Cloud Implementation Security Challenges

Mervat Bamiah, Sarfraz Brohi, Suriayati Chuprat
Universiti Teknologi Malaysia, Malaysia
abmervat3@live.utm.my
nbsarfraz2@live.utm.my, suria@ic.utm.my

Muhammad Nawaz Brohi
Preston University Ajman, UAE
mnbrohi@preston.ae

***Abstract*- Cloud computing offers significant features such as resource pooling, scalability, on-demand self service, availability, and reliability to organizations to improve their quality of services. For example by using cloud computing services in healthcare it is possible to reach large population of people in isolated geographical areas which will assist in saving their lives in critical situations. It enables the use of latest technologies through its various service delivery and deployment models via the internet on pay-per-use billing pattern. However, cloud computing has dark side when it comes to security and privacy considerations. Critical industries such as healthcare and banking are reluctant to trust cloud computing due to the fear of losing their sensitive data, as it resides on the cloud with no knowledge of data location and lack of transparency of Cloud Service Providers (CSPs) mechanisms used to secure their data and applications which have created a barrier against adopting this agile computing paradigm. This paper addresses cloud computing security concerns that must be considered in order to adopt cloud services in information critical industries.**

Keywords— Cloud Computing, Healthcare, Security Challenges

I. INTRODUCTION

Cloud computing evolved as a new IT paradigm to provide an agile method to deliver real time scalable services to industries, organizations and individuals in cost effective way. It is a business model that has inherited the benefit of other technologies such as distributed, pervasive, ubiquitous, utility computing and virtualization [1-2]. In-spite of the unique features of cloud computing, still there are several challenges regarding to its dynamicity and multi-tenancy that requires significant isolation between its computing resources, beside implementing strong security and privacy techniques. These challenges are shown in Fig.1 which will be discussed in section-II.

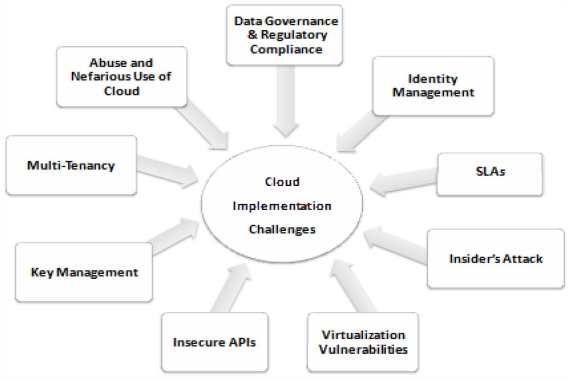

Figure1. Cloud Computing Implementation Challenges

II. CLOUD SECURITY CHALLENGES

Several security challenges should be addressed in cloud computing before adopting it in information critical industries. These challenges are described as follows:

A. Insecure Applications Programming Interfaces (APIs)

Cloud services are accessed and managed by clients via software interface and APIs. These APIs have significant roles in provisioning, monitoring, orchestration and management of the processes running in a cloud computing environment. The security and availability of cloud services depends on security of APIs so they must include features such as encryption, activity monitoring, and authentication as well as access control mechanisms [3]. Insecure cloud computing software services interfaces and APIs may lead to major security concerns for both CSPs and clients. APIs should be designed to protect against both accidental and malicious attacks. Some of the security concerns include cyber attacks and illegitimate control over user accounts. Hackers and unauthorized users always find new ways into networks that may result in data breaches which can damage businesses that operates from the cloud. CSPs have to enhance their security by encryption, abstraction, and encapsulation mechanisms [3]. Attackers also are targeting the digital keys used to secure the internet infrastructure. The unique codes (API keys) are used by cloud services to identify third-party applications that are using them. These keys can be attacked which may cause Denial-of-Service (DoS) or rack up fees on behalf of the victim. An improper implementation that allows simple access to an API via a secret key may facilitate the attackers to have absolute access if the secret key can be sniffed out or stolen from an authorized user's electronic device, which will have vital impact on the client's data. There is a need to protect these cloud API keys with best practices in a secure manner.

B. Virtualization Vulnerabilities

On a cloud infrastructure virtualization is achieved by using a hypervisor or Virtual Machine Monitor (VMM) that allows multiple Virtual Machines (VMs) to run on a single host OS or directly on the underlying hardware concurrently to facilitate sharing of cloud resources. Associating multiple servers with one host removes the physical separation between servers, increasing the threats of malicious attacks on VMs and root to access the hypervisor. By exploiting this vulnerability, an attacker can gain access and target numerous areas of a virtualized cloud infrastructure e.g. hypervisor, hardware, guest OSs and the applications within individual VMs [4]. Some threats such as VM escape, system configuration drift,

insider threats and root kits might take place due to use of vulnerable access control mechanisms [5]. This requires deploying strong security isolation mechanisms to eliminate the threats by modifying the hypervisor directly access, or installing a rootkit on virtualization host, in addition to the probability of targeting the virtualization management system.

C. Key Management

There are several key management challenges within the cloud environment such as: Key stores that must be protected in storage, in transit, and in backup. Improper key storage may lead to the compromise of all encrypted data. Accesses to key stores have to be limited to the authorized personnel who require the individual keys. These keys ought to be under policies governing them. They should not be with the same person who is given the keys and who is storing them since loss of keys means loss of data which keys are protecting [6]. Several possible threats can occur in 1) Communication channels between CSP and end users during cloud migration and other business communications between CSP-to-CSP. 2) Storage areas of clients' data. 3) Hypervisors and VMs. Vulnerable area to threats should be securely protected and isolated by the use of appropriate up-to-date cryptography systems with efficient key management to secure clients' data and their applications on the cloud [4].

D. Data Governance and Regulatory Compliance

Clients are responsible for their data and applications even if it resides on third party storage such as cloud [7]. There should be shared data security terms and conditions included in Service Level Agreements (SLAs) initiated between CSPs and clients based on their data sensitivity. Cloud computing must be under well developed information security governance processes, as part of the client's overall corporate governance obligations with due care in terms of scalability, availability, measurability, sustainability and cost effectiveness. Since cloud physical storages are widely distributed across multiple jurisdictions that have different laws regarding to data security, privacy, usage and intellectual property. CSPs are responsible for incorporating the corresponding regulatory compliance with government and legal country specific policies when deploying clients' data and applications [4]. CSPs ought to satisfy privacy rules by using up-to-date security techniques such as encrypting clients' data and documents on the fly, and on the cloud with the use of strong techniques (e.g. 256 bit AES algorithms) as well as using firewalls to restrict the traffic to each cloud instance by source IP address. In addition to allowing the access to clients data through Secure Socket Layer (SSL) encrypted endpoints. Furthermore, providing a disaster recovery mechanism that starts quickly in case of a server failure and developing an authorization model to provide discretionary, role-based and context-aware authorizations to prevent any unauthorized access [8].

E. Service Level Agreements (SLAs)

SLAs refer to a legal contract that describes the minimum performance criteria CSPs promises to meet while delivering the required service(s) to their client(s). It defines the responsibilities of the related parties and sets out the remedial action plus any consequences that will take effect if performance falls below the promised standards [9]. Lack of trust by clients will create a barrier against adopting cloud computing paradigm. This lack of clients trust may occur as a result of SLAs not offering a commitment to allow cloud users to audit their data. The loss of data governance causes concerns when user's sensitive data and mission-critical applications move to a cloud computing environment where providers cannot guarantee the effectiveness of their security and privacy controls [10]. Clients must understand their security requirements, what control and federation patterns are necessary to meet those requirements in order to protect their rights and themselves against critical business security threats, besides holding CSP responsible for service failure and their confidential data loss.

F. Multi-Tenancy

In cloud environment, multi-tenancy means clients can share infrastructure and databases in order to take advantage of cost and performance that comes with economies of scale. Sharing IT resources may encounter threats of data loss, misuse, or privacy violation. Ensuring security by means of integrity, availability, confidentiality and non-repudiation is a must in cloud computing environment where the clients' data are under the control of CSP in multi–tenant shared environment [11]. Security must be considered in all aspects of cloud infrastructure as shown in Fig. 2 [12] below.

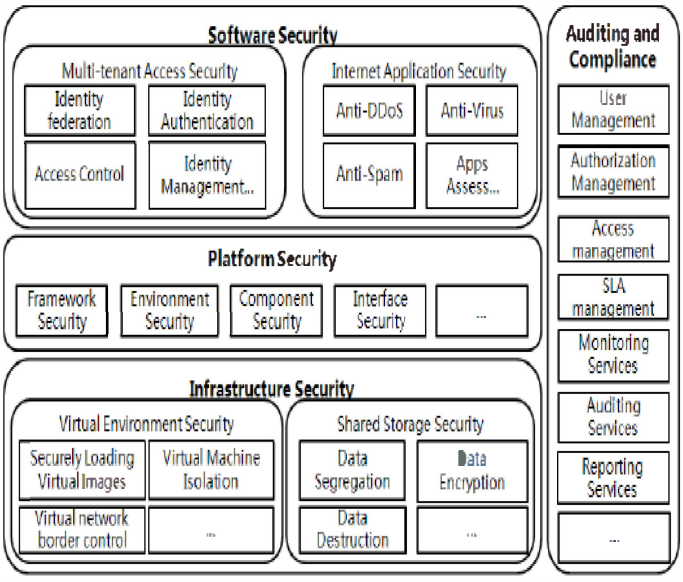

Figure 2. Cloud Computing Security Architecture [12]

Table 1 [13] illustrates the security requirements that should be considered to eliminate the threats and create clients trust in all cloud service layers as follows:

TABLE.1 User's Specific Security Requirements [13]

Level	Service Level	Users	Security Requirements	Threats
Application Level	Software as a Service (SaaS)	End users	•Privacy in multi-Tenant Environment • Data protection from exposure •Accesscontrol •Communication protection •Software security •Service availability	•Interception •Modification of data at rest and in transit •Data interruption (deletion) •Privacy breach •Impersonation •Session hijacking •Exposure in network
Virtual Level	Platform as a Service (PaaS) Infrastructure as a Service (IaaS)	Developers	•Accesscontrol •Application security •Datasecurity •Cloud management control security •Secure images • Session hijacking • Virtual cloud protection • Communication security	•Programmingflaws •Software modification •Software interruption (deletion) •Impersonation •Traffic flow analysis • Exposure in network • Defacement • Connection flooding • DDOS • Impersonation • Disrupting communications
Physical Level	Data Center	Owners of the infrastructure	•Legal use of cloud computing • Hardware security • Hardware reliability • Network protection • Network resources protection	• Network attacks • Connection flooding • DDOS • Hardware interruption • Hardware theft • Hardware modification • Misuse of infrastructure • Natural disasters

Privacy, on the other hand varies from country to country in terms of cultures and jurisdictions. It is about compliance with applicable data protection laws and regulations relating to data transfer or location, as well as the purpose of processing and subject rights of data access and control. The challenge is how to protect the privacy while sharing the personal data [12]. When addressing privacy in the cloud, two aspects must be distinguished: 1) applications running in the cloud should protect the privacy of the data they process; 2) CSPs should protect clients' data that is stored or processed on their infrastructure [14]. In cloud computing environment usually clients can access, use, store and deliver their data across the globe via Internet. However, they do not control their data since it resides on the cloud, there is a strong possibility that clients and their competitors data can reside on the same physical storage device with logical segregation which can result in one client's private data can be viewed by other users. This can create an issue of data theft. In addition, the data being on a multi-tenant model raise the concerns of the security an auditing mechanisms applied by the CSP that should ensure proper data isolation for protecting data from threats or external penetrations, also preventing unwanted changes by the CSP or any unauthorized access or attacks. This isolation of data, and maintaining proper compliance and SLAs is a must in cloud computing environment [4]. Strong security and privacy mechanisms should be applied to gain clients confidence of cloud paradigm.

G. *Insider's Attack*

According to The CERT Insider Threat Center [15], a malicious insider refers to "current or former employee, contractor or other business partner who has or had authorized access to an organizations network, system or data and intentionally exceeded or misused that access in a manner that negatively affected confidentiality, integrity, and availability of the organizations information or information systems". According to International Data Corporation (IDC) survey which posed 440 organizations to specifically address the insider threat, stated that organizations are increasingly aware that stronger application identity controls are necessary to meet data security challenges by strong authentication, data monitoring, and advanced access control technologies against insider attacks [11]. There are several types of malicious insiders identified by [16] such as rogue cloud provider administrator, or an unauthorized access by an employee in a specific organization who exploits cloud weaknesses, and the insider who uses cloud resources to carry out attacks against the organization's local IT infrastructure. The risk of a malicious insider is high since CSPs control the clients' data, and there is lack of transparency in the way processes and procedures are done (how CSPs grant their employees access to physical and virtual assets, and how they monitors these employees, or how they analyzes and reports on policy compliance)[10]. Fig.3 [16] describes the threats by various malicious insiders.

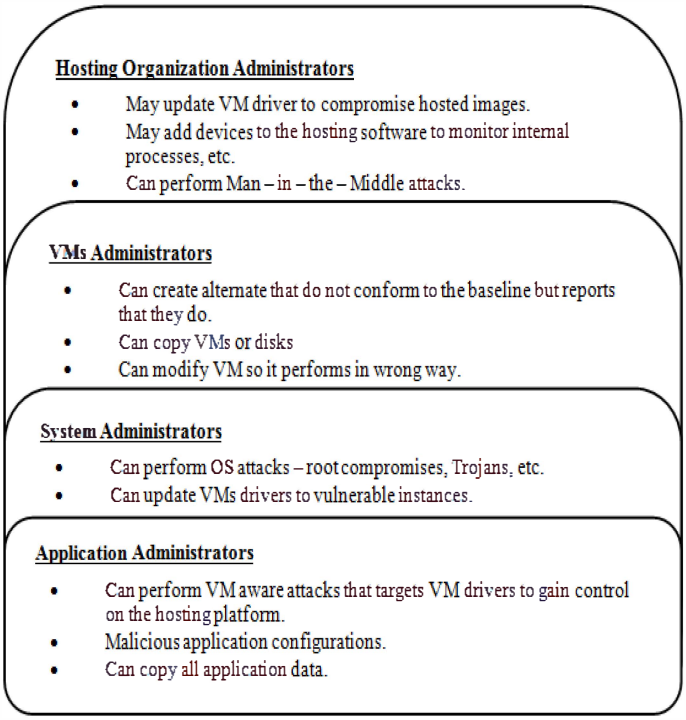

Figure 3. Cloud Administrators and Potential Threats [16]

H. Identity Management

Identity management is the building block of achieving confidentiality, integrity and availability. Due to heterogeneity in cloud systems and models, a federated identity management system which allows users single sign on (SSO) is required across multiple type of cloud systems that satisfies legal and policy requirements [18]. Cloud computing has various service delivery and deployment models that raised the need for an appropriate identity management (IDM), in terms of security, privacy, and provisioning of services to ensure the authorised access as well as to manage access control points, Virtual Machines (VMs) or service identities, etc. Meanwhile access to its relevant stored data has to be monitored and granted by the defined access level for that mode as mentioned in the SLA [19-20]. The security challenges for adopting these models and the relative advantages and disadvantages are listed in Table 2 [21].

TABLE.2 IDM Security Challenges [21]

IDM	Advantages	Disadvantages	Security Challenges
Independent IDM stack	• Easy to implement • No separate integration with the organization's directory.	• The user needs to remember separate credential's.	• Should be highly configurable to facilitate compliance with the organization's policies.
Credential Synchronization	• Users do not need to remember multiple passwords.	• Require integration with the organization's directory. • Has higher security risk value due to the transmission of user credentials' outside the organization perimeter.	• There is a need to ensure security of users credentials' during transit and storage to prevent their leakage.
Federated IDM	• Users do not need to remember multiple passwords. • No separate integration with the organization's directory. • Low security risk value as compared to credential synchronization.	• More complex to implement.	• There is a shared need between the cloud vendor and client to ensure that proper trust relationship and validation are established for secure federation of user identities.

I. Abuse and Nefarious Use of Cloud

Since cloud computing offers various computing services on demand in low cost and sometimes in free trial versions, people may misuse these services regarding to their benefits. According to Cloud Security Alliance (CSA) [3] the threat of misusing cloud computing services is a challenge that should be faced since this threat can result from various situations such as tampering of information by internal personnel (malicious insiders), the destruction of network and system resources by external personnel or hackers (malicious outsiders) who intrude through the vulnerability of cloud information system. In addition to threat of system failures and information damage which caused by lack of accountability or carelessness of internal personnel, however, system attack and information leakage are caused by unprofessional operation of internal personnel. These threats are illustrated in Fig.4 [17] as follows.

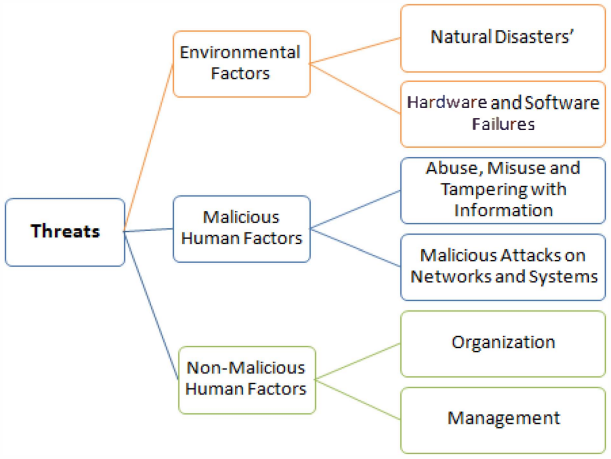

Figure 4. Cloud Information System Threat Factors [17]

Strong authentication and access control mechanisms should be applied in addition to security and privacy tools and techniques to provide isolation of clients from each other's VMs, as well as applying disaster recovery methods to provide data availability and to secure the data from environmental incidents that causes data loss.

III. CONCLUSION

Several industries are moving towards adopting cloud computing regarding to it significant features and low cost. However, the industry data being under the control of CSP created a risk of data leakage that posed a barrier against trusting this agile paradigm. Clients must make sure that the CSP is willing to undergo external audits and/or security certifications. In this paper we tried to view cloud challenges to be considered and solved in order for clients to be confident to implement the cloud paradigm in critical industries.

ACKNOWLEDGMENT

Our gratitude goes to God Almighty who gave us the knowledge to complete this work.

REFERENCES

[1] IBM, "IBM Data Center Networking: Planning for virtualization and cloud computing," International Technical Support Organization, 2011.

[2] Appistry, "Unlocking the Promise of Cloud Computing for the Enterprise Achieving scalability, agility and reliability with cloud application platforms," [Online] Available at: http://charltonb.typepad.com/papers/Unlocking_the_Promise_of_Cloud_Computing_for_the_Enterprise.pdf .

[3] P. Praveen , et al, "Challenging Threats and Flaws in Cloud Computing Environment," International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012, pp.1-5.

[4] M. Srinivasan, et al.,"State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud computing environment," In: International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012), ICACCI '12, ACM, 2012, CHENNAI, India.

[5] A. Tolnai and S. von Solms, "The Cloud's Core Virtual Infrastructure Security," Global Security, Safety, and Sustainability Communications in Computer and Information Science, 2010, Volume 92, pp. 19-27.

[6] S. Lei, D. Zishan, and G. Jindi, "Research on Key Management Infrastructure in Cloud Computing Environment," Grid and Cooperative Computing (GCC), 2010 9th International Conference on, pp. 404–407, Nov. 2010.

[7] F. Sabahi, "Cloud computing security threats and responses," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, pp. 245–249, May 2011.

[8] M. Poulymenopoulou, F. Malamateniou, and G. Vassilacopoulos, "E-EPR: a cloud-based architecture of an electronic emergency patient record," In Proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '11). ACM, 2011 , Article 35 , 7 pages

[9] R. Padhy, M. Patra, and S. Satapathy," SLAs in Cloud Systems: The Business Perspective," International Journal of Computer Science and Technology , March 2012, Vol. 3, Issue 1. Page no. 481 488.

[10] K. Mu-Hsing, "A Healthcare Cloud Computing Strategic Planning Model," Computer Science and Convergence, Lecture Notes in Electrical Engineering, 2012, Volume 114, Part 6, pp. 769-775.

[11] CPB UK Ltd," Security Survey Results - Threats Anticipated by Organisations," Business Technology Group (BTG), 2011 [Online] Available at: http://www.btg-uk.com/security-research.html

[12] D. Chen, H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.

[13] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Elsivier, Volume 28, Issue 3, March 2012, pp. 583–592.

[14] C. Probst," Privacy Penetration Testing: How to Establish Trust in Your Cloud Provider," European Data Protection: In Good Health?, Springer Jan 1, 2012, Part 3, pp. 251-265.

[15] D. Cappelli, A. Moore, and R. Trzeciak, "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)," ser. SEI Series in Software Engineering. Addison-Wesley Professional, 2012.

[16] W. Claycomb and A. Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges," in COMPSAC 2012: Trustworthy Software Systems for the Digital Society, COMPSAC 2012, The 36th Annual International Computer Software and Applications Conference 2012 .

[17] Q. Li and Z. Xie, "A Correlation Analysis Method for Threat Factors in Information System Based on Cloud Model," Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference on, pp. 541–544, Apr. 2010.

[18] V. Winkler, "Designing Cloud Security," chapter7 in Securing the Cloud: Cloud Computer Security Techniques and Tactics, Elsevier,2012, pp. 307-327.

[19] M. Srinivasan and P. Rodrigues, " A roadmap for the comparison of identity management solutions based on state-of-the-art IdM taxonomies," Springer Communications in Computer and Information Science, 2010 , pp. 349-358.

[20] M. Srinivasan and P. Rodrigues, "Analysis on identity management systems with extended state-of-the-art IdM taxonomy factors," International Journal of Ad hoc, Sensor & Ubiquitous Computing , December 2010, Vol.1, No.4, pp. 62- 70.

[21] S. Subashini and V.Kavitha "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, Elsivier, Volume 34, Issue 1, January 2011, Pages 1–11