ISSN:0975-9646

Survey about Cloud Computing Threats

Raju M[#1], Lanitha B[*2]

PG Scholar, Department of CSE, CMS College of Engineering, Namakkal, Tamilnadu, India[#1]
Assistant Professor, Department of CSE, KGiSL Institute of Technology, Coimbatore, Tamilnadu, India[*2]

***Abstract*— This Paper provides survey of cloud computing threats and serves as an up-to-date threat identification that will help cloud users and providers to make informed decisions about risk mitigation within a cloud strategy.**
***Keywords*— Threats, Risk Analysis, cloud computing.**

I. INTRODUCTION

Cloud computing enables users, through the Internet or other digital networks, to access a scalable and elastic pool of data storage and computing resources, as and when required. Some predict that cloud technology will be among the most significant disruptive technologies over the next two decades, with major implications for markets, economies and societies.

Characteristics	1960 1970 1980	1980 1990 2000	2000 2010 above
	Mainframe computing	Client/server computing	Cloud computing
Technology	Centralized computation & storage; thin clients	Optimized for efficiency because of high cost	High up -front costs for hardware and software
Economic	PCs and servers for distributed computation, storage	Optimized for agility because of the low cost	Perpetual licence for operating system and application software
Business model	Large data centres, ability to scale, commodity hardware, devices	Optimized for agility an order of magnitude better	Ability to pay as you go, and only for what you use

Fig. 1 mainframes to the cloud

Cloud services can also be deployed to users in a variety of ways, the most significant of which are summarized below:

- *Public clouds:* open resources that offer services over a network that is open for public use. Many mass market services widely used by individuals, such as webmail, online storage and social media are public cloud services.
- *Private clouds:* proprietary resources provided for a single organization (for example, a Government or large enterprise), managed and hosted internally or by a third-party.
- *Community clouds:* resources/services provided for and shared between a limited range of clients/ users, managed and hosted internally or by a third-party.
- *Hybrid clouds:* a mix of the deployment models described above, for example, public and private cloud provision.

Three categories of cloud services infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

Fig. 2 service model for cloud computing

Potential advantages include:

- Reduced costs for rented IT hardware and software compared to in-house equipment and IT management;
- Enhanced elasticity of storage/processing capacity as required by demand;
- Greater flexibility and mobility of access to data and services;
- Immediate and cost-free upgrading of software;
- Enhanced reliability/security of data management and services.

Potential risks or disadvantages include:

- Increased costs of communications (to telecommunication operators/Internet service providers (ISPs));
- Increased costs for migration and integration;
- Reduced control over data and applications;
- Data security and privacy concerns;
- Risk of services being inaccessible, for example, due to inadequate ICT or power infrastructure;
- Risk of lock-in (limited interoperability and data portability) with providers in uncompetitive cloud markets.

II. CLOUD SERVICES

a) Infrastructure as a service (IaaS): In this category, the cloud provider's processing, storage, networks and other fundamental computing resources allow the cloud customer to deploy and run software, which can include operating systems and applications. The cloud customer does not manage or control the underlying infrastructure but has control over operating systems, storage and deployed applications, and may have limited control of select networking components (for example, host firewalls). Making use of the elasticity of IaaS for data storage and processing capacity allows an organization or enterprise to access computing infrastructure in a flexible and timely manner.

b) *Platform as a service (PaaS):* In this category, the cloud customers deploy their own applications and data on platform tools, including programming tools, belonging to and managed by the cloud provider. Application developers working on mobile applications commonly use cloud-based

platforms to develop and launch their services. The cloud customer does not manage or control the underlying cloud infrastructure such as network, servers, operating systems, or storage, but has control over the deployed applications and perhaps over configuration settings for the application-hosting environment.

c) Software as a service (SaaS): In this category, the cloud customer takes advantage of software running on the cloud provider's infrastructure rather than on the customer's own hardware. The applications required are accessible from various client devices through either a thin client interface, such as a web browser (web based email), or a program interface. In SaaS services, the customer has no control over the underlying cloud infrastructure, accessing applications through a web browser or separate programme interface. Another formulation of XaaS that might broadly be included in SaaS is CaaS (communications as a service), which includes cloud services for messaging and voiceover Internet protocol (IP).

Traditional IT		IaaS	
User manages	Applications	User manages	Applications
	Data		Data
	Runtime		Runtime
	Middleware		Middleware
	Operating system		Operating system
	Virtualization	Delivered as a service	Virtualization
	Servers		Servers
	Storage		Storage
	Networking		Networking
PaaS		SaaS	
User manages	Applications	Delivered as a service	Applications
	Data		Data
Delivered as a service	Runtime		Runtime
	Middleware		Middleware
	Operating system		Operating system
	Virtualization		Virtualization
	Servers		Servers
	Storage		Storage
	Networking		Networking

Fig. 3 Different computing categories

➢ *Broad network access:* Capabilities can be accessed over the network using standard terminal devices such as PCs, laptops, tablets and smart phones.

➢ *Rapid elasticity:* The capability for rapid scaling, up or down, of the access or services provided in accordance with user requirements.

➢ *Measured service:* The business model that data access or service provided is monitored.

➢ *On-demand self-service.* Based on the principle that users can provision relevant resources as and when required, on their own initiative, without having to negotiate access terms at the time of need.

➢ *Resource pooling.* The resources supplied by a cloud provider serve multiple users rather than being dedicated to a single user, and they are assigned as required by user demand, resulting in them being less costly per unit than they would be if provided for a single user.

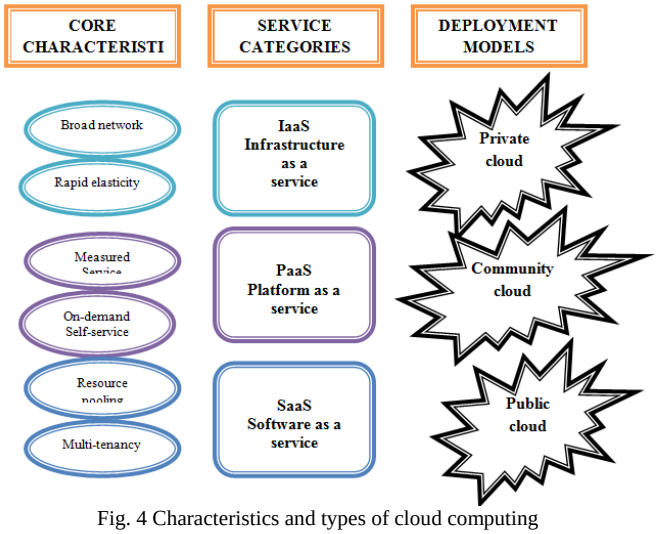

Fig. 4 Characteristics and types of cloud computing

➢ *Multi-tenancy.* Physical and virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from, and inaccessible to one another.

III. THREATS

Cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. A cloud technology exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. Absence of these standards, businesses are vulnerable to security breaches that can quickly erase any gains made by the switch to SaaS. In recent years, Cloud computing released the Security Guidance for Critical Areas in Cloud Computing and the Security as a Service Implementation Guidance.

The threats report reflects the current consensus among experts about the most significant threats to cloud security. While there are many vulnerabilities to cloud security, this report focuses on threats specifically related to the shared, on-demand nature of cloud computing. In this paper, experts identified the following nine critical threats to cloud security.

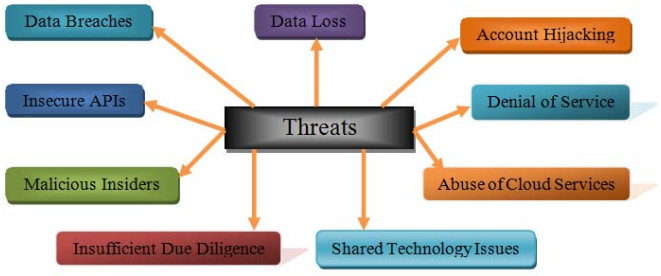

Fig. 5 critical threats in cloud computing

IV. TYPES OF THREAT AND CONTROL

1) *Data Breaches:* Cloud computing introduces significant new avenues of attack [1] [2]. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing how a virtual machine could use side channel timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. However, in many cases an attacker wouldn't even need to go to such lengths. If a multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well.

TABLE I
CONTROLS OF DATA BREACHES

Data Breaches	Controls
Data Governance	Retention Policy Secure Disposal Non-Production Data Information Leakage Risk Assessments
Information Security	Encryption Encryption Key Management
Security Architecture	Production/Non-Production Environments Remote User Multi-Factor Authentication

2) *Data Loss:* Both consumers and businesses, the prospect of permanently losing one's data is terrifying. Attackers broke into Mat's Apple, Gmail and Twitter accounts.

Of course, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customer's data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders [3] [4]. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

TABLE II
CONTROLS OF DATA LOSS

Data Loss	Controls
Data Governance	Retention Policy Risk Assessments
Resiliency	Environmental Risks Equipment Location

3) *Account or Service Traffic Hijacking:* Attack methods such as fraud and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites[5] [6] . Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks. Amazon experienced a Cross-Site Scripting (XSS) bug that allowed attackers to hijack credentials from the site.

TABLE III
CONTROLS OF ACCOUNT OR SERVICE TRAFFIC HIJACKING

Account or Service Traffic Hijacking	Controls
Information Security	User Access Policy User Access Restriction/Authorization User Access Revocation User Access Reviews Incident Management
Security Architecture	User ID Credentials Remote User Multi-Factor Authentication Audit Logging / Intrusion Detection

4) *Insecure Interfaces and APIs:* Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Organizations and third parties often build upon these interfaces to offer value-added services to their customers [7] [8]. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

TABLE IV
CONTROLS OF INSECURE INTERFACES AND APIS

Insecure Interfaces and APIs	Controls
Information Security	User Access Restriction/Authorization
Security Architecture	Data Security/Integrity Application Security

5) *Denial of Service:* Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications [9] [10]. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding .While DDoS attacks tend to generate a lot of fear and media attention, they are by no means the only form of DoS attack [11] [12]. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases, or other cloud resources, allowing a malicious individual to take out an application using a single extremely small attack payload – in some cases less than 100 bytes long.

TABLE V
CONTROLS OF DENIAL OF SERVICE

Denial of Service	Controls
Information Security	Baseline Requirements
Operations Management	Capacity/Resource Planning
Resiliency	Equipment Power Failures
Security Architecture	Application Security

6) *Malicious Insiders:* The risk of malicious insiders has been debated in the security industry [13] [14]. While the level of threat is left to debate, the fact that the insider

threat is a real adversary is not. A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

TABLE VI
CONTROLS OF MALICIOUS INSIDERS

Malicious Insiders	**Controls**
Compliance	Third Party Audits
Data Governance	Ownership / Stewardship Handling / Labeling / Security Policy Information Leakage
Facility Security	User Access Unauthorized Persons Entry Off-Site Authorization
Human Resources Security	Background Screening
Information Security	User Access Restriction / Authorization User Access Reviews Roles / Responsibilities Segregation of Duties Encryption Encryption Key Management Audit Tools Access
Risk Management	Assessments
Security Architecture	Segmentation

7) *Abuse of Cloud Services:* One of cloud computing is greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable [15] [16]. However, not everyone wants to use this power for good. It might take an attacker year to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a DDoS attack, serve malware or distribute pirated software.

TABLE VII
CONTROLS OF ABUSE OF CLOUD SERVICES

Abuse of Cloud Services	**Controls**
Information Security	Incident Response Legal Preparation Acceptable Use

8) *Insufficient Due Diligence :* Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking [17]. Without a complete understanding of the CSP environment, applications or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

TABLE VIII
CONTROLS OF INSUFFICIENT DUE DILIGENCE

Insufficient Due Diligence	**Controls**
Data Governance	Risk Assessments
Information Security	Baseline Requirements Industry Knowledge / Benchmarking
Operations Management	Capacity / Resource Planning
Risk Management	Program Assessments
Resiliency	Management Program Impact Analysis Business Continuity Planning
Security Architecture	Data Security / Integrity Application Security Network Security Segmentation

9) *Shared Technology Vulnerabilities:* Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it is the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models [18] . A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

TABLE IX
CONTROLS OF SHARED TECHNOLOGY VULNERABILITIES

Shared Technology Vulnerabilities	**Controls**
Data Governance	Handling / Labeling / Security Policy
Information Security	Baseline Requirements User Access Policy Segregation of Duties Encryption Vulnerability / Patch Management
Security Architecture	User ID Credentials Segmentation Shared Networks Audit Logging / Intrusion Detection

V. DISCUSSION

a) Data Breaches: Data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other. You may be able to encrypt your data to reduce the impact of a data breach, but if you lose your encryption key, you'll lose your data as well. Conversely, you may decide to keep offline backups of your data to reduce the impact of a catastrophic data loss, but this increases your exposure to data breaches.

b) Data Loss: New data protection rules, data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications. Additionally, many compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the

cloud, loss of that data could the organization's compliance status.

c) *Account Hijacking:* Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach. Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

d) Insecure APIs : Most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

e) Denial of Service: Denial-of-service attack is like being caught in rush-hour traffic gridlock: there is no way to get to your destination, and nothing you can do about it except sit and wait. A consumer, service outages not only frustrate you, but also force you to reconsider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile after all. Since cloud providers often bill clients based on the compute cycles and disk space they consume, there is the possibility that an attacker may not be able to completely knock your service off of the net, but may still cause it to consume so much processing time that it becomes too expensive for you to run and you will be forced to take it down yourself.

f) *Malicious Insiders:* A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information. From IaaS to PaaS and SaaS, the malicious insider has increasing levels of access to more critical systems, and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at great risk here. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

g) Abuse of Cloud Services: This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers.

h) *Insufficient Due Diligence:* An organization adopts cloud technologies subjects itself to a number of issues. Contractual issues arise over obligations on liability, response, or transparency by creating mismatched expectations between the customers. Pushing applications that are dependent on internal network-level security controls to the cloud is dangerous when those controls disappear or do not match the customer is expectation. Unknown operational and architectural issues arise when designers and architects unfamiliar with cloud technologies are designing applications being pushed to the cloud. The bottom line for enterprises and organizations moving to a cloud technology model is that they must have capable resources, and perform extensive internal and CSP due-diligence to understand the risks it assumes by adopting this new technology model.

i) *Shared Technology Issues:* A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it potentially can affect an entire cloud at once.

TABLE X
RISK ANALYSIS FOR THREATS

Threats	**Risk Analysis**
Data Breaches[1][2]	Confidentiality, Information Disclosure
Data Loss[3][4]	Availability, Non-Repudiation, Repudiation, Denial of Service
Account Hijacking[5][6]	Authenticity, Integrity, Confidentiality, Non-repudiation, Availability, Tampering with Data, Repudiation, Information Disclosure, Elevation of Privilege, Spoofing Identity
Insecure APIs[7][8]	Authenticity, Integrity, Confidentiality, Tampering with Data, Repudiation, Information Disclosure, Elevation of Privilege
Denial of Service[9][10][11][12]	Availability, Denial of Service
Malicious Insiders[13][14]	Spoofing, Tampering, Information Disclosure
Abuse of Cloud Services[15][16]	N/A
Insufficient Due Diligence[17]	All
Shared Technology Issues[18]	Information Disclosure, Elevation of Privilege

VI. CONCLUSIONS

Cloud computing threats recognizes that a central component of managing risks in cloud computing is to understand the nature of security threats. The purpose of the Cloud Computing Threats in 2013 report is to provide organizations with an up-to-date, expert-informed understanding of cloud security threats in order to make educated risk-management decisions regarding cloud adoption strategies.

REFERENCES

[1] http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf
[2] http://msdn.microsoft.com/en-us/library/Aa479086
[3] http://news.investors.com/technology/011613-640851-cloud-computing-data-loss-high-in symantec-study.htm
[4] http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/
[5] http://www.theregister.co.uk/2010/04/20/amazon_website_treat/
[6] http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/
[7] http://www.darkreading.com/cloud-security/167901092/security/application security/232900809/insecure-api-implementations-threaten-cloud.html
[8] http://www.darkreading.com/authentication/167901072/security/news/232602844/web-services-single-sign-on-contain-big-flaws.html

[9] http://www.infoworld.com/d/cloud-computing/cloud-use-grows-so-will-rate-of-ddos-attacks-211876
[10] http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/
[11] https://www.owasp.org/index.php/Application_Denial_of_Service
[12] http://security.radware.com/knowledge-center/DDoSPedia/
[13] http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/
[14] http://www.darkreading.com/insider-threat/167801100/security/news/240146276/cloud-s-privileged-identity-gap-intensifies-insider-threats.html
[15] http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf
[16] http://news.cnet.com/8301-1023_3-57534707-93/pirate-bay-ditches-servers-and-switches-to-the-cloud/
[17] http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php
[18] http://www.informationweek.com/security/application-security/new-virtualization-vulnerability-allows/240001996

Raju M is a PG Scholar (ME (CSE)), Department of Computer Science in CMS College of Engineering, Namakkal, Tamilnadu, India. His research areas of interest include Wireless Sensor Networks, and Cloud Computing.

Lanitha B is a Assistant Professor, Department of Computer Science at KGiSL Institute of Technology, Coimbatore, Tamilnadu, India. Her research interest include Digital Image Processing, , Data mining, Wireless Sensor Networks, Cloud Computing and Information Systems.