International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Multi-Tenant Framework for An Enterprise System on Cloud

Dr. Sarvjit Singh Bhatia[1], Vikram Gupta[2]

[1]Senior Faculty, PG Deptt .of Computer Science, Khalsa college Patiala, Punjab, India – 147001

[2]Research Scholar, Uttarakhand Technical University, Dehradun, Uttarakhand, India

Abstract: ***Enterprise systems provide integrated information for all activities in an organization. These systems serve as a vital asset to any organization and hence it becomes mandatory to ensure their security. Information security combines systems, operations and internal controls to ensure the availability, integrity and confidentiality of data and operational procedures in an organization. In the present scenario these services are offered on the cloud mainly to reduce inherent risk associated with the traditional enterprise systems. Cloud computing represents a significant shift in the way that IT resources are managed, operated, and consumed. This change exposes several benefits to enterprises, promoting greater IT efficiency and agility. This paper is intended to suggest a Multitenant security framework of enterprise systems on cloud. The dependency on integrated information systems (Enterprise Systems) in an organization is increasing day by day. An enterprise system is a combination of several applications that supports and automates business processes and manages business data. The term enterprise system is often used synonymously with enterprise business application or with the more restricted term an enterprise resource planning (ERP) system [Gulla,(2004)]. Enterprise Systems help in carrying out various tasks with greater operational efficiency and reliability. They also facilitate to keep information updated and available across the organization 24 * 7. These systems process thousands of transactions every day and store information about all aspects of the business. According to Haigh D [Haigh ,(2004)] the potential benefits of enterprise systems depend on the way they are employed to improve the business processes. As enablers of successful business reengineering projects, they help the organizations to save money, keep their business data consistent, current and available, speed up business processes, and improve the quality and reliability of the processes.***

Keywords: Enterprise Systems, Information security,Cloud computing, multi tenancy , Enterprise Resource Planning (ERP)

1. Introduction

Enterprise systems, even those that are industry specific, are designed for a large audience of companies looking to achieve success by following a template of best business practices [Moon, (2008)]. But many a times, the ERP software's tries to replicates existing processes which leads to costly program modifications. This, in turn, can result in unnecessary manual tasks and issues of software maintenance, which neutralize the original benefits of the software. On the other hand the benefits of these systems cannot be enjoyed to the fullest by the organization due to huge investment and implementation failure. Hence it's time for companies to move on to eliminate these massive shackling on-premise systems that has been inhibiting growth and creativity for so long [Djohnson, (2011)]. Moving onto Cloud helps to overcome many of the limitations of on-premise enterprise systems. Enterprise Resource Planning (ERP) systems have been around for over two decades in which case organizational data reside within the premise of the organizations . However, with the emergence of cloud computing which is a paradigm concept of accessing a network of remote servers via the Internet for the purpose of managing, processing and storing data, many enterprises have seized the opportunity based on its many advantages over the traditional model, such as scalability, flexibility, cost effectiveness, reliability, broad network access, etc to move their businesses to the cloud [1]. Therefore, Cloud ERP is just a name coined from the combination of Enterprise Resource Planning (ERP) Systems and Cloud Computing. In spite of these numerous benefits of cloud computing, many organizations, most especially, large enterprises, are hesitant and afraid to migrate their precious organizational data to the cloud apparently on the ground of insecurity.

2. Benefits of Cloud based Enterprise systems

- Group Organization: All the different branches of an organization can access the same cloud based system in real time through the web.
- Uptime: The system is always up and running, which guarantees a zero down time.
- Reduced Cost: The business model of Cloud computing is pay-per-use and hence the customers only need to pay on the basis of the usage of a particular service.
- Scalability: Cloud based enterprise systems gives the organization the flexibility to add more users as the business grows. In the case of on-site ERP solutions it is often necessary to provide additional hardware.
- Unrestrained Access: Any user can access the system based upon the roles assigned to them. Since Cloud supports Ubiquitous network access, the system can be accessed using various devices of their choice and through any wired or wireless protocols.
- Human Resources: Maintenance of the system is done by the service provider. Hence no additional skilled man power needs to be employed by the organization.

- Increased performance Requirements: Expanding the system, handling peak load performance issues etc. become very simple for the organization.
- Customization: The customer has got the freedom to choose from among the modules and the services offered by the cloud service provider.
- Speedy Implementation: Cloud ERP typically takes 3-6 months compared to the 12 months that it typically takes to implement an on-premise solution.

3. Theoretical Background

According to the official NIST definition, "Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [Peter et al., (2009)]. Basically, ERP is designed to integrate data from across all the business functions within an organization and also to integrate data as it concerns supply, production, distribution and product delivery to customers [15]. In traditional ERP, software or solutions are installed locally in computers and data are stored in servers in-house. Platforms and infrastructure are under the control of the organization. Moreover, management of data including its security, maintaining the server and cost of general maintenance of infrastructure and space occupied as well as disaster recovery provision are all responsibility of the enterprise [16]. However, with the emergence of cloud computing which is a paradigm concept of accessing a network of remote servers via the Internet for the purpose of managing, processing and storing data, many enterprises have seized the opportunity based on its many advantages over the traditional model, such as scalability, flexibility, cost effectiveness, reliability, broad network access, etc to move their businesses to the cloud. Therefore, Cloud ERP is just a name coined from the combination of Enterprise Resource Planning (ERP) Systems and Cloud Computing. Cloud-based ERP systems are basically provided using the Software-as-a-Service (SaaS) architecture, under a situation where users rent the software and use, rather than buy it [17].

4. Cloud Based ERP Security Layers

Cloud security needs to be enforced at the Physical, Network, Data and Application level. Since social engineering is on the rise, while providing physical security, the cloud provider must define and enforce rules of conduct and social guidelines for employees. Network security should protect all virtual access points to the cloud by employing well-managed security rules and procedures to block attacks. Data security should ensure that both the data in storage as well as data in transit are protected from unauthorized third parties. Since most applications are built to be run in the context of an enterprise data center, the lack of physical control over the networking infrastructure might mandate the use of encryption in the communication between servers of an application that processes sensitive data to ensure its confidentiality. [Savage, (2011)] Literature reveals that many organizations are migrating their on-premise enterprise systems to Cloud based Software-as-a-service (SaaS) enterprise system. ERP.com claims that cloud-based enterprise systems are easier to use, deploy and maintain, thus further reducing the time and cost of meeting specific business needs and stay competitive in the market [Rich, (2010)]. In a 1999 article that described issues surrounding ERP implementation, the authors have mentioned that the process often takes more than 3 years [Bingi et. al., , (1999)]. Traditional implementation often runs into millions of dollars [Seddon et al , (2010)]. This trend appears to be changing. In a recent blog post describing trends for ERP in 2011, ERP consultant Eric Kimberling predicts a "heavy adoption of Software-as-a-Service [SaaS] models at small and mid-size businesses" [Kimberling , (2011)].

5. Proposed Multi-tenancy Framework and Cloud Security

Literature reveals that many organizations are adopting cloud–based enterprise systems in the present scenario. But at the same time the enterprises should be convinced that security is not a threat for their implementation. Hence this study has been under taken to propose a framework to enhance the security. The idea of multi-tenancy is fundamental to cloud computing. Multi-tenancy is a term that defines the use or sharing of the same application or resources by two or more (multiple) consumers that may come from the same or different organizations. This is a situation where the organization operating systems and applications are run on virtual machines (VM) hosted in parallel configuration with the VM of other organization on shared physical devices [2], [3]. According to [4], "Information Security or Security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction". In a multitenant environment, where multiple independent users or consumers share the same physical infrastructure, and in a scenario where the tenants which may have opposing goals share a pool of resources, securing the multiple tenants‟ sensitive data and information becomes a challenge. Also, conflict of interest may result. So, how does multi-tenancy deal with conflict of interest? Can tenants get along together and „play nicely‟? If they can‟t, can they be isolated? How to provide separation between two or more tenants? Thus an attacker can legitimately be in the same physical machine as the target [6]. Multi-tenancy is known to be the root cause of concerns for many users [5]. Nevertheless, the fact remains undeniable that it enables optimal server utilization, thus lowering costs of infrastructure. However, the threats posed by multi-tenancy feature of cloud differ as we move from one cloud delivery model to another [7]. According to a report released by Gartner, 60% of virtualized servers will be less secure than the physical servers which they replace [8]. Currently, as identified by [9], multi-tenant cloud is faced with two major sources of threats: virtualized infrastructure which can be attacked by the exploitation of possible security vulnerabilities in the massive and complex virtualized pile of software; also, attacks from unauthorized accesses to sensitive and precious data from cloud operators. Hence, in multi-tenancy, residual data can be visible to a co-tenant while trace of operations by a co-tenant is also very

possible. These have been found to constitute a challenge to the security and privacy of data in cloud environments [10]. A couple of researchers have worked in the area of ensuring security in the multitenant domain: [11] (Isolation and customization); [12] (Suggests removal of virtualization layer); [13] (Incorporation of Active Protection System); [14] (Constructing a Virtual Machine Monitor in form of a new Micro-Kernel), and many others. However, research is still ongoing as more and more vulnerabilities, threats, risks and security challenges emerge with time.

6. Benefits of Multi-tenancy Framework

In a cloud-based enterprise system, the sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the service provider's end. The communication management module assures the security of the information that gets communicated in the cloud environment either within a network or across networks.

6.1 Transmission Security Component: Ensuring the confidentiality of data transmitted between different participants in a cloud environment is more difficult compared to an on-premise environment. Security of transmitted data can be achieved through encrypting all communications from the source to destination using encryption algorithms such as DES, Triple DES, RSA etc.

6.2 Network Security Component: Applications running in an external cloud environment requires passing data between the cloud and the user location. Frequently the communication occurs over the Internet and over Wireless networks. The network security component of the security framework can use strong network traffic encryption techniques like Secure Sockets layer (SSL) and Transport layer security (TLS) to protect all communications with the server. The SSL algorithm is supported by all major browsers and requires less computing overhead. SSL encapsulates application specific protocols like HTTP to form HTTPS and hence none can hijack a session or read the data. The network security component may include tests that check for various security threats such as network penetration and packet analysis, session management weaknesses, Insecure SSL trust configuration.

6.3 Data Security Component: In the SaaS model, the enterprise data is stored outside the enterprise boundary at the SaaS vendors end. Data security mechanisms limits access to data objects to specific individuals. The data security component may enforce data security for ERP systems either through business logic or at the database layer. The business logic applied for data security authenticates users and provides them with specific rights to data objects and controls the specific actions that individual users can perform on different objects. The component should support different level of security such as read-only, insert, delete and edit according to the role of the user and the type of object. The component should include mechanisms to protect against attacks such as Cookie manipulation, Cross-site scripting (XSS), Hidden field manipulation etc. [Bhadauria et al., (2011)]

6.4 Data Integrity Component: Maintaining data integrity ensures uniformity in the different instances of same data residing at multiple locations. The integrity component should ensure that the integrity of enterprise's data stored in the database in cloud is not compromised.

6.5 Identity Management Component: Identity management involves identifying individuals in a system and filtering the access to the resources in that system by placing restrictions on the established identities. The identity management component may follow credential synchronization model to support identity management and sign on services [Subashini and Kavitha , (2010)]. In this model, the SaaS vendor supports replication of user account and SaaS application. The user account information creation is done separately by each enterprise within the enterprise boundary to comply with its regulatory needs. Relevant portions of user account information's are replicated to the SaaS vendor to provide sign on and access control capabilities. The Identity management module must contain mechanisms to ensure security of the credentials during transit and storage and to prevent their leakage.

7. Conclusion

Cloud based SaaS enterprise systems are growing in popularity due to its ability to cater to the increasing volume and range of services required by enterprise systems. The goal is to develop a prototype based on the proposed framework, capable of addressing the problem of choosing suitable Cloud ERP providers for the industry on the security and privacy apparatus provided by the providers in a multi-tenant environment. The future prospects of this framework is expected to be validated via tangible evidence.

References

[1] Lin, A and Chen, N. C. (2012): Cloud computing as an innovation: Perception, attitude, and Adoption; International Journal of Information Management, Vol. 4 No.1.
[2] Pek, G., Butty´an, L and Bencs´ath, B (2013): A Survey of Security Issues in Hardware Virtualization. ACM Computer Surv. 45, 3, Article 40, 34 pages.
[3] Brooks, T. T., Caicedo, C and Park, J. S (2012): Security Vulnerability Analysis in Virtualized Computing Environments; International Journal of Intelligent Computing Research (IJICR), Volume 3, Issues 1/2, Mar/Jun 2012, pp 277-291.
[4] Al-Jahdali, H., Townend, P and Xu, J (2013): Enhancing Multi-Tenancy Security in the Cloud IaaS Model over Public Deployment; In proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. Pp. 385-390.
[5] Wood, K and Anderson, M (2011): Understanding the Complexity Surrounding Multi-tenancy in Cloud Computing; In proceeding of the Eighth IEEE International Conference on e-Business Engineering (ICEBE), pp. 119 – 124.
[6] Musson, B. (2012): Clouds on the Horizon: Cloud Security in Today"s DoD Environment, Memorandum of the United StatesDepartment of Defense. July, 2012.

[7] Marinescu, D. C (2013): Cloud Computing: Theory and Practice. (1st Edition), 24 May 2013. 416 Pages.
[8] Gartner Inc., Six Most Common Virtualization Security Ristks and How to Combat Them; STAMFORD, Conn. Available at: http://www.gartner.com/it/
[9] Zhang, F., Chen, J., Chen, H and Zang, B (2011): CloudVisor: Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization. Association for Computing Machinery (ACM). SOSP ‟11, Cascais Portugal, Oct 23-26, 2011
[10] CSA (2011): Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Cloud Security Alliance. Pg. 1-177.
[11] Cai, H., Wang, N and Zhou, M. J (2010): A Transparent Approach of Enabling SaaS Multi-tenancy in the Cloud; 2010 IEEE 6th World Congress on Services, pp. 40-47.
[12] Keller, E., Szefer, J., Rexford, J and Lee, R. B (2010): NoHype: Virtualized Cloud Infrastructure Without the Virtualization, The 37th Annual International Symposium on Computer Architecture, June 19-23, 2010.
[13] Flood, J and Keane, A (2010): A Proposed Framework for the Active Detection of Security Vulnerabilities In Multi-Tenancy Cloud Systems; In Proceedings of the 3rd IEEE International Conference on Emerging Intelligent Data and Web Technologies, pp 231-235.
[14] Steinberg, U and Kauer, B (2010): NOVA: A Microhypervisor-based Secure Virtualization Archietecture; In Proceedings of Eurosys, ACM, pp 209–222.
[15] Sumner, M (2004) Enterprise Resource Planning. Pearson / Prentice Hall.
[16] Duan, J., Faker, P., Fesak, A and Stuart, T (2012): Benefits and Drawbacks of Cloud-Based versus Traditional ERP Systems. Proceedings of the 2012-13 Course on Advanced Resource Planning, 12/2012
[17] Ivanov, I. I (2012): Cloud Computing in Education: The Intersection of Challenges and Opportunities, Web Information Systems and Technologies (101:1), pp. 3 – 16.

Author Profile

Dr. Sarvjit Singh Bhatia, received the MCA degree from Thapar University Patiala, M.Tech From PTU jalandhar and Ph.D from Punjabi University Patiala. His area of interest is interfacing the Cloud Computing with ERP. He has written the books on Implementation of ERP in SMEs, Computer organization and Architecture, Relational Data Base Management System, Object oriented programming C++ etc.