IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. II (Jul.-Aug. 2017), PP 39-43
www.iosrjournals.org

A Quantitative Analysis of Infrastructural Security Concerns in Cloud Computing for Indian SMEs

[*]Monisha Singh[1], C. Suresh Kumar[2]
[1]*JJT University, India*
[2]*Dr. Nagarathinam's College of Engineering, India*
Corresponding Author: Monisha Singh

Abstract: *SMEs (Small and Medium-size Enterprises) are essential drivers for innovation and growth in India. It is observed that SMEs are picking up the most from cloud computing, as it is a complex and costlier task to set-up and run ICT (Information and Communication Technology) in a traditional way. But, many SMEs generally do not see all the information security risks involved in cloud computing and have to compromise on their data at the end. This paper provides a guidance for SMEs of India about the security aspects of cloud computing. It facilitates the decision making process through the proposal of a taxonomy which highlights the security factors to be considered when evaluating the cloud as a potential solution. The data was collected through a quantitative survey which gave inputs for forming up the taxonomy based on the scenario in India. This paper provides a roadmap to the current and potential stakeholders of cloud who need to ensure security of data*.

Keywords: *Cloud Adoption, Cloud Computing, Cloud Security, Security Taxonomy, Indian SMEs.*

Date of Submission: 05-07-2017 Date of acceptance: 15-07-2017

I. Introduction

Cloud computing has turned out to be more than just an IT buzzword. It has already made a significant impact on the way organizations operate and deal with the daily issues. Indian SMEs are adopting and utilizing this technology for their benefits at a higher rate. Implementing information technology solutions and platforms could be a complex job for SMEs as it may lead to a heavier cost. Cloud computing services make it easier for SMEs to host light weight applications and services and build the desired infrastructure. Many organizations have started implementing cloud computing solutions for their overall growth and business strategy [1]. As far as cost enhancement and monetary downturn are concerned, SMEs consider cloud as the best approach. Although there are many benefits in adopting this technology, but at the same time there are significant barriers to the same. Many organizations integrate their products with cloud to a greater extent, because of which more and more information gets transferred onto the cloud. Eventually, it increases the probability of losing control over data. Though many organizations have started storing their data on cloud, but majority of them are yet to get comfortable with the idea that their data would be secure and would not be misused once ported onto the cloud [2]. Transferring sensitive data onto cloud is one of the major concerns of SMEs. Service availability, data confidentiality, provider lock-in issues are other issues which contribute towards the loss of data. They are derived from cloud features like scalability, virtualization and resource sharing. Therefore, SMEs need to understand and carefully assess the risks against the benefits. They should check the sensitivity of data and decide what information should be stored in cloud and to what extent. The type of cloud whether it is public, private, hybrid or community cloud is also accountable for deciding what kind of data should be transferred. So, the criticality of data, type of cloud, and the extent of usage of cloud services should be considered before making a decision for moving information to cloud. The present work is an attempt to identify, classify and organize the main security concerns of Indian SMEs in cloud computing, and propose a security taxonomy. This will facilitate a decision making process which will benefit all the small organizations which are planning to move information onto cloud. The main components of cloud infrastructure security are defined and presented at three different levels. This paper is organized as follows. Section 2 presents the related work and section 3 highlights the research methodology used. The results of the survey are discussed in Section 4 and conclusions are presented in Section 5.

II. Related Work

The ever increasing interest in cloud computing has given a reason to study the recent trends in security for such a technology [3]. ENISA (European Network and Information Security Agency) has developed a risk assessment which highlights all the risks and vulnerabilities. It also offers a survey of related works done by many researchers and their recommendations [4]. CSA (Cloud Security Alliance) has also developed a guide to

provide an insight on the security domains of cloud [5]. The documents provided by ENISA and CSA, present various concerns and recommendations regarding services of cloud computing. Though these studies have given valuable inputs, but there are no standardized methods defined which can organize cloud computing security aspects. Cloud computing comprises mainly of two types of model - deployment and service. Each model has its own security issues. Thus, ensuring security of sensitive data in cloud is difficult [6]. In IaaS (Infrastructure as a Service) model, the main responsibility of service provider is to secure infrastructure and abstraction layers, the remaining issues are consumer's responsibility. Therefore, SMEs should be aware of the risks associated with data intrusion before they move their data on cloud. IaaS cloud models are likely to get attacks like XML Signature Element Wrapping [7]. In PaaS (Platform as a Service) model, the service provider is responsible for providing secured platform used for development, but the applications developed using that platform is purely the responsibility of consumers. Hence, some more consideration should be given to the services and binding issues with PaaS cloud models. Jensen [8] highlights that PaaS models are prone to cloud malware injection attacks and metadata spoofing attack. In SaaS (Software-as-a-Service) model, the service provider is responsible for providing security control for infrastructure, applications and data. According to a Forrester research [9], enterprises are least interested in SaaS because of security concerns. When the data is transferred to a remote server through internet, the risk of unauthorized access comes in, which is a major concern in SaaS. This opens up the way for opponents to hack passwords, access data which can be then modified or damaged. Sensitive information on human resources and payment details become vulnerable because of such unauthorized access. Denial of service attacks and network failure are also the concerns of SaaS. Neves [10] determines the issues related to political, economic, social and technological factors which act as a hindrance in the adoption of cloud computing. The paper gave an overview of the trends in cloud computing which can help in decision-making process for SMEs. Yuri Demchenko [11] discusses about the aspects of the cloud security highlighted the conceptual issues, basic requirements and security mechanisms for dynamic cloud infrastructures. Pengfei You [12] discusses regarding the security issues concerning data, application and virtualization in cloud computing, and also the available solutions to these issues. Bernd Gastermann [13] focuses on security aspects of SMEs and highlights the way to minimize the areas vulnerable for threats and strengthen the software components to defy network attacks. The paper presents various methods to protect data on client as well as server-side.

III. Research methodology

Aiming to provide taxonomy for the security issues faced by Indian SMEs in the current scenario, viewpoints of industries which have implemented cloud computing services were analyzed through a survey. The study started by gathering all the security issues and their available solutions from:

a) Conference and Journal papers published by IEEE, Springer and Web science.

b) Organization's reports, white papers, reports from CSA and ENISA.

The questionnaire was designed based on the information derived from the above mentioned sources and was sent to 120 SMEs of few Indian cities like Delhi, Bangalore, Mumbai, Pune, Hyderabad and Chennai. SMEs were asked to list out the security issues which they considered as their biggest challenge. Further, all the solutions preferred by SMEs to overcome those issues were also explored.

IV. Results And Discussions

From the analysis of security concerns in cloud computing infrastructure, it is observed that each issue has a different impact on distinct sets of data. In this section, all the security concerns and vulnerabilities of cloud computing are presented. Data is classified into categories, thus providing the cloud security taxonomy. It is subdivided into three categories, namely network, application and host level based on the survey results. Each category highlights various security issues with the details in subdivisions, identified by SMEs of India. This organization is represented in Figure 1.

Network level:

A. Transit :

1. **Sniffing/Eavesdropping:**Unprotected data in transit in the network is interpreted by the attackers. *Countermeasures:* Implementing IPSec (Internet Protocol Security) to encrypt network traffic, tightening of security by system administrator, using anti-virus software.
2. **Man-in-middle**: Here, the attacker takes hold and alters the communication between two parties who believe that they are directly communicating with each other.
   Countermeasures: Using encrypted network connections provided by HTTPS or VPN (virtual private network) technology.

B. Firewall:

3. **DoS/DDoS attack**: Authorized users are denied of having access and use services on network. Attackers may request more computational resources, which causes legal users to run out of resources. *Countermeasures*: Firewalls should be configured properly, enforcing strong passwords and policies to

offer limited computational resources, limit the number of ICMP and SYN packets on router interfaces, filtering private IP addresses.

4. **Spoofing/Phishing** - Attackers get access to a system by using a false identity. Using stolen user credentials or a false IP address they get access to all the privileges.
   Countermeasures: Packet filtering**,** avoiding trust relationships use spoofing detection software, use cryptographic network protocols.

Application Level:

C. Insecure Interfaces or APIs:

5. **Unauthorized Resource Access:**
6. **Resource Availability:** APIs (Application Program Interfaces) are the means of communication between cloud services and its consumers. If APIs are not secured, the resources will become vulnerable for threats as unauthorised access of resources may happen.
   Countermeasures: Analyse the security model of cloud provider interfaces, ensuring strong authentication and access controls, understand the dependency chain associated with APIs.

D. Resource Usage:

7. **Resource Exhaustion**: It's the inability to provide additional capacity of resources in times of crisis or emergencies.
   Countermeasures: Processes for capacity management, effective real time monitoring and reporting, analysis and study to be carried out by the Cloud Provider.
8. **Unexpected Costs**: Cloud computing is often pay-as-you-go, so costs may go unexpectedly very high depending on the usage.
   Countermeasures: Customers should check their service usage scales and associated costs.

E. Authentication:

9. **Account/Service Hijacking**: An account hijacking can happen through different ways like social engineering and weak account credentials. An attacker gets access to the resources through victim's account.
   Countermeasures: Prohibit sharing of account credentials, force two-factor authentication techniques, monitoring to detect unauthorized activity.
10. **Device Theft/Loss:** In SMEs generally employees use different types of devices which are not fully under the control of IT experts. Device loss can give opportunities for attackers to steal the data. *Countermeasures:* ensure that device theft/loss is mitigated, by using backups, encryption, data minimization, etc.

Host Level:

F. Isolation Failure:

11. **Logical Isolation:** As cloud tenants share the same physical infrastructure, customers may be affected by peaks in resource usage.
12. **Physical Isolation: I**f redundancy for computational resources does not exist the services of cloud may get hampered.
    Countermeasures: Check the SLA (Service Level Agreements), implement physical and logical redundancy in the network infrastructure.

G. Cross VM Attacks:

13. **Side-channel attack:** Here, the attacker observes the activity of the shared physical device eg. Processor cache and hence tries to steal the information.
    Countermeasures: lock down operating system images and application instances as much as possible, dedicate time to tuning and collecting local process monitoring data and logs for cloud systems.
14. **Malicious VM creation:** An attacker creates a Virtual Machine image containing malicious code and stores it in the provider's repository [14].
    Countermeasures: Mirage [15] – a virtual machine image management system which includes access control framework, image filters, source tracking and repository maintenance services.
15. **Insecure VM migration**: Live migration of virtual machines exposes the contents of the VM state files to the network. This gives a chance to attackers to the access data and migrate VM to an untrusted host. *Countermeasures:* Protection Aegis for Live Migration of VMs (PALM), VNSS framework.
16. **Sniffing/Spoofing VM Networks:** A malicious VM can access the virtual network or even use ARP (Address Resolution Protocol) spoofing to redirect packets from/to other VMs [16].
    Countermeasures: Virtual network framework based on Xen network modes: "bridged" and "routed".

H. Hyperviser Vulnerabilities:

17. **VM Escape**: In order to take control of infrastructure, hypervisor is exploited [17].
    Countermeasures: HyperSafe, TCCP (Trusted Cloud Computing Platform), TVDc (Trusted Virtual Datacenter).

18. **VM Hopping:** gaining access to another VM is called hopping[4].
    Countermeasures: preventing the database server from directly accessing the internal network, using private VLANs, using secure operating systems.
19. **Shared Technology**: If the components of shared infrastructure (e.g., CPU caches, GPUs, etc.) are not designed to support multi-tenant architecture, it causes the intrusion of threats.
    Countermeasures: Monitor unauthorized changes, promote strong authentication and access control, enforce service level agreements, conduct vulnerability scanning and configuration audits.

I. Data Access :

20. **Data Loss/Leakage/Breaches**: When data gets leaked into the wrong hands while it is being transferred, stored, audited or processed, it is known as data loss or leakage [19].
    Countermeasures: FRS (Fragmentation-redundancy-scattering) Techniques, digital signatures, encryption, implementing API access control, implement strong key generation, encrypt the data in transit, analyse data protection during design, run time, storage and destruction practices.
21. **Malicious Insider:** *Any* current or former employee, or other business partner who has or had authorized access to an organization's network and systems, misuse their access to the organisation's data.
    Countermeasures: Enforcing strict supply chain management, specify human resource requirements, maintain transparency and compliance reporting, determine security breach notification processes.
22. **Physical Hazards:** When customers get affected by natural disasters occurring at data centers far from their premises.
    Countermeasures: follow measures to protect the cloud service from physical hazards, take backups of data regularly, migrate to another data center or provider when needed.

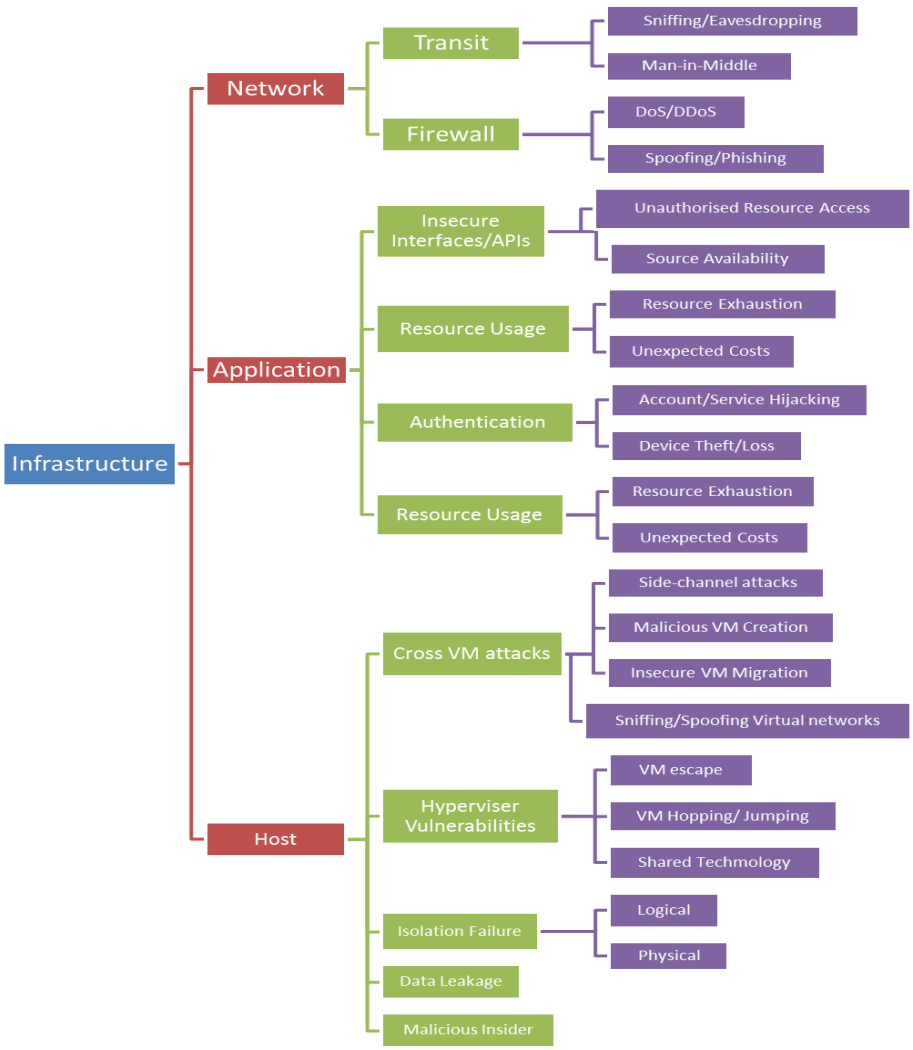

Figure 1. Security Taxonomy

V. Conclusions

Security is a vital perspective for giving a reliable environment and empowers the utilization of applications in cloud. Moving information and business procedures to virtualized frameworks is the biggest concern of all the organizations. A secure cloud computing environment depends on various security solutions provided by the cloud providers. In this paper, the major security issues of cloud computing faced by SMEs of India are explored. The outcome of survey is the proposed taxonomy which can be fruitful for all the upcoming SMEs as it provides a roadmap of the security issues. Before implementing cloud technology, SMEs can think over the concerns and their solutions. It also guides the cloud providers to know the areas of improvement and the need to blend security solutions from various places in order to achieve the desired security level.

References

[1] Cloud Computing For Small And Medium-Sized Enterprise, Office of Privacy Commissioner of Canada.
[2] Changing the Business Ecosystem, KPMG India, 2011.
[3] IbrahimAS, Hamlyn-HarrisJ, Grundy. Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC2010 Cloud Workshop, APSEC'10, 2010.
[4] Catteddu D, Hogben G, "Benefits, risks and recommendations for information security. Tech.rep", European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment.
[5] Security Guidance for Critical Areas of Focus in Cloud Computing. Tech.rep, Cloud Security Alliance, 2009.
[6] Kandukuri, B.R., Paturi, V.R., Rakshit, A.: Cloud Security Issues. In: IEEE International Conference on Services Computing, pp. 517–520, 2009.
[7] McIntosh, M., Austel, P.: XML Signature Element Wrapping Attacks and Countermeasures. In: SWS 2005: Preceedings of the 2005 Workshop on Secure Web Services, pp. 20–27. ACM Press, 2005.
[8] Jensen, M., Gruschka, N., Iacono, L.: On Technical Security Issues in Cloud Computing. In: IEEE International Conference on Cloud Computing, pp. 109–116 (2009).
[9] Top Corporate Software Priority Is Modernizing Legacy Applications, Forrester Research, Press release, 2009.
[10] Fátima Trindade Neves, Fernando Cruz Marta, Ana Maria Ramalho Correia, Miguel de Castro Neto: The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors. In: 11th Conferência da Associação Portuguesa de Sistemas de Informação, 2011.
[11] Yuri Demchenko, Canh Ngo, Tomasz Wiktor Wlodarczyk, Chunming Rong, Wolfgang Ziegler "Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services" in Third IEEE International Conference on Cloud Computing Technology and Science, 2011.
[12] Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue, "Security Issues and Solutions in Cloud Computing", in 32nd International Conference on Distributed Computing Systems Workshops, 2012.
[13] Bernd Gastermann, Markus Stopper, Anja Kossik, and Branko Katalinic : On-Premises Cloud Storage – Security Aspects for Small and Medium-sized Enterprises, in Proceedings of the International Multi Conference of Engineers and Computer Scientists 2015 Vol II, IMECS 2015, March 18 - 20, 2015, Hong Kong.
[14] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50-57, March-April 2011.
[15] Wei J, Zhang X, Ammons G, Bala V, Ning P: Managing Security of virtual machine images in a Cloud environment, in *Proceedings of the 2009 ACM workshop on Cloud Computing Security*. NY, USA: ACM New York; 91–96, 2009.
[16] Jenni Susan Reuben, "A Survey on Virtual Machine Security", in TKK T-110.5290 Seminar on Network Security, 2007.
[17] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, "Ensuring data storage security in Cloud Computing," in *17th International Workshop on Quality of Service*, Charleston, SC, 2009, pp.1-9, 2009.
[18] Top Threats To Cloud Computing V1.0, Cloud Security Alliance, 2010.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Monisha Singh. "A Quantitative Analysis of Infrastructural Security Concerns in Cloud Computing for Indian SMEs." IOSR Journal of Computer Engineering (IOSR-JCE) 19.7 (2017): 39-43.