully delivering computing services, but yet to receive much needed attention to offer comprehensive evaluation of the existing security and privacy issues. Due to the distributed and dynamic infrastructure, cloud computing has some inherent limitations that easily affect its security attributes. Preliminary studies have showed most of the organizations are reluctant to migrate their assets into cloud mostly because of the security and privacy concerns. The study is to find out all the possible security threats and challenges along with corresponding compromised security attributes in cloud infrastructure. The study will enable any researchers to develop cumulative knowledge for future research extension and evaluation in cloud computing.

Keywords: cloud computing, cloud challenges, cloud security attributes, cloud threats

1 Introduction

Cloud computing comprises of various technologies. Cloud service providers build large data centers and make available these resources to be shared by different customers. As a result, it complicates the IT systems and network environments [1]. Cloud users outsource their business software and data to cloud service providers for cost savings and greater performances and might not worry regarding the security of their software and data as they are in expert hands [2]. No matter what high degrees of implementation process or reliable measure cloud service providers take, any kind of security problems can happen in cloud infrastructure [1,3,4]. Due to the distributed and dynamic interactions in cloud, it is difficult to understand where the attacks might come from. Problems such as overheating, mis-configuration servers, power outages, hardware failure, packet or data loss, data corruption, bandwidth or network cycles failure, malware threats, botCloud, cyber-attacks, VMs isolation, system holes, security models and standardization, older versions of browsers and interfaces, breaches of data confidentiality, unauthorized access or accidental loss and many more. Typically, cloud computing comprises not only with computing services but also management services as well, such as, self-service, resource metering, quota management, service level monitoring, data replication, backup and recovery. Such level of service abstractions can easily be operated by using simplified interfaces, while at the same time, it contradicts with intrinsic underlying complexities that might influence security and privacy concerns [5], and are not compatible with traditional security models and controls [6].

2 Secutiry Challenges

One of the greatest benefits of using cloud services is that it allows access to unlimited resources. Any attacker with an anonymous registry can use array of cloud servers to crack an encryption key in minutes [7]. The attacker can stage a DDoS attack (distributed denial-of- service) by consuming excessive amounts of finite system resources, such as processor power, memory, disk-space or network bandwidth [8]. Such can result an unbearable system gridlock, services slowdown and leave cloud customers confused and frustrated. Due to the consumption of processing time, the cloud customers are often being charged automatically, as the billing of services are based on the compute cycles and storage space [9]. Compromised cloud instances are misused to execute follow-on attacks like rainbow tables, CAPTCHA control [7] or botCloud, which is command & control by a malicious entity to initiate cybercrimes [10]. In real cases, cloud service providers fail to provide security and privacy for data protection like the way they always claim guarantee to the customers about it [11].

Security has been ranked as a top-ten obstacle for adopting cloud computing [4,12,13,14]. According to a survey on 263 IT executives and CIO's by IDC in 2009, security was the highly cited challenge and rated as the biggest reason for seizing organizations from using cloud services. The survey in figure 1 by IDC is given below [13]:

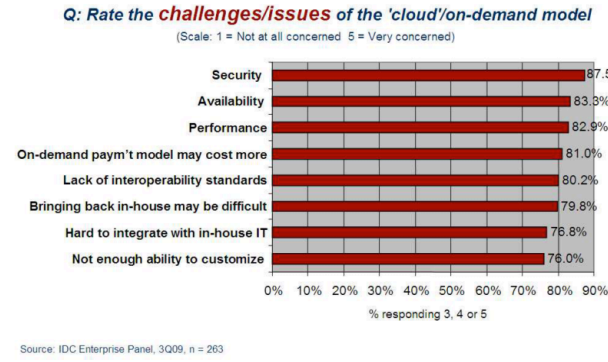

Fig. 1. IDC Survey in 2009 [13]

There are many risks and vulnerabilities to cloud security. Followings are some of the recent cloud service failures listed:

1. arsTechnica: KrebsOnSecurity, security news site, went dark for more than 24 hours because of DDoS attack on routers and security cameras. Again, five days later, more attacks took place over 48 hours causing botnet devices to increase from 6,800 to 15,000 [15].

2. nixCraft: A massive DDoS attack against a cloud-based DNS provider Dyn.com took down major websites: Twitter, Netflix, PayPal, CNN, Pinterest and more [16].
3. Infoworld: DDoS attack against Evernote and made the service standstill for around 10 hours [17].
4. Apple's iCLoud server inaccessible for few hours [18].
5. Infoworld: As Cloud Use Grows, So Will Rate of DDoS Attacks – Arbor Networks, security provider, examined 130 enterprises and network operations professionals. The findings were 76% had to deal with DDoS attack; 43% had partial or total outages due to DDos attack [19].
6. Infoworld: Lack of abuse detection allows cloud instances to be used as botClouds - A study to investigate cloud providers' detection patterns of malicious attacks by using free and infinite cloud resources. The result was cloud providers do not detect attacks launched from their networks [20].
7. CNET: Pirate Bay ditches servers and switches to the cloud [21].
8. InformationWeek: Security breaches at Sony Online Entertainment - more than 100 million users' account were compromised due to cyber-attacks [22].
9. Cloudtweaks: Insider threats to cloud computing [23].

3 Related Work

According to Cloud Security Alliance [24], some of the top threats are: Insecure Interfaces and APIs, Shared Technology Vulnerabilities, Denial of Service/Distributed (DoS/DDoS), Business Discontinuity, Unambiguous Regulatory and Legal Issues, Malicious Insiders or Espionage and Abuse of Cloud services. Doelitzscher et al. [25] analyzed the top security threats based on the publications from regulatory bodies and identified abuse of cloud resources, lack of security monitoring in cloud infrastructure and defective isolation of shared resources as focal points yet to be researched. He argued that after some quick evaluation on the identified threats the regulatory bodies suggest to their audit solutions instead of proposing in-depth compilation of security risks and areas of concern [26]. Islam and Manivannan have extensively classified and characterized various cloud security and privacy challenges in cloud computing [63]. Doelitzscher et al. [25] further emphasized security as a major research area in cloud computing. [Khan and Yasiri have analyzed that most security issues are due to vulnerabilities in virtualization, storage and network [64]. Rick Gordon, managing director at Civitas Group, expressed his concern regarding lack of standard security audit availability, data lock-in and transparency of internal data security procedures provided by cloud service providers [27]. As the cloud customers outsource their business information into a data-centre, they have concern regarding security and privacy of business data and users' interactions. For instance, a hacker can use the virtualization technology to launch new attacks to access data. They have further consented that cloud service providers should preserve data integrity and user privacy [28]. Morsy et al. investigated that existing security threats in terms of cloud architecture, deployment model, cloud characteristics and stakeholders concerns [62]. Lindemann analyzed in her research the existing state of abuse detection and prevention only in IaaS cloud environment. The researcher found that the existing intrusion detection and prevention techniques are in limited use because of high level of control in cloud environment. The researcher proposed possible ways of improving techniques rather than providing finished solutions [60]. According to Alani [61], there is no clearly identified cure to the abuse of cloud service threat, only, the cloud service providers tend to use security software as firewalls, intrusion detection and prevention in order to reduce the risk of attacks. Other challenges are service migration and the continuity of service. Till to date, no regulatory bodies have proposed any agreement on the interfaces standardization of cloud computing. As a result, once customers started using the cloud services and if any problem arises, like Internet problems, power cut-off, service disruption or system bugs, they are most likely to be locked-in and can be negatively affected for the business continuity [29]. If there is no common standard for cloud application development data lock-in took place and forced the developer to depend on the proprietary software environment of PaaS [39]. Okonoboh and Tekkali [1] identified in their research that there is lack of standardization in access controls, data storage, performance metrics and evaluation and hence generates security concerns with possibility of data access or loss. NIST addressed, services from different cloud providers, organization applications developed in cloud, customers' applications running on their devices, all have different plug-ins and extensions for web browsers that are untrustworthy for security [31]. Due to older version of web browsers or operating systems leads to vulnerabilities, as the add-ons do not provide auto updates [12, 39]. Accessing public websites, social media, personal Webmail leverage social engineering attacks, which can impact negatively on customers' underlying platform and cloud services accessed [31]. Cloud service availability is always a concern for both cloud service providers and customers. For example, Salesforce.com was down for about 40 minutes on 6 January 2009; GoogleApps9 and Flexiscale10 reported outages in 2008. The reasons were, range from simple error to lack of new business documentation process and so on [32]. Cloud service providers and customers also encounter problem in analyzing resources utilization, even though there are defined SLAs do exist. They further opinioned in their research that service provider should make ensure that every customer is renowned and that no one would have authentication to access other's information or data.

In spite of remarkable potential benefits that cloud services can provide there are always risks associated with it. According to a fact sheet of Office of the Privacy Commissioner of Canada [33], even though the storing of data in cloud is inexpensive and cloud providers assure that data will not be misused but there is always a tendency of data retention indefinitely, hence increasing the risks of security breaches in cloud computing. For in-

stance, disposed of hard disks without being wiped off data hence misuse of personal information or a permissions bug can make data distorted that cannot be read properly or improperly exposed. Some other potential security risks identified through literature reviews are as the communication between customers and support team is in clear text over Internet, Virtual Machines isolation, Database Administration may leave on disk unintentionally, some employees have access to sensitive data, usage of older version of browsers or operating systems and many more [12, 31, 33]. Storage APIs are proprietary, needs active standardization, leading problem to customers transferring their data from one providers' to another, hence risk of data lock-in, unavailability of services or lack of business continuity also causes data lock-in risks [12]. Another instance, encryption is used to segregate data, but at times, accidents can make data totally irretrievable or can complicate availability [34].

Many studies have been conducted on cloud computing security and privacy issues and were broadly discussed from various perspectives to identify threats and challenges. Several frameworks, models and tools were proposed to mitigate the identified problems. However, most of the proposed works were developed based on the viewpoints of cloud service providers only. Instead, a transparent framework is required to convince potential cloud customers to adopt the services. Furthermore, most of the proposed works were not generalized in terms of either service or deployment model aspects, i.e, a framework is required to cover SaaS, IaaS, PaaS or even public, private or hybrid model aspects. Various regulatory bodies have proposed frameworks, but none has been identified as a global standard that can illustrate a complete overview of how cloud entities work together with a solid ground of trusted infrastructure. A generic audit framework is needed to assess and evaluate overall organizational security objectives which would be acceptable to both cloud users and providers. Followings are some of the related work discussed:

Putri and Mganga [35] suggested a SLA based information security metrics for operating in cloud. However, the research has only considered from the viewpoints of cloud providers, rather than other cloud stakeholders. Besides, the proposed security metrics was not generalized for different service models (IaaS, PaaS, SaaS).

Tariq et al. [36] produced SLA based information security metrics, by using COBIT framework, to evaluate performance of the service object rather than information security risks in cloud computing.

Okonoboh and Tekkali [1] has discussed in their research how attackers found a specialized method, known as Zero-Day exploits, to launch malicious attacks on deployed application in real-time that has security hole. The attacks can be of Zero-day malware, software injection, buffer overrun, scanning worm and more. The researchers have identified threats and vulnerabilities and proposed some real-time mitigation techniques but again the findings were not sufficient to generalize the effect of different service or deployment models. They further argued that due to lack of adequate information pose threats to cloud security, otherwise it will enable to provide the appropriate security for a particular area within a cloud environment. The study suggests to take appropriate measures for security and privacy issues for securing business activities and processes so that organization can focus into development, continuously and effectively with integrity and security in cloud. The contribution of the study was sought for validity in academia and industry by the researchers.

Xiao and Xiao [37] have used attribute-driven methodology to identify security attributes as confidentiality, accountability, integrity, availability and privacy-preservability. The researchers have discussed vulnerabilities that may be exploited by attackers and have drawn threat models with defense strategies.

Hamza and Omar [38] have identified four threats leading from abuse and nefarious use of cloud services. Host Hopping Attacks – exploits resource sharing characteristics of cloud computing. Due to lack of secured isolation mechanism of resources, malicious attackers can hop from one host to another causing severe damage like distorting image and reputation, gaining illegal access to sensitive information or interrupting services. Malicious Insider – System administrators or Information security managers with high privilege roles can use their privileged access to multiple customers' data residing on same physical servers and that can be leaked or sold to other parties of interest. Unfortunately, cloud providers hides such issues due to reputation and customer trust concerns. Identify Theft Attacks – Malicious attackers exploit unlimited resources and set up rogue clouds to attract individuals to host their business data and applications, causing their identity at risk and lead to financial fraud. Service Engine Attacks – Service engines are IaaS platform, used to manage customers' resources, often rented by customers as well. Attackers can abuse this feature by renting VM to hack service engine through other customers' VMs in order to breach and compromise confidential data by breaking the isolation feature that separates customers' data. The authors narrated that cyber criminals are exploiting and misusing cloud computing services due to weak registration process and lack of security controls, and pointed out that extensive research is required to identify the risks and impact of the threat – abuse of cloud services.

Similarly, Hashizume [8] identified in her research that there are security measures being developed to mitigate or stop part of the whole system but no global security analysis were produced for complete cloud computing. She further addressed some security metrics also need to be implemented considering layers of service models.

Bulusu and Sudia [4] argued that security in cloud computing depends completely on cloud service providers as they are responsible for storing data and applications. Even with the strongest security measures, some level of flaws can always be found. Therefore, it is essential to identify security challenges so to improvise and update solutions in order to handle such challenges.

Hsu [40] advised organizations, using cloud services, need to form their own secured governance model within their existing information technology processes.

Marston et al. [41] suggested about initiating IT audit practices in line with local, regional or international policies.

Mell and Grance [5] from NIST have also contended that the operations, such as security policies, robustness of controls, visibility performances and management controls can be ensured by service provider or an organization through auditing or vulnerability testing.

The Cloud Security Alliance (CSA) has acknowledged some critical security and privacy issues in cloud computing, such as, data loss, data breaches, malicious insiders, denial of service, insufficient due diligence, shared technology vulnerabilities, insecure APIs, abuse of cloud services and account hijacking [7]. But according to Alshamaileh [39] and Kazim and Zhu [59], the recommendations provided in CSA guidance are not applicable to all business uses. The researchers addressed that businesses are likely to consider guidelines from the research community if there is anything related to new innovations, like many organizations are concern about the security and privacy issues in cloud computing services [39].

4 Security Attributes

Information security encompasses mainly with four fundamental security attributes, confidentiality, availability, integrity, and accountability. The other identified attributes complement the characteristics of secured information as privacy, non-repudiation, reliability, usability and auditability [1, 12, 35, 37, 42, 43, 44, 45]. People view security challenges in different perspective and so is the security attributes, which depends on individuality, understandability and interpretability [46]. System vulnerability refers to security weakness or hole, which create security threat to system integrity and performance. The vulnerability issues are common fact in a distributed computing environment and has large effects on security attributes in cloud computing. Ensuring system integrity involves proper security and privacy management and access control, correct manipulation of data and information and compliance of audit and standard polices. According to NIST, opportunities of improving information security also benefit privacy. Effective privacy, just as security, can exist upon a sound foundation of organizational, operational and technical implications of information security. Some aspects of privacy are closely related to confidentiality, integrity and availability of security attributes [31]. Different types of security attributes are described as following:

Availability: concerns with the cloud services being operational and accessible from anywhere at anytime required by the business processes. It also concerns with the fact that the services are inaccessible to any unauthorized access [1, 35, 44]. The attribute can be compromised due to technical or non-technical issues as business discontinuity or regulatory actions [12]. Lack of performance on infrastructure level resources allocation can also lead to unavailability of services and weak SLAs [30].

Accountability: concerns with the requirement that the actions of an entity can be traced uniquely to that entity [47]. It refers to the principles that responsibilities for supervision of information system resources are assigned explicitly and that assignees are liable to proper authorities for stewardship of resources under their control [48]. The responsible person actually keeps track of the actions related to information security [35].

Confidentiality: concerns with the sensitive information in a cloud are not being intercepted or accessible to view or read by any unauthorized access [1, 35, 44, 49].

Integrity: concerns with the requirement for protection against either intentional or accidental challenges to violate the property of data (not altered through unauthorized manner) or the quality of a system (performs function in an unimpaired manner) [47]. It ensures accuracy, completeness, validity of data and system for the benefit of business requirements and expectations, and has not been modified by any unauthorized access [1, 35, 44, 49].

Non-repudiation: concerns with the ability to prove the occurrence of a claimed action and its originating entities [49]. To repudiate means to deny. Non-repudiation is to provide assurance that the authorized person cannot deny the authenticity of their performed actions [50].

Security: concerns with the set of characteristics and mechanism that span the information system both logically and physically [47]. It refers to the protection of data or applications from unauthorized access.

Privacy: concerns with the capacity of an individual to access data and applications for unethical activities.

Reliability: concerns with the ability of a system or a component to perform its intended behaviour and results under consistent conditions [49].

Usability: concerns with the ease of use and operability of services to achieve business objectives with effectiveness, efficiency and satisfaction [1, 44].

Auditability: concerns with obtaining audit evidence and evaluating it objectively to determine the extent to meet audit criteria [1, 44, 49].

5 Standard and Regulatory Bodies

The organizational viewpoint towards cloud computing services can vary greatly based on business objectives, asset held, legal obligations, exposure to public, challenges and risks tolerance capabilities. According to Jansen and Grance [31] from NIST, without understanding the context of the organizational infrastructure and the consequences from the possible challenges that it faces, it

is difficult to determine the appropriateness of cloud services from a risk perspective. The authors added that the organizational information technology controls practices that are related to policies, procedures and standards used for application development and service provisioning should be extended to cloud computing environments. Organizations should verify cloud providers' security and privacy assurance claims or certification and compliance review through independent assessment, and must understand their own responsibilities over the computing environment and security implications. They should employ appropriate security management practices and controls over cloud computing solutions. It is important to define service legal agreements (SLA) between cloud service provider and customer initially, otherwise it would be difficult to confer them later [53].

SLA is a written agreement between service providers and customers, stating various issues and responsibilities depend on negotiation between the two parties. It defines what type of service levels a customer should receive, rather than how to achieve them. It represents the understanding of the expected level of services to be delivered and the compensation available at the point of failures of the specified services to the cloud customers [31, 35]. The agreement management involves two phases as contract enforcement and monitoring to ensure compliance in real-time [1].

Due to the growth of data, the policies and procedures for data maintenances keep changing. Typically, policies are obligated by legislation and regulations, such as HIPAA, SOX, NIST or other federal and state compliances. Data is stored on cloud provider's servers that could be installed anywhere across the globe, and hence leading to conflict with various legal issues and requirements during data transferring. For instance, company under U.S. Safe Harbor Program might not satisfy EU legal obligations and making the program ineffective, as data needs to be stored outside of both Europe and U.S. The program also would not work for some certain organizations like financial industries. What works for one organization may not necessarily work for another. Some EU cloud service provides offers to store data on European servers, but this in turn, limits the flexibility and efficiency of cloud computing. The legal and regulatory compliances for data security can be range from strictly enforced to non-existent, some are principle-based or even location wise law-based [53]. According to the authors, no universally adopted security standard is out there but only conflicting laws, regulations and different perceptions of protecting organizational privacy. Same thought has also been shared by Qian et al. [29], no regulatory bodies have reached to an agreement of providing standard external interfaces in cloud computing. Huang and Nicol [46] also observed that, even, a formal process for assessment of cloud services by any other independent third audit parties, acceptable to both cloud providers and customers, does not exist.

Desai [54], a law professor and research counselor at Google Inc., put forwarded that general data protection laws require appropriate technical and organizational security measures to protect data against accidental loss or from illegitimate access. There are different data protection laws, regulatory bodies defining standard and policies, such as, Sarbane-Oxley Act, National Institute of Standards and Technology (NIST) [5], Cloud Security Alliance (CSA) [7], SysAdmin, Audit, Network, Security (SANS) [56], IT Infrastructure Library (ITIL) [57] and more. They are simple and suitable, however they have been developed specially for the US government, which might not be acceptable by researchers from other parts of the world. Some of them are developed only to meet specific system and are not even validated across academia or industry [35, 59].

There are comprehensive security frameworks and leading industry standards/regulatory available for organizations to understand their context, applicability and usability. Most of the identified frameworks have some limitations, such as some were developed to meet specific system, some were only policy-based and designed only for related organizations, some were not globally accepted or have been validated by academia or industry.

6 Threats and Challenges

A "threat" is an act of coercion of a potential attack to elicit negative response. It is generally an effect that can be described as anything that would tamper, destruct or interrupt of any service or item of value [51]. The term "risk" refers to the possibility of being targeted by an attack, getting success and exposed by the attack. The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful [52]. In general, the threats exploit the vulnerabilities of a system, which leads to risk by damaging assets and causing exposure. However, threats can be identified in order to mitigate risks and countermeasure for vulnerabilities.

A list of 26 threats and potential challenges to cloud computing along with prevention techniques and compromised security attributes are presented in Table 1 below:

TABLE 1
List of Threats and Challenges in Cloud Computing

Threat	Abuse of Cloud Services
Description	CSP provides unlimited resources availability hence anonymous registration. Using array of cloud servers, an attacker can crack an encryption key in minutes. Results: malicious coder; spammers; password & key cracking; DDoS; dynamic attack; botnet command & control; rainbow tables; CAPTCHA control.
IPS	IaaS, PaaS
Prevention	Strict in registration & validation processes; fraud monitoring of credit card; introspection of customer network traffic; observing public blacklist for own network; networks based IDS system.
Attributes	Confidentiality, Reputation, Availability
Source	[7], [24], [37], [38], [58], [59], [60]

TABLE 1 CONTINUATION…

Threat	Insecure interfaces & APIs
Description	CSP provides software interfaces or APIs with basic security controls. Customers provision, manage, orchestrate, monitor and even build value-added services using these interfaces. Results: unauthorized access; clear-text authentication; transmission of content; limited monitoring & logging capabilities; API dependencies.
IPS	IaaS, PaaS, SaaS
Prevention	Analyze & enhance security systems of CP interfaces; ensure strong authentication & access controls with encrypted transmissions; recognize the dependency chain relative to API.
Attributes	Confidentiality; Integrity; Accountability; Availability
Source	[7], [24], [35], [58], [59], [60], [64]
Threat	Malicious Insiders/Unauthorized Internal Access
Description	Threats amplify due to the convergence of IT services under a single management domain; General lack of transparency into CSP processes & procedures; less visibility into the hiring standard and practices of cloud employees' lead to adversary. A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information. Results: Espionage; hacker; organized crime; corporate espionage; spoofing; tampering, information disclosure; nation-state sponsored intrusion; Brand damage; financial impact; productivity losses; impact on business continuity, traditional security and disaster recovery;
IPS	Iaas, PaaS, SaaS
Prevention	Customers should understand how the providers detect and defend against malicious attack; Strict supply chain management and assessment; recruitment as legal contracts; transparency into information security & management practices; security breach notification; limiting access only to authorized personnel; auditing on employees;
Attributes	Confidentiality, Integrity, Availability
Source	[7], [24], [35], [59]
Threat	Ambiguous ownership & responsibility
Description	Lack of clear ownership and defined responsibilities for data protection may responsibility result in failure of meeting regulatory and of data legal obligations
IPS	IaaS
Prevention	Detailed in legal agreement.
Attributes	Accountability
Source	[35], [58]

TABLE 1 CONTINUATION…

Threat	Shared Technology Vulnerabilities/Lack of data segregation
Description	A virtualization hypervisors are used to address gap in computing infrastructures that were never designed for strong compartmentalization in a multi-tenant architecture (IaaS), re-deployable platforms (PaaS) or multi-customer applications (SaaS). Results: it exhibits flaws, have inappropriate access controls & influence in underlying platform. Risk of accessing compromising data of other customers.
IPS	Iaas, PaaS, SaaS
Prevention	Implement security practices for configuration or installation; Strong authentication & access control for administrative access & operations; Monitor for unauthorized activity; SLA for remediation; conduct vulnerability scanning & configuration audits.
Attributes	Confidentiality, Integrity, Availability
Source	[7], [24], [35], [58], [64]
Threat	Account or Service hijacking
Description	Theft can be performed by several ways such as social engineering, weak credentials, phishing, fraud, exploitation of software vulnerabilities. Results: Attacker accesses to credentials & passwords and tracks activities and transactions; manipulate data, falsified information & redirect to illegitimate sites.
IPS	IaaS, PaaS, SaaS
Prevention	Avoid sharing of account credentials; Leverage strong two-sided authentication techniques; Multilevel authentication at different levels; Intrusion Detection System; Proactive monitoring to detect unauthorized activity; Understand cloud providers' security policies and SLAs.
Attributes	Confidentiality, Integrity, Availability, Non-repudiation
Source	[7], [8], [24], [59], [64]
Threat	Malware Attacks/Difficult Intruder Detection
Description	Such attack includes rootkit attack, Trojan horses, Cross Site-Scripting (XSS) attacks and viruses. Difficult to detect intruder as the cloud is accessed by multiple users from many different customers using simple devices.
IPS	PaaS, IaaS
Prevention	Security controls; Cloud service operations management; Application security;
Attributes	Confidentiality, Integrity, Availability, Accountability
Source	[35]

TABLE 1 CONTINUATION…

Threat	Data Loss
Description	Due to the number of interactions between known/unknown risks & challenges in the architectural or operational characteristics of CC. Accidental deletion or alteration of records without a backup; Storage on unreliable media; Loss of encoding key by customer; unauthorized access to sensitive data; operational failures; disposal challenges; risk of association; jurisdiction & political issues; data centre reliability; physical catastrophe; disaster recovery; Results: devastating business impact; damage to brand & reputation; impact stakeholders' moral & trust; loss of property; leakage of data lead to compliance violations & legal ramifications.
IPS	Iaas, PaaS, SaaS
Prevention	Sufficient authentication, authorization and audit (AAA) controls; Encrypt & protect data integrity in transit to cloud; Implement strong key generation, storage management & destruction practices; SLA for wipe persistent media before drowning & backup and retention strategies; Auditing; Notification to customers for the occurrences, otherwise data destruction & corruption of personal data are considered forms of data breaches; Backup of data
Attributes	Availability, Non-Repudiation
Source	[7], [12], [24], [35], [37], [58], [59]
Threat	Insufficient Due Diligence
Description	Only cloud beneficial features & functionalities are advertised but no details of internal security procedures, configurations, patching, logging & auditing. Often concern questions (who access, vendor disclose data, logs stored etc) are overlooked and leave customers with an unknown risk profile that may include serious threats. Version of software, code updates, vulnerability profiles, intrusion attempts & security designs are factors to estimate company's security behaviour.
IPS	IaaS, PaaS, SaaS
Prevention	Disclosure of applicable logs & data; Disclosure of infrastructure details; Monitoring & alerting necessary information to customers.
Attributes	Confidentiality, Availability, Integrity
Source	[7], [24], [59]
Threat	Unauthorized Modification
Description	Due to inadequate access control can lead to unauthorised modification of virtual images.
IPS	IaaS
Prevention	Adequate access controls implementation
Attributes	Confidentiality, Integrity, Availability
Source	[35]

TABLE 1 CONTINUATION…

Threat	Denial of Service (Distributed DDoS)
Description	Such attack prevent customers to access their data or application; Consume infinite system resources – processor power, memory, disk space, network bandwidth; Asymmetric application-level DoS does malicious attack using vulnerabilities in web servers, databases or other resources to take out an application. Results: system slowdown; service outages; traffic gridlock; frustrated customers; bill increases for customers as an attacker consume disk space or compute cycles or processing time etc.; network topology identified; access to enough host;
IPS	IaaS, PaaS, SaaS
Prevention	Cloud service operations management; Application security; trace for bandwidth starvation; migration of application to other subnet; check resource consumption; monitor traffic activity; Intrusion Detection System in VMs
Attributes	Availability
Source	[8], [24], [35], [37], [59], [64]
Threat	Data Breaches/ Data Theft
Description	In a multitenant infrastructure, if cloud service database has error in design, a flaw in one client's application will allow an attacker to access not only to that application data but every others' data as well. Offline backups of data to avoid catastrophic data loss will also increase the chance of exposure to data breaches.
IPS	IaaS, PaaS, SaaS
Prevention	Encrypt data to reduce data breach - Loosing encryption key is also loosing data. Implement proper VMs isolation; proper access controls from unauthorized access; risk assessment
Attributes	Confidentiality
Source	[24], [35], [59]
Threat	Cross-VM attacks via side channels
Description	Exploits multi-tenancy nature; VMs co-reside on same physical server; timing side-channels as insidious threat hard to control for massive parallelism and shared infrastructure; no trail or raising alarms of malicious attackers; Results: unauthorized access of data; measure cache to estimate server load; detect keystroke timing to steal passwords; detecting visitors' count to a webpage;
IPS	IaaS, PaaS
Prevention	Physical isolation enforcement; new cache designs; fuzzy time to signal by eliminating fine-grained timers; cryptographic implementation of timing-resistant cache; co-residency detection
Attributes	Confidentiality
Source	[7], [37]

TABLE 1 CONTINUATION…

Threat	Inadequate Authentication & Authorization controls
Description	Threats amplify due to lack of authentication and authorization protection mechanism. Results: hacker; spoofing; tampering, information disclosure; nation-state sponsored intrusion; Brand damage; financial impact; productivity losses;
IPS	Iaas, PaaS, SaaS
Prevention	Customers should understand how the providers detect and defend against malicious attack; transparency into information security & management practices; security breach notification; Enforce required controls.
Attributes	Confidentiality, Integrity, Availability
Source	[35]
Threat	Regulatory & Legal Issues
Description	Customers' data and application are being stored at an unknown or not repudiated cloud providers' that may risk of compromising privacy & confidentiality of data and application; Insecure data storage; SLA violation; dishonest MapReduce; customers' identity disclosure; inaccurate billing of resource consumption; Results: DDoS attack; increase cost; accessing customers' information; lack of computation integrity
IPS	PaaS, SaaS
Prevention	Understand SLAs; Audit to check with SLA; Trust mechanism establishment; Research blacklist of cloud provider; transparency in billing – including I/O time, internal network bandwidth; secure provenance to improve data forensic; policy planning; keep trace of loggings;
Attributes	Confidentiality, Accountability
Source	[37]
Threat	Data Scavenging
Description	Data cannot be deleted completely unless the device is destroyed, which may allow an attacker to recover sensitive data.
IPS	IaaS, PaaS, SaaS
Prevention	Destruction of device after use;
Attributes	Confidentiality
Source	[8], [64]
Threat	Audit Discrepancy
Description	Third party audit difficulty due to accessibility of data centre at distributed geographic locations.
IPS	IaaS, PaaS, SaaS
Prevention	ISO and CSA audit guidelines
Attributes	Availability
Source	[35]

TABLE 1 CONTINUATION…

Threat	Business Continuity
Description	Risk of cloud service provider going out of business; technical/non-technical reasons; Results: data loss; negative publicity;
IPS	SaaS, PaaS
Prevention	Understand Backup & Recovery policies; SLAs agreement; use multiple cloud providers; providers offer specialized techniques for higher reliability at higher price;
Attributes	Availability, Accountability
Source	[12], [35], [58]
Threat	Service Disruption
Description	Disruption of business operations due to break down, unavailability of cloud services, or insufficient resource capacity provided by cloud provider.
IPS	IaaS, PaaS, SaaS
Prevention	Multiple cloud providers accessibility; backup & disaster recovery policies;
Attributes	Availability
Source	[35], [58]
Threat	Phishing Attack/ Social Engineering attack
Description	Phishing/social engineering attacks to cloud provider lead to account or service hacking.
IPS	PaaS, SaaS
Prevention	Proactive monitoring to detect unauthorized activity; Understand cloud providers' security policies and SLAs.
Attributes	Confidentiality
Source	[35]
Threat	Data Leakage
Description	When the data gets into a wrong hand during transferring, storing, manipulating or auditing.
IPS	IaaS, PaaS, SaaS
Prevention	Leverage strong two-sided authentication techniques;
Attributes	Confidentiality, Accountability
Source	[8], [58], [64]
Threat	Data lock-in
Description	Lack of standardization in storage APIs; proprietary; customer cannot retrieve data or programs from one platform to another; Results; Data loss; price increase; providers' business discontinuity;
IPS	PaaS, SaaS
Prevention	Standardized APIs; Compatible software to enable surge or hybrid cloud computing; open-source of proprietary cloud APIs;
Attributes	Availability, Non-Repudiation
Source	[12], [58]

TABLE 1 CONTINUATION …

Threat	Data Inconsistency
Description	Risks of data inconsistency due to inconsistency of interfaces with internal systems. Also caused by dynamic update - insertion, deletion and modification from multiple customers; Administrative errors; Dishonest computation services; Results: Data loss, altered or compromised
IPS	SaaS, PaaS
Prevention	Standardization of application interfaces; Auditing protocol for data integrity; Re-computation or Replications;
Attributes	Integrity
Source	[35], [37], [58]
Threat	Eavesdropping
Description	Access of data during transmission over network.
IPS	SaaS
Prevention	Encrypted data; Application security controls;
Attributes	Confidentiality
Source	[35], [64]
Threat	Identity Theft
Description	Using others identity to access data or application lead to compromise of confidentiality and integrity.
IPS	PaaS, SaaS
Prevention	Implement strong authentication and authorization techniques
Attributes	Confidentiality, Integrity
Source	[35]
Threat	Bug Detection
Description	Cloud providers face difficulty in detecting bugs in cloud environment as it has huge database as well as high number of services and customers
IPS	IaaS, PaaS, SaaS
Prevention	Track bug logs;
Attributes	Availability
Source	[35]

7 CONCLUSION

Cloud computing has several layers of abstraction and technologies, this further complicated the integrity of the systems and attracts one security challenge to other. Each layer of cloud has certain type of vulnerability issues, consequently any weakness in software or hardware causes major challenges in cloud computing. The vulnerabilities issues are very common in a distributed computing environment. In order to overcome such challenges a good measures of security controls is required, which will be globally standard and generalized in terms of every layer of cloud service and deployment models. Security and privacy is still a major concern in cloud computing with various risks and challenges that need much more attention from academia and industry.

REFERENCES

[1] M. A. Okonoboh and S. Tekkali, "Real-Time Software Vulnerabilities in Cloud Computing: Challenges and Mitigation Techniques," Blekinge Institute of Technology, 2011.

[2] G. Anthes, "Security in the cloud," *Commun. ACM*, vol. 53, no. 11, p. 16, Nov. 2010.

[3] X. U. Chun-xiang, H. E. Xiao-hu, and D. Abraha, "Cryptanalysis of Wang's Auditing Protocol for Data Storage Security in Cloud Computing," in *Information Computing and Applications*, 2012.

[4] S. Bulusu and K. Sudia, "A Study on Cloud Computing Security Challenges," Blekinge Institute of Technology, 2012.

[5] P. Mell and T. Grance, "NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[6] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "NIST Cloud Computing Synopsis and Recommendations," *NIST Special Publication 800-146*, 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.

[7] J. Archer, D. Cullinane, N. Puhlman, A. Boehme, P. Kurtz, and J. Reavis, "Cloud Security Alliance Top Threats V1.0," 2010.

[8] K. Hashizume, "A reference architecture for cloud computing and its security applications," Florida Atlantic University, 2013.

[9] C. Hoff, "Cloud Computing Security: From DDoS (Distributed Denial Of Service) to EDoS (Economic Denial of Sustainability)," *Rational Survivability*, 2008. [Online]. Available: http://www.rationalsurvivability.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-service-to-edos-economic-denial-of-sustainability/.

[10] Hayati, "Hayati | Datacentre Management . org," 2012. [Online]. Available: http://www.datacentremanagement.org/tag/hayati/.

[11] H. Takabi, J. B. . Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, 2010. [Online]. Available: http://csis.pace.edu/~marchese/SE765/Paper/security2.pdf.

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A View of Cloud Computing.," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[13] A. Omotunde, O. Awodele, O. Kuyoro, and C. Ajaegbu, "Survey of Cloud Computing Issues at Implementation Level," *CIS J.*, vol. 4, pp. 91–96, 2013.

[14] B. Bertholon, "Towards Integrity and Software Protection in Cloud Computing Platforms," 2013.

[15] D. Goodin, "Record-breaking DDoS reportedly delivered by >145k hacked cameras," *arsTECHNICA*, 2016. [Online]. Available: http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/.

[16] V. Gite, "DDoS attack on Dyn.com," *nixCraft*, Oct-2016.

[17] J. Rapheal, "The worst cloud outages of 2014," *Infoworld*, 2014. [Online]. Available: http://www.infoworld.com/article/2606209/cloud-computing/162288-The-worst-cloud-outages-of-2014-so-far.html.

[18] M. Gurman, "9to5Mac Apple Intelligence," 2014. [Online]. Available: http://9to5mac.com/2014/06/12/app-store-itunes-store-apple-tv-features-currently-facing-server-problems-inaccessible-for-some-users/.

[19] D. Linthicum, "As cloud use grows, so will rate of DDoS attacks," *Infoworld*, 2013. [Online]. Available: http://www.infoworld.com/article/2613310/cloud-security/as-cloud-use-grows--so-will-rate-of-ddos-attacks.html.

[20] L. Constantin, "Study: Lack of abuse detection allows cloud computing instances to be used like botnets," *InforWorld*, 2012. [Online]. Available: http://www.infoworld.com/article/2615764/security/study--

lack-of-abuse-detection-allows-cloud-computing-instances-to-be-used-like-botnets.html.
[21] D. Kerr, "Pirate Bay ditches servers and switches to the cloud," *CNET*, 2012. [Online]. Available: http://www.cnet.com/news/pirate-bay-ditches-servers-and-switches-to-the-cloud/.
[22] M. J. Schwartz, "New Virtualization Vulnerability Allows Escape To Hypervisor Attacks," *Informationweek*, 2012. [Online]. Available: http://www.darkreading.com/risk-management/new-virtualization-vulnerability-allows-escape-to-hypervisor-attacks/d/d-id/1104823?
[23] Walter, "Insider Threats To Cloud Computing," *Cloudtweaks*, 2012. [Online]. Available: http://cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/.
[24] CSA, "Cloud Security Allainace - The Notorious Nine," *Infoworld*, 2013. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
[25] F. Doelitzscher, "Security audit compliance for cloud computing," University of Plymouth, 2014.
[26] N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 1, no. 1, p. 11, 2012.
[27] C. Onwubiko, "Security Issues to Cloud Computing," in *Cloud Computing: Principles, Systems and Applications*, Springer, 2010, pp. 271–288.
[28] M. D. Dikaiakos, G. Pallis, P. Mehra, and A. Vakali, "Distributed Internet Computing for IT and Scientific Research," *IEEE Computer Society*, 2009. [Online]. Available: http://linc.ucy.ac.cy/publications/pdfs/mic2009050010.pdf.
[29] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud Computing : An Overview," pp. 626–631, 2009.
[30] M. Böhm, S. Leimeister, C. Riedl, and H. Krcmar, "Cloud Computing - Outsourcing 2.0," 2009.
[31] W. Jansen and T. Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing," 2011.
[32] S. Gadia, "Cloud Computing : An Auditor's Perspective," *ISACA J.*, vol. 6, pp. 1–5, 2009.
[33] OPC, "Introducing to Cloud Computing," *Office of the Privacy Commissioner of Canada (OPC)*, 2011. [Online]. Available: http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf.
[34] J. Brodkin, "Loss of customer data spurs closure of online storage service 'The Linkup' | Network World," *Networkworld*, 2008. [Online]. Available: http://www.networkworld.com/article/2274737/data-center/loss-of-customer-data-spurs-closure-of-online-storage-service--the-linkup-.html.
[35] N. R. Putri and M. C. Mganga, "Enhancing Information Security in Cloud Computing Services using SLA Based Metrics," Blekinge Institute of Technology, 2011.
[36] M. Tariq, I. Haq, and J. Iqbal, "SLA based Information Security Metrics in Cloud Computing from Cobit framework," *Academia*, 2013.
[37] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 843–859, Jan. 2012.
[38] Y. A. Hamza and M. D. Omar, "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing," *Int. J. Comput. Eng. Res.*, vol. 3, no. 6, pp. 22–27, 2013.
[39] Y. Y. Alshamaileh, "An empirical investigation of factors affecting cloud computing adoption among SMEs in North England," Newcastle University of Business School, 2013.
[40] W. L. Hsu, "Conceptual Framework of Cloud Computing Governance Model – An Education Perspective," *IEEE Technol. Eng. Educ.*, vol. 7, no. 2, pp. 12–16, 2012.
[41] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud Computing - The business perspective," *Decision support systems*, 2011. [Online]. Available: http://www.acc.ncku.edu.tw/chinese/faculty/shulc/courses/IT_Competitive_Advantage/assignments/2012-fall/cloud-computing-business-perspective.pdf
[42] F. Alali and C.-L. Yeh, "Cloud Computing: Overview and Risk Analysis," *J. Inf. Syst.*, vol. 26, no. 2, pp. 13–33, 2012.
[43] J. H. Allen, S. Barnum, R. J. Ellison, G. McGraw, and N. R. Mead, *Software Security Engineering: A Guide for Project Managers*. Peasrson Education, Inc., 2008.
[44] S. Ragi and V. S. K. Maddineni, "Security Techniques for protecting data in Cloud Computing," Blekinge Institute of Technology, 2011.
[45] P. Donadio, "Virtual Intrusion Detection Systems in the Cloud," *Wiley Online Libr.*, vol. 17, no. 3, pp. 113–128, 2012.
[46] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 2, no. 1, p. 9, 2013.
[47] G. Stonebumer, A. Goguen, and A. Feringa, "NIST Risk Management Guide for Information Technology System," 2002.
[48] CIAO, "Practices for Securing Critical Information Assets," 2000.
[49] ISO/IEC 27000, "Information technology — Security techniques — Information security management systems — Overview and vocabulary," *ISO/IEC 27000*, 2014. [Online]. Available: http://www.iso27001security.com/html/27000.html.
[50] M. Rouse, "What is nonrepudiation? - Definition from WhatIs.com," *TechTarget*, 2008. [Online]. Available: http://searchsecurity.techtarget.com/definition/nonrepudiation.
[51] SANS, "An overview of Threat and Risk Assessment," *SANS Institute*, 2002. [Online]. Available: http://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76.
[52] C. Perrin, "Understanding risk, threat, and vulnerability," *TechRepublic*, 2009. [Online]. Available: http://www.techrepublic.com/blog/it-security/understanding-risk-threat-and-vulnerability/.
[53] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy An Enterprise Perspective on Risks and Complaince*. O'Reilly, 2009.
[54] D. Desai, "Beyond location: Data Security in the 21st Century," *Commun. ACM*, vol. 56, no. 1, p. 34, Jan. 2013.
[55] J. Archer, D. Cullinane, N. Puhlman, A. Boehme, P. Kurtz, and J. Reavis, "Cloud Security Alliance - Security Guidance for critical areas of focusing in cloud computing V3.0," 2011.
[56] SANS, "Information Security Resources," *SANS Institute*, 2010. [Online]. Available: http://www.sans.org/information-security/
[57] ITIL, "ITIL Open Guide," *Information Technology Infrastructure Library*, 2010. [Online]. Available: http://www.itlibrary.org/.
[58] K. Lee, "Security Threats in Cloud Computing Environments," *Int. J. Secur. Its Appl.*, vol. 6, no. 4, pp. 25–32, 2012.
[59] M. Kazim and S. Y. Zhu, "A survey on top security threats in cloud computing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 3, pp. 109–113, 2015.
[60] J. Lindemann, "Towards abuse detection and prevention in IaaS cloud computing," *Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015*, pp. 211–217, 2015.
[61] M. M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques," *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, pp. 202–213, 2014.
[62] M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust.*, no. December, p. 7, 2010.
[63] T. Islam and D. Manivannan, "A Classification and Characterization of Security Threats in Cloud Computing," *Int. J. Next-Generation Comput.*, no. March, pp. 1–20, 2016.
[64] N. Khan and A. Al-Yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," *Procedia Comput. Sci.*, vol. 94, pp. 485–490, 2016.

Ishrat Ahmad, PhD candidate at London School of Commerce/Cardiff Metropolitan University, UK. Email: ahmad.ishrat611@yahoo.com

Dr. Humayun Bakht, Director of Studies at Cardiff Metropolitan University/London School of Commerce and Principal Examiner Professional Issues in IT (PITT) at NCC Education. Email: humayunbakht@yahoo.co.uk

Dr. Uma Mohan, Supervisor and Senior Programme Leader at London School of Commerce, UK. Email: uma.mohan@lsclondon.co.uk