A SECURITY FRAMEWORK FOR AN ENTERPRISE SYSTEM ON CLOUD

Ms. SUMITRA BINU
Research scholar (Ph.D) , Dept.of Computer Science, Christ University
Bangalore, Karnataka, India - 560029
sumitrabinu@gmail.com

Dr. J. MEENAKUMARI
Associate professor, Dept. of Computer Science, Christ University
Bangalore, Karnataka, India - 560029
Meenakumari.j@christuniversity.in

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 security framework of enterprise systems on cloud.

Keywords: Enterprise Systems; Information security; Cloud computing; Efficiency; Agility; Framework.

1. Introduction

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.

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.

2. Benefits of Cloud based Enterprise systems

- 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.

- 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.
- Uptime: The system is always up and running, which guarantees a zero down time.
- 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.
- Group Organization: All the different branches of an organization can access the same cloud based system in real time through the web.
- Speedy Implementation: Cloud ERP typically takes 3-6 months compared to the 12 months that it typically takes to implement an on-premise solution.
- 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.

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)]. Cloud supports three service delivery models and four deployment models. Even though services offered by Cloud can be exploited by enterprises to leverage their business and enhance profitability by concentrating more on improving their business processes there are lot of security related aspects that needs to be considered.
According to the information security framework specified by Marnewick and Labuschagne [Marnewick and Labuschagne ,(2005)] the three main components include people, policy and technology and this work has been explained from on-premise enterprise systems perspective and do not address the security requirements of cloud-based enterprise systems . Hassan Tabaki et al [Tabaki et al., (2010)] proposed a comprehensive security framework for cloud computing environments. The work done by Mohamed Almorsy et al. [Almorsy et al., (2011)] discusses a cloud computing security management framework that is based on improving the collaboration between cloud providers, service providers and service consumers in managing the security of the cloud platform and the hosted services. The approach adopted for providing security is based on aligning FISMA standard with the cloud model. The article by Djohnson [Djohnson, (2011)] discusses the security issues in ERP cloud, but do not address the issues related to integrity of data as well as providing security during transmission of data within and across networks.

4. Cloud Based ERP Security Layers and Deployment Model

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 Security Framework Components

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. Figure 1 represents the components of the proposed security frame work for cloud-based enterprise systems.

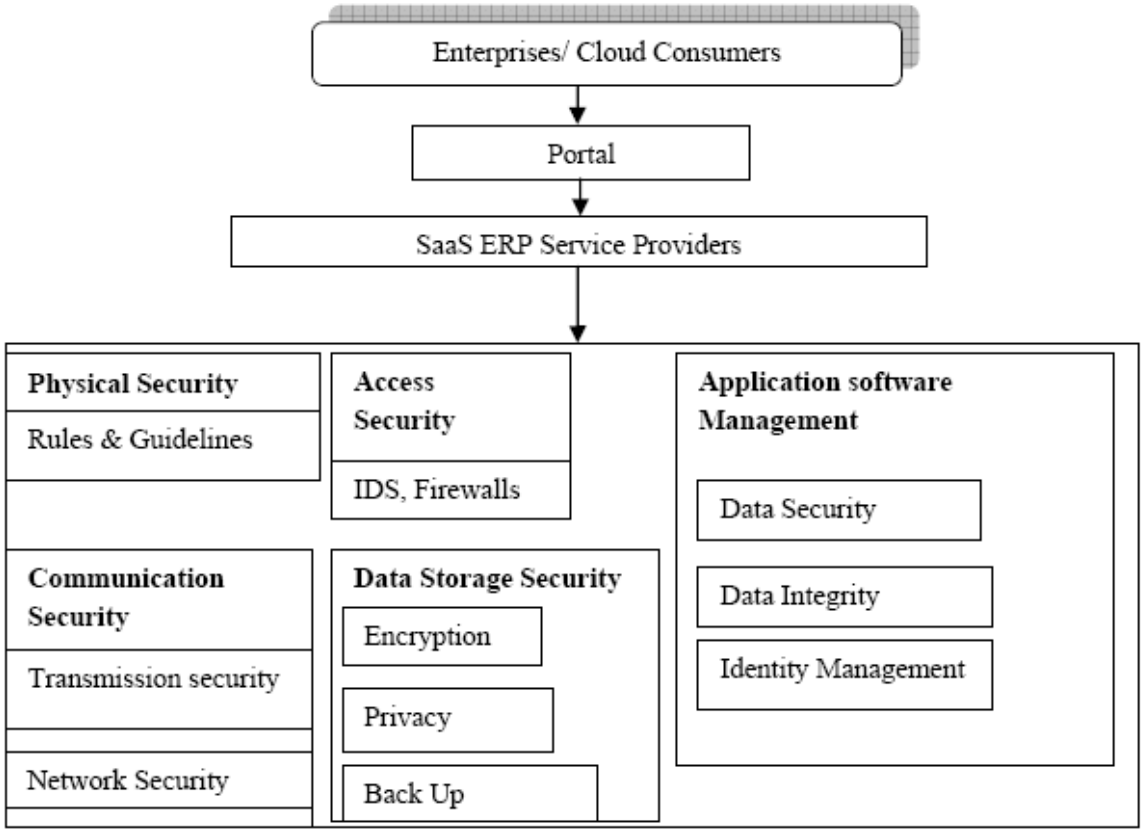

Fig 1. Proposed Security Framework for Cloud Based Enterprise Systems

5.1 *Physical Security Management Module:*

When an organization has its application running in an external cloud, the physical environment is off premise. A violation to physical security means that an unauthorized user with malicious intent has physical access to the hardware where either the application is running or data is stored. The physical security component must define and enforce rules of conduct and social guidelines for employees and have mechanisms to ensure that the rules are being adhered to. Also the component must include the solutions for disaster recovery.

5.2 *Data Storage Security Management Module:*

When ERP data is accessed by users, the business logic available in the system must ensure that only authorized users are able to access the data and that there is clear segregation of data stored by different users. The system also has a provision for backing up the data to aid in instances of disaster recovery. To carry out its tasks, the module may include the following three components:

5.2.1 *Encryption Component*: Sensitive data should be encrypted when it rests in the database or in a file system. This prevents direct access to data and ensures that all accesses are filtered by the application logic. The encryption component can use the public-key or private-key encryption techniques to secure the sensitive data resting in the cloud. The component should also include the business logic to ensure that if there is any required data indexing, then it is not broken in the encryption process. The encryption and decryption process creates processing overhead and hence non-sensitive data should be stored in the clear to minimize costs.
5.2.2 *Privacy Component*: One of the major characteristics of cloud computing that has led to its acceptance is multi-tenancy which permits multiple users to simultaneously store their data in the same location using the applications provided by SaaS. In such a situation, intrusion of data of one user by another user becomes possible. This intrusion can be done by exploiting the loop holes in the application such as vulnerable virtual machine images or by injecting client code into the SaaS system. The Privacy component should therefore ensure a clear boundary for each user's data [Subashini and Kavitha , (2010)].
5.2.3 *Backup Component:* In a cloud based enterprise system, the SaaS vendor needs to ensure that all data owned by a particular enterprise is backed up on a periodical basis which can be of use in disaster recovery. The component can further secure the backed up data by storing it in an encrypted form which prevents accidental leakage of sensitive information.

5.3 ***Access Security Management Module:***
Access security violations can happen from internal as well as external sources. Internal access Security is required to prevent illegal users from accessing resources and sending unauthorized queries to servers. The lack of proper implementation of access security could impact the availability of an application by authorized users such as in the case of a Denial of Service (DoS) attack. The access security module should have an Intrusion Detection Mechanism (IDS) to guard against such attacks. The module should have various perimeter security devices such as firewalls and must ensure that the various security policies put forward by the organization are incorporated and adhered to.

5.4 ***Application Software Management Module****:*
This module contains the business logic that ensures the security and integrity of data. The module also includes mechanisms for authenticating the users for providing services. The business logic included in the module also does the task of identity management. The various components of the module include:

5.4.1 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)]
5.4.2 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.
5.4.3 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.

5.5. ***Communication Management Module:***

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.

5.5.1 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.

5.5.2 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. 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. Security challenges faced by cloud based systems needs to be addressed for the successful implementation of SaaS enterprise systems. A security framework has been designed for providing better security for cloud based enterprise systems. The proposed framework tries to address the security issues faced by SaaS based system.

References

[1] Almorsy et al. (2011). Collaboration-Based cloud Computing Security Management Framework. Conference proceedings of IEEE International conference on Cloud computing (CLOUD 2011), Washington DC, USA 99

[2] Bhadauria et al., " A survey on Security Issues in Cloud Computing", arXiv:1109.5388v1

[3] Bingi, P et al., "Critical issues affecting an ERP implementation", *Information Systems Management*,:Vol. 16, P.7, Summer 1999]

[4] Djohnson, "Security Issues in Cloud ERP," October 6, 2011. http://erpcloudnews.com/2011/10/security-issues-in-cloud-erp/

[5] Goel et al., (2011) , "Impact of cloud Computing on ERP implementations in Higher Education", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.2, No.6, 2011

[6] Gulla, J.A (2004), Introduction to Enterprise Systems, Norwegian University of Science and Technology Trondheim, Norway ,white paper, 2004.

[7] Haigh, D. (2004). Enterprise Resource Planning. The Pennsylvania State University

[8] Hayes (2008), Cloud Computing.Commun. ACM 51, 7(July 2008), 9 – 11

[9] Kimberling, E. Top ten ERP software predicts for 2011. Panorama Consulting group [online]. http://Panorama-consulting.com/top-ten-erp-software-predictions-for-2011].

[10] Mall and Grance (2009) "The NIST Definition of Cloud Computing," version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory (http://csrc.nist.gov/publications/nistpubs/800-145/sp800-145.pdf)

[11] Marnewick, C. and Labuschagne, L. (2005). "A security framework for an ERP system". Conference proceedings of the Information Security South Africa. Conducted by ISSA. Johannesburg: ISSA.

[12] Moon (2008), "Are the Rewards of ERP systems Worth the Risk" http://www.techrepublic.com/blog/tech-news/are-the-rewards-of-erp-systems-worth-the-risk/2133

[13] Rich (2010), "ERP and Cloud Computing trends", January 28, 2010 http://www.erp.com/section-layout/51-erp-success-stories/5674-erp-and-cloud-computing-trends.html

[14] Savage., "Cloud application security issues and Considerations," April 20, 2011 http://searchcloudsecurity.techtarget.com/news/2240034925/Cloud-application-security-issues-and-considerations

[15] Seddon, P.B et al., "A multi-project model of Key factors affecting organizational benefits from enterprise systems, "MIS Quarterly, Vol.34, P.305, Jun 2010

[16] Subashini, S and Kavitha, V (2010), "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, ,no.1, pp. 1 -11, 2010.

[17] Takabi, H etal., (2010), "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments", in 2010 IEEE 34th Annual Computer Software and Application Conference Workshops, July 2010.