Chapter

Introductory Chapter: Cloud Computing Security Challenges

Dinesh G. Harkut

1. Introduction

Cloud Computing is currently one of the hottest topics in computing and information technology (IT). The term "Cloud Computing" does not represent a host of new technologies, rather these technologies are combined and effectively upgraded so that they enable new IT services and new business models.

Cloud computing is a technology paradigm that is offering useful services to consumers. Cloud Computing has the long-term potential to change the way information technology is provided and used. The entire cloud ecosystem consists of majorly four different entities which plays vital role to fulfill the requirements of all the stake holders. The role played by each individual depends on their position in the market and their business strategy. These most prominent entities in the cloud ecosystem are:

- **Cloud Service Provider:** it provides cloud services available to cater the needs of different users from different domain by acquiring and managing the computing resources both hardware and software and arranging for networked access to the cloud customers.

- **Cloud Integrator:** the facilitators, one who identify, customize and integrate the cloud services as per the requirement and in accordance with the customers' needs. It plays the important role of matchmaking and negotiating the relationship between the consumer and producer of the services.

- **Cloud Carrier:** it is an intermediary which facilitates the connectivity and takes the cloud services at the doorsteps of end-user by providing access through different network access and devices.

- **Cloud Customer:** the actual user of services extended by the service provider which may be an individuals or organizations which in turn may have their own end-users like employees or other customers.

2. Types of service models

Cloud service providers harness the benefit of huge computing resources span over large geographical area to provide seamless, efficient and reliable services to customers at marginal price. The computing resource deployed over the Internet comprises hardware and application software and OS used in virtualization, storage

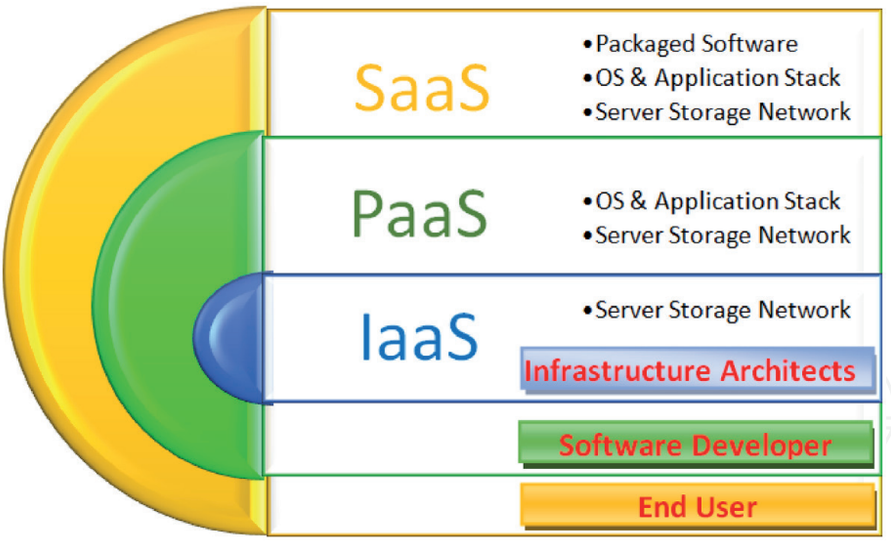

Figure 1.
Cloud service model.

and compute purposes. There are basically three different service models (**Figure 1**) of offering high-volume low-cost services to the end user:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

2.1 Software as a service (SaaS)

In this model, various applications are hosted by a cloud service provider and publicized to the customers over internet, wherein end user can access the software using thin client through web browsers. Here all the software and relevant data are hosted centrally on the cloud server. CRM, Office Suite, Email, Games, Contact Data Management, Financial Accounting, Text Processing etc. are typically falls under this category.

2.2 Platform as a service (PaaS)

A PaaS is typically is a programming platform for developers. This platform facilitates the ecosystem for the programmers/developers to create, test, run and manage the applications. It thus provides the access to the runtime environment for application development and deployment tools. Here developer does not have any access to underlying layers of OS and Hardware, but simply can run and deploy their own applications. Microsoft Azure, Salesforce and Google App Engine are some of the typical examples of PaaS.

2.3 Infrastructure as a service (IaaS)

IaaS facilitates availability of the IT resources such as server, processing power, data storage and networks as an on demand service. Here user of this service can dynamically choose a CPU, memory storage configuration according to needs. A cloud user buys these virtualized and standardized services as and when required.

For example, a cloud customer can rent server time, working memory and data storage and have an operating system run on top with applications of their own choice.

3. Types of deployments

Furthermore, these services can be deployed into Public Clouds, Private Clouds or Hybrid Clouds; each has its own advantages and disadvantages.

3.1 Public cloud

In the Public Cloud delivery mode, all the physical infrastructure are owned by the provider of the services which were provided off-site over the Internet hosted at cloud vendor's premises. Here the customer has no control and limited visibility over where the service is hosted as all these massive hardware installations are distributed throughout the country or across the globe seamlessly. This massive size enables economies of scale that permit maximum scalability to meet varying requirements of different customers and thus provides greatest level of efficiency, maximum reliability through shared resources but with rider cost of added vulnerability.

3.2 Private cloud

In case of Private Cloud mode, entire infrastructure is owned, managed and operated exclusively by the organization or by a third-party vendor or both together and is hosted on the organization premise using virtualization layer. It also facilitates flexibility, scalability, provisioning, automation and monitoring and thus offers the greatest level of control, configurability support, high availability or fault tolerant solutions and advanced security which is missing in public cloud. Basically, very concept of private clouds is driven by concerns around security and keeping assets within the firewall which results it to significantly more expensive with typically modest economies of scale.

3.3 Hybrid cloud

As name suggest, Hybrid Cloud includes a variety of product mix from both Public and Private Cloud options sourced from multiple providers at added cost to keep track of multiple different security platforms by ensuring all aspects of business to communicate with each other seamlessly. In case of Hybrid approach, operational flexibility, scalability, efficiency and security are properly balanced by hosting mission critical applications and sensitive data protected on the Private Cloud and generic application development, big data operations on non-sensitive data and testing on the Public Cloud. Hybrid Cloud thus leverage benefits of both Public and Private Cloud by maintain balance between the efficiency, cost saving, security, privacy, and control.

The combination of the different service and deployment models enables different business models with new business roles. A cloud service is likely to have many layers of abstraction that build on top of each other with define roles and duties. Accessibilities of these predefine services to the end user depends on the different service model. Abstraction layers of standard Cloud model is depicted in adjoining **Figure 2**. Service providers may adapt and compose several services into one, which is then offered to the cloud customers.

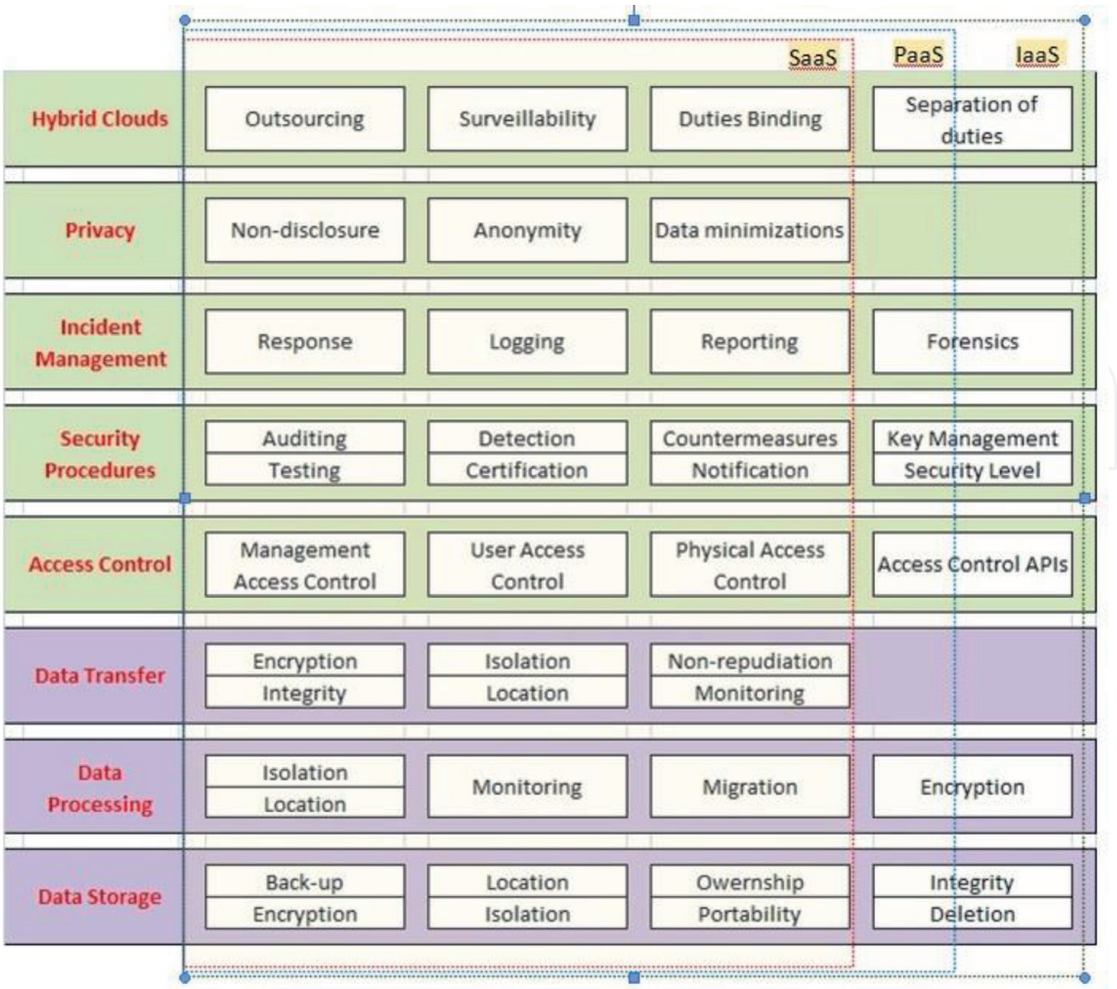

Figure 2.
Abstraction layers of model cloud.

Cloud computing has emerged as a major shift in how computing resources are deployed and consumed both by individuals and enterprises Cloud computing is an approach that covers a wide spectrum of cloud tools and models. This technology has a lot of potential and promises its consumer an enhancement in agility, efficiency and profitability by offering software, platform, and infrastructure delivered as services at very negligible cost by reducing up-front investment and ease of use by providing most user and eco-friendly operations. Like other technology, cloud also offers many benefits which come with some rider cost associated with it. Cloud too has its weaknesses and that is security.

Essentially, security in the cloud environment does not differ from the one in the traditional computing model. In both cases, the major focus is on the issues of protecting data from theft, leakage or deletion. Unlike in traditional computing model, issue of security in the cloud is slightly different. When individual users or organizations move computer systems and data to the cloud, security responsibilities become shared between user and cloud service provider. When an increasing number of individual users and businesses are moving their precious data and entire IT infrastructures to the cloud, it is natural to start wondering how security and privacy are handled in the cloud.

Due to its intrinsic nature, however, the cloud environment highly susceptible to security threats as compared to its counterpart as data is stored with some third-party provider and accessed on the web which increases the overall vulnerability and thus affects overall reliability. Moreover, as most of the precious data is transferred to the cloud, it is difficult to maintain its integrity and thus overall data security is compromised.

Furthermore, with the advancement of technology and passage of time, the entire cloud ecosystem has evolved and instead of relying on single cloud provider for buying/renting a cloud service, individual user or business organizations having freedom and flexibility to exploring more options to select multiple service providers simultaneously for different needs from pool of different cloud service provider and thus eventually leads to more diffuse, seamless integrations of multiple service providers term as fog computing. To make thinks further complicated, data and services may be replicated horizontally among these multiple service providers and as a consequence, it is often extremely difficult to determine the physical location as to where the data is being stored or processed at any one time.

All this constituted the obvious security implications as data is transmitted and stored in different locations over the Internet and shared among multiple service providers simultaneously. Such data is neither within the control of the individual/owner nor the individual service provider specifically in fog environment which is common now a days. Apart from just data, virtualization and applications are equally important security issues in cloud computing. Thus, Security has severe impact on the overall decision making process as to whether an individual or organization will adopt for the cloud services or not.

Though cloud services have ushered in a new age of transmitting and storing data and cloud has its own beneficial power but it is imperative to take focused security approach, reviews the changes needs to undertake before making decision to migrate to the cloud. Some of the key aspects of cloud security in nut shell are depicted in **Figure 3**.

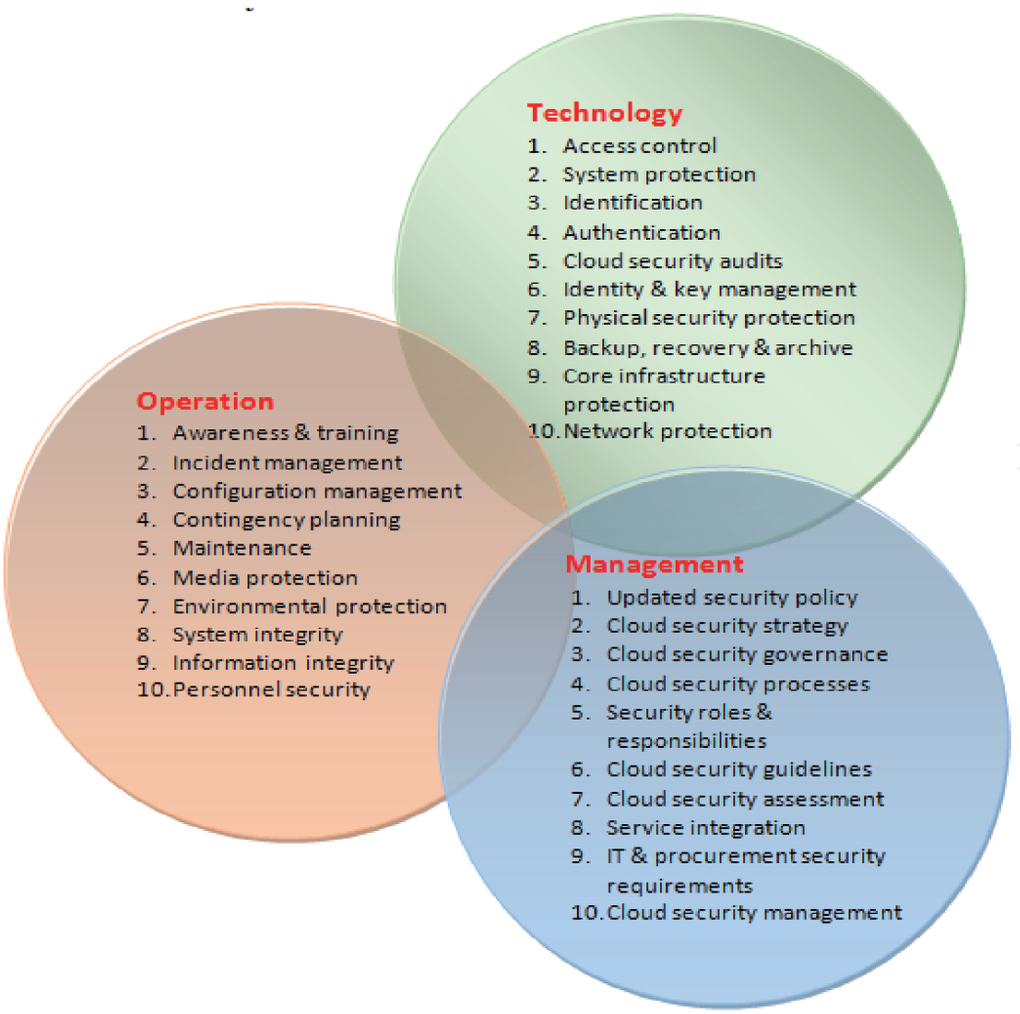

Figure 3.
Aspects of cloud security.

Cloud Security Simplified:

- Access Control
- System Protection
- Personal Security
- Information Integrity
- Cloud Security Management
- Network Protection
- Identity Management

4. Vulnerabilities and threats

Cloud computing being a modern technology offers numerous advantages. In order to harness all these benefits, one has to scrupulously investigate as many cloud security measures as possible. These concerns may vary from vulnerability to malicious code penetration to hijacked accounts to full-scale data breaches. Based on literature searches and analysis efforts, some of the major cloud-unique vulnerabilities and threats were identified which one must consider before making decision to migrate to cloud for opting the services are as follows:

1. Data Breaches/Data Loss
2. Denial of Service Attacks/Malware Injection
3. Hijacking Account
4. Inadequate Change Control and Misconfiguration
5. Insecure Interfaces and Poor APIs implementation
6. Insider Threats
7. Insufficient Credentials and Identity/Compromised accounts
8. Weak control plane/Insufficient Due Diligence
9. Shared Vulnerabilities
10. Nefarious use or Abuse of Cloud Services
11. Lack of cloud security strategy/Regulatory violations
12. Limited cloud usage visibility

4.1 Data breaches/data loss

Cloud computing and services being relatively new and enable accessing remote data via the Internet is the most vulnerable source for misconfiguration or exploitation. This very intrinsic property of cloud becomes unique set of characteristics which make it more vulnerable to all form of data breaches. Data breaches or losses can be any form of cyber security attack in which confidential or sensitive information is stolen, viewed or used by an unauthorized stranger or it may the result out of accidental deletion by service provider or a natural catastrophe, like fire outbreak or earthquake. This may results to the loss of intellectual property (IP) to rivals, impacts the competitive edges, financial losses out of regulatory implications, affecting brand value and goodwill of organization and thus overall market value may be at stake as it foster mistrust from customers and business partners. Though Encryption techniques can protect data but at the cost of system performance. Thus robust and well-tested Data breach avoidance, data loss preventions, data backup and recovery data management strategy must be adopted before making up mind to migrate to cloud.

4.2 Denial of service attacks/malware injection

The basic framework of cloud which offers scalability and speed also becomes nurturing ground for delivering super scalable malware. Cloud applications themselves are great weapon for spreading the malicious attacks on a large scale to cause greater harm like hijacking accounts, breaching data. Malware injections are basically code scripts which are embedded into the basic cloud service modules thus run as legitimate instance having access to all the sensitive resources and thus intruder can eavesdrop, compromise the overall integrity of vital information. Denial of Service attack (DoS) makes valuable services unavailable to the legitimate user thus hamper the overall performance and security. DoS may act as catalyst and used as smokescreen to hide the malicious activities bypassing the firewall of cloud and thus can spread easily to cause greater harm instead of infecting one device.

4.3 Hijacking account

The recent growth and easy adaption of cloud services by organization leads to altogether new set of issues related to hijacking account. Imposter now can easily exploit the ability to gain access to login credentials and thus the sensitive data comprises of business logic, functions, data and applications stored on the remote cloud. Account hijacking which includes scripting bugs, reused password, cross-site scripting enables the intruder to falsify and manipulate information. Man-In-Cloud Attack, Key-logging, Phishing, and buffer overflow are some other similar threats which eventually leads to theft of user token which cloud platform uses to verify each individuals without requiring login credentials typically during data updation or sync. The impact of the account hijacking can be severe, some even leads to significant disruption of business operations by means of complete eliminations of assets and capabilities. Thus account hijacking needs to be dealt seriously as tangible and intangible impact out of leakage of sensitive and personal data may damage the reputation and band value.

4.4 Inadequate change control and misconfiguration

Volume and scope of the various resources used in cloud environment augmented with complexity and dynamism of resources poses major challenge in configuring effectively for efficient use. Inappropriately configure precious computing

resources, results in making these resources soft target for vulnerable malicious undesired activities and thus entire cloud repositories may exposed to intruders. The overall business impact depends on the nature of the misconfiguration, and how quickly it has been detected and resolved. Excessive undesirable permission, unrestricted access to ports and services, unsecured data storage, unchanged default credentials & configuration settings, disabling standard security controls, logging & monitoring are some typical issues related with misconfiguration which must be dealt with utmost care by continuously scanning for misconfigured resources in real time as traditional change control and configuration management technique becomes ineffective in cloud environment.

4.5 Insecure interfaces and poor APIs implementation

Application Programming Interfaces (APIs) as name suggests is an interface between the system and outside un-trusted entities most exposed parts of a system accessible via the Internet, facilitates users to customize their cloud experience and also indirectly provide the safe conduit or entry points for strangers. A poorly designed weak set of interfaces exposes organizations precious sensitive resources to various security issues related to confidentiality, integrity, availability, and accountability. Apart from giving programmers the tools to build and integrate their applications with other job-critical software, API also serves to authenticate, provide access, and effect encryption. The cloud assets can be compromised if the vulnerability of an API which lies in the communication that takes place between applications is exploited. Thus standard and open API frameworks must be referred while designing the interfaces which may help to protect against both accidental and malicious attempts to circumvent security.

4.6 Insider threats

The human intervention in data security has many faces and many sources. The insider human element may be from any hierarchy; both service provider and client organizations can abuse their authorized access to the organization's or cloud provider's networks, systems, and data as they are uniquely positioned to cause damage without even breaking the firewalls and other security defense mechanism. The human element of data security has many faces and being authorized and operated on a trusted level, these insiders may misuse information or perform nefarious activities through malicious intent, accidents, carelessness or malware. Various measures to mitigate the consequences of insider threats includes routine audits of on-offsite servers, frequent change in passwords, confined privileged access to security systems and central servers to limited numbers of employees apart from controlling access and offering business partnerships to the employees. Prevention is better than cure; dealing with such category of threat would become more expensive and complex as it involves containments, forensic investigation, escalation, surveillance and monitoring.

4.7 Insufficient credentials and identity/compromised accounts

Inadequate credential, identity or key management may leads to unauthorized access to data and information. As a result, malicious intruders camouflaged as genuine users can manipulate the sensitive data. If the impostor manages to gain access to cloud user's credentials, it can target the entire resource s of cloud along with the user organization's assets and even influence the organization's administrative user as well. Other tenants of the same cloud are also at high risk to security

incidences and breaches. An Automated regular rotation of cryptographic keys and passwords, removal of unused credentials, implementation of proper scalable central programmatic credential management system, and use of multifactor authentication process are some of the measures which must be undertaken by the cloud provider to deviate the risk of data breaches. Moreover, due diligence should be taken to ensure that third parties to whom cloud provider may have outsources operations or maintenance work satisfy the requirements of security as contracted by cloud service provider because it indirectly levitate the threats and compromised the overall security. Strictest credential access, multifactor authentication, segregated and segmented accounts are some of the suggested measures one should opt for to mitigate the risk.

4.8 Weak control plane/insufficient due diligence

Non-standard data formats, non-standard APIs, and excessive reliance on loud provider's proprietary tools make it difficult and expensive affaires to migrate from one vendor to other. This may results in either cloud provider will start exploiting or in case if for some reason cloud provider ceases its operation and goes out of business, moving data to other in timely manners becomes hectic and eventually may result in loss of data too. Thus to avoid such grim situation of Vendor lock-in, adequate control plan and due diligence should be in place before making decision migrating to any cloud. Any hasty decision without anticipating the quality and nature of services from cloud provider may pose security risk, especially when the desired services are bound and control under legal and statutory obligations or services hired for handling highly sensitive or personal or financial data. Cloud service user must perform due diligence and ensure that proposed cloud service provider possesses an adequately strong control plane in place; absence of this could results in data loss, either by theft or corruption. Apart from technical issues discussed above, one equally important parameter which must be given due weightage in decision making process is people factor. If a person in charge is unable to exercise full control over data security, infrastructure and verification, then security, integrity and stability of data may be stake.

4.9 Shared vulnerabilities

Multi-tenancy feature of cloud makes cloud services cost effective for individual organization but incidentally it leads to yet another security issue. Exploitation of system and software vulnerabilities within cloud infrastructure, services results into failure to maintain physical and logical separation among different tenants in multi-tenant environment. This failure to maintain separation can further be exploited by intruders to gain un-authorized access from one tenant's resource to others. Such attacks can be accomplished by exploiting the vulnerabilities of either cloud provider or any of the tenants whose security is more vulnerable. This may results in increasing the attack surface, leading to an increased chance of data leakage. Moreover, the cloud security by default is a shared responsibility of both cloud service provider and client organization, so proper understanding is imperative to implements effective security. Failure to achieve this seamless integration for security implementation can result in data and resources being compromised.

4.10 Nefarious use or abuse of cloud services

Intruders by exploiting the vulnerabilities of cloud computing resources may target user's cloud provider's resources to host malware activities. Intruder either may launching DoS attacks and thus makes services unavailable to legitimate

users or these resources can be used for some illegitimate use for illicit purpose like mining crypto-currency, automated click trailing, brute-force attacks for security breach by intruders and while the customer foots the bill. The bill could be substantially high as activities like mining requires huge resources. Attackers may use the clouds exceptional storage capacity to store and propagate malware and illicit activities like sharing of pirated software, books, videos or music and invites legal consequences in intellectual copyright fines and settlements which can be even more cost prohibitive. Furthermore, complexity of cloud service implementation aids intruders to hide and remain undercover for prolonged period of time and such unnoticed threats, risks and vulnerabilities poses more challenges for legitimate service provider and user. To restrain the nefarious use and abuse of cloud services and mitigate the risks posed by cloud service usage one must have to procuring security technology for actively monitoring cloud infrastructure usage and devise proper security guidelines which define what are the legitimate and appropriate behavior and what leads to abuses and methods of detecting such behaviors.

4.11 Lack of cloud security strategy/regulatory violations

It is imperative to formulate a strong cloud security strategy, regulations and risk management policy should be devise before making mind to migrating to cloud provider for various services instead of simply lift and shift without any due diligence. Mostly many organizations are bound by and force to comply with certain rules, regulations and law of land of origin and these compliances should be center point for overall security policy. Sensitive health data, private student data, personal financial data, proprietary intellectual property data, research data and confidential business logics constitutes different category of data which are typically migrated to cloud for various services and mostly protections of these data are cover under respective apex authorities or commission and infringement of any kind will invite the formidable fine and penalties. Security architectures and framework must be aligns with the underlying business goals and objectives. Cloud provider being third party, upon agreeing to provide the services, also become liable for extending the appropriate security measures as weak security can lead to financial loss, reputational damage, legal repercussions, and fines.

4.12 Limited cloud usage visibility

The moment organization decides to migrate the assets and operation to the cloud, it starts losing the overall visibility and control over those assets. The ability to decide, visualize and analyze whether the services offered by clouds are safe or malicious, decides the degree of visibility of cloud usage. Even though organizations are hiring the services of cloud provider, still it is imperative on their part to perform analysis and run time monitoring. To enhance the cloud visibility and thus mitigate the risk, it is crucial to develop comprehensive solution that brings people, process and technology at one common place and elucidate accepted cloud usage policies to each and every stack holder. Otherwise lack of awareness about organizations governance controls and policies may results in placing sensitive data in public access and compromising the cloud containers by inappropriate setup of cloud services. Thus lack of governance, lack of security and lack of awareness leads to catastrophic risk. Installing firewall, implementing organization wide zero-trust model, run time analysis of outbound activities and keeping track of anomalies are some of the measures which will be helpful in restraining the suspicious behaviors and mitigating the overall risk.

5. Conclusion

Cloud is new buzzword and evolving at a phenomenal speed, even in the context of the fast-moving IT sector and becoming increasingly in demand around the world. As it evolves, lack of faith in the security features imparted by cloud is cited as main barriers and concerns which discourage users putting their confidential data into this faceless nebulous and intangible entity known as the cloud. Information security and data protection are the two main concerns which stand in the way of a wider deployment and acceptance of cloud. Over a passage of time, most powerful security standards are emerging and constantly evolving aiming to overcome many of these challenges. Clearly, there are both challenges and opportunities with the cloud and due to the economics of scale, a cloud provider are opting for a dedicated team of security specialists and cloud data centers have physical protection on par with military installations thus able to provide vastly better security procedures, physical protection than any small or medium-sized enterprise. In summary, as with each new technology, Cloud is a double-edge sword and clearly there are both challenges and opportunities with the cloud.

Author details

Dinesh G. Harkut
Prof. Ram Meghe College of Engineering and Management, Sant Gadge Baba Amravati University, India

*Address all correspondence to: dg.harkut@gmail.com