ISSN 22773061

Challenges and Security Issues in Future IT Infrastructure Components

Syed Mubashir Ali
Department of Computing, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, SZABIST, United Arab Emirates
mubashir8733@gmail.com

ABSTRACT

Over the past 2 decades, the information technology infrastructure has gone through an exponential change with the introduction and evolution of new technologies and trends. Organizations previously having their data on-premise and their infrastructure comprising of multiple server machines on multiple server racks and dedicated client personal computers (PCs) are moving towards cloud computing & virtualization to Smartphone and tablets. This rapid advancement and constant change, although increasing productivity for the organizations is resulting in a rising number of challenges and security issues for the organizations, their managers, IT administrators and technology architects. This paper discusses the future IT infrastructure components and the challenges & security issues that arise after their implementation that needs to be taken care of in order to get the full advantage of IT.

Indexing terms/Keywords

Cloud computing, IT infrastructure, Mobile devices, Information security, Virtualization.

Academic Discipline And Sub-Disciplines

IT, Computer Engineering, Computer Science, IT Infrastructure, Information Security, Cloud Computing;

SUBJECT CLASSIFICATION

IT Infrastructure, Information Security

TYPE (METHOD/APPROACH)

Literary Analysis;

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 8, No 2
editor@cirworld.com
www.cirworld.com, member.cirworld.com

INTRODUCTION

IT infrastructure has been evolving and will continue to grow and advance exponentially in the future. It started from mainframe centric infrastructure to globally dispersed and distributed clusters. Enterprises from initially using desktops and laptops are moving towards mobile and cloud computing. Marketing and advertising channels previously used short messaging services and television advertisements are now shifting towards social media and social network marketing. This evolution of IT infrastructure provided more flexibility to the businesses and enterprises. This continual change and advancement in the IT infrastructure will raise some security issues that previously either didn't exist or were insignificant for the organizations. In this and future era of information and knowledge management; data and information privacy, integrity, reliability and security are and will be the most important aspects and a challenge for IT engineers, scientists and researchers. This study will focus on future IT infrastructure components including cloud computing, virtualization and mobile devices (e.g. Smartphone, tablets). Then will explain the challenges and security issues that arise after their implementation. And the final part will conclude the discussion of this research paper.

FUTURE IT INFRASTRUCTURE COMPONENTS

Future IT infrastructure could be having many different components but this study will consider cloud computing, virtualization and mobile devices. Cloud computing is a model for IT infrastructure which provides ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimum management effort or service provider interaction. [1]

Virtualization is the simulation of the software and/or hardware upon which other software executes. This simulated systems environment is called a virtual machine (VM) or simulated network is called virtual network (VN). [2] In future IT infrastructure, organizations and IT architects will focus on improving the client and business users' user-experience, achieving agreed service level, to utilize the full processing power of the underutilized servers and reduce the overheads of air conditioning and power consumption by multiple physical server machines. As a result, there will be an increased implementation of virtualization of IT infrastructure as it reduces the need for multiple servers thus reducing IT infrastructure deployment & maintenance cost and provides efficient use of the existing resources within the organization.

There has been a rapid growth of mobile device usage all over the world. [3] The increase in use of mobile devices (e.g. Smartphone, tablets) is increasing day by day within enterprise as well as home users; as more advanced mobile operating systems (e.g. Android, IOS, Windows Phone) and powerful productivity applications are now available and an increasing trend of "Bring your own device" (BYOD). By 2014, it is predicted that there will be more broadband users on mobile phones and tablets than traditional internet users. Interestingly, Smartphone statistics indicate that 48 percent of users use their smartphones to aid their work. [4]

CHALLENGES AND SECURITY ISSUES

Technology and inventions do have their own advantages. But the use of technology have been known to develop some challenges, risks and security issues that needs to be addressed in order to have the real benefit from the investment in the IT infrastructure. Following are some of the challenges and threats that may arise in the future IT infrastructure.

Service Reliability

In cloud computing, one of the major issues is service reliability. Organizations as the technology is advancing, are and will store huge amount of their mission critical data and information on cloud which they need to be accessible 24/7. For the data to be readily available when needed from the cloud, the cloud service provider needs to have a highly reliable service. Therefore a considerable amount of investment and planning is required from the cloud service provider on their technology infrastructure to implement effective measures including but not limited to redundant servers on multiple geographical locations to provide service reliability. For-example in February 2008, cloud storage infrastructure of Amazon's Web Service (Amazons-S3) experienced a downtime of several hours that caused access issues and loss of data. [5] If an organization as big as Amazon could face reliability issues, other cloud service providers can be more prone to service reliability issues and downtime. Hence cloud computing reliability issue needs to be addressed properly since for mission critical data, small amount of downtime can result in a huge financial and business loss for organizations.

Data Encryption

Organizations have many sensitive data that they store on cloud and on premise. VMs and on cloud data is accessible through cloud and Virtual Private Network (VPN) on PCs and mobile devices. This sensitive data needs to be encrypted. In case, where an attacker manages to gain unauthorized access to that information that is encrypted will not be able to get advantage of or misuse that information.

Inter-Network Dependency

Cloud computing as well as mobile devices in enterprises needs internet availability at all times. Employees and organizations will have their emails, documents and data on cloud and on email servers and in order to access them they need access to internet. In order to access the data remotely through Virtual Private Network (VPN) on premise or on cloud needs always-on internet. This raises issue that what if internet service is down or unavailable, and what will happen to the client systems and critical business operations that needs to run 24/7 such as hospitals and financial institutions. In some developing countries, where there are power breakdowns and internet service is not considered to be reliable will greatly face the risk of data unavailability. [5]

Unauthorized Access

Smartphones and other mobile devices will contain organizations' sensitive information in the form of stored emails and documents that are vulnerable to leakage if the mobile device gets unauthorized physical access in case it gets lost or stolen. With the increasing trend of BYOD, there will be potential threats due to lack of control over such mobile devices.[6] Isolation between virtual machines can provide certain level of security through VPN tunneling and encryption, [7] but still there will be threats of intrusions and attack to the physical VM that needs to be addressed.

CONCLUSION

The technological revolution will bring in and make various technologies and platforms more popular and more feasible to be integrated in the future IT infrastructure. This evolution and advancement of information technology infrastructure will offer a number of benefits and advantages to the organizations and helps them to have better business productivity. This advancement in technology although providing several benefits will raise some security issues that needs to be addressed in order to avoid financial loss and to get the actual payback and return on investment on IT infrastructure to the organizations.

ACKNOWLEDGMENTS

I would like to thank my professor, Dr. Tariq Rahim Soomro for his continued support for conducting this study.

REFERENCES

[1] Mell, P. and Grance, T. 2011. The NIST definition of cloud computing (Draft), Recommendations of the National Institute of Standards and Technology. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[2] Scarfone, K., Souppaya, M. and Hoffman, P. 2011. Guide to security for full virtualization technologies. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

[3] World Economic Forum. 2012. Global IT report 2012. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

[4] MacCormick, J. S., Dery, K. and Kolb, D. G. 2007. Engaged or just connected? Smartphones and employee engagement. Organizational Dynamics. 41(3), 194.

[5] Bamiah, M. A. and Brohi, S. N. 2011. Seven deadly threats and vulnerabilities in cloud computing. International Journal of Advanced Engineering Sciences and Technologies, Vol , (9).

[6] Niharika Singh, N. 2012. B.Y.O.D. genie is out of the bottle – "Devil Or Angel". Journal of Business Management and Social Sciences Research, Vol, (1).

[7] Chowdhury, N. M. K. and Boutaba, R. 2009. Network virtualization: state of the art and research challenges. Communications Magazine, IEEE. Vol, 47(7).

Author' biography with Photo

Syed Mubashir Ali has completed his BS in Computer Engineering from National University of Computer and Emerging Sciences – FAST, Karachi, Pakistan. Currently he is enrolled in MS Computing in IT at Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, SZABIST, Dubai, United Arab Emirates. His research interest includes IT infrastructure, Cloud computing, Standardization of IT, IT governance, E-Learning, Enterprise resource planning and IT performance measurement.