Chapter 10
Enterprise Security Framework for Enterprise Cloud Data Centres

Muthu Ramachandran
Leeds Beckett University, UK

ABSTRACT

Enterprise security is the key to achieve global information security in business and organisations. Enterprise Cloud computing is a new paradigm for that enterprise where businesses need to be secured. However, this new trend needs to be more systematic with respect to Enterprise Cloud security. This chapter has developed a framework for enterprise security to analyze and model Enterprise Cloud organisational security of the Enterprise Cloud and its data. In particular, Enterprise Cloud data & Enterprise Cloud storage technologies (Amazon s3, Drop Box, Google Drive, etc.) have now become a normal practice for almost every computing user's. Therefore, building trust for Enterprise Cloud users should be the one of the main focuses of Enterprise Cloud computing research. This chapter has developed a framework for enterprises which comprises of two models of businesses: Enterprise Cloud provider enterprise model and Enterprise Cloud consumer enterprise model.

INTRODUCTION

Enterprise Cloud computing technology has emerged to provide a more cost effective solution to businesses and services while making use of inexpensive computing solutions which combines pervasive, internet, and virtualisation technologies. Enterprise Cloud computing has spread to catch up with another technological evolution as we have witnessed internet technology, which has revolutionised communication and information superhighway. Enterprise Cloud computing is emerging rapidly and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to software engineering and its related processes. For example, current challenges that are faced with cyber security and application security flaws, lessons learned and best practices can be adopted. Similarly, as the demand for Enterprise Cloud services increases and so increased importance

DOI: 10.4018/978-1-5225-8176-5.ch010

sought for security and privacy. The business of Enterprise Cloud technology can only be sustained if we can maintain balance between demand for services in-line with improved Enterprise Cloud security and privacy. Popović & Hocenski (2010) have reported an analysis of results from an IDC ranking of security challenges that 87.5% responded to demand for Enterprise Cloud security against on-demand Enterprise Cloud services. This confirms the importance of Enterprise Cloud security against Enterprise Cloud services.

Enterprise Cloud service providers such as Microsoft, Google, Sales force.com, Amazon, GoGrid are able to leverage Enterprise Cloud technology with pay-per-use business model with on-demand elasticity by which resources can be expended or shortened based on service requirements. They often try to co-locate their servers in order to save cost. There every effort by several other enterprises to establish their Enterprise Cloud efforts to build their own Enterprise Cloud (private Enterprise Clouds) on their premises but can't afford to compromise security of their applications and data which is their major hurdle in their new effort. Most important of all, they need to develop a legitimate and controlled way of establishing service-level-agreements with their clients and to embed these rules to be built-in with services.

Standardisation has been active in software development and information technology to ensure systematic use of process, methods, and to that of client's requirements. Standards include on Quality, Quality of Services (QoS), Usability, and Process such as ISO, CMMI, and others to ensure product and service quality are adhered. The emergence and adherence of standardization such as Information Technology Infrastructure Library (ITIL), ISO/IEC 27001/27002, and Open Virtualization Format (OVF 2010) are critical in establishing expected Enterprise Cloud sustainability and trust in this new technological service business. Hence, it is highly recommended OVF standard as a vendor and platform independent, open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines (software stacks that incorporates the target applications, libraries, services, configuration, relevant data, and operating enterprise).

This paper proposes two tier enterprises for Enterprise Cloud computing: Enterprise Cloud provider as an enterprise and an Enterprise Cloud consumer as an enterprise. This will allow us to apply best practice security measures, principles, and frameworks. This chapter addresses some of the key research issues in this area such as how do we learn and adopt a decade of best practices on enterprise security to Enterprise Cloud technology transition? How we can also improve and sustain Enterprise Cloud enterprise security framework continuously?

BACKGROUND

Enterprises Engineering incorporates a systematic and comprehensive approach to modelling, designing, and developing enterprises includes software and service based enterprises. Caminao project (2013) provides a comprehensive framework for enterprises engineering methods and concepts. The internet technology has revolutionized the way we live on a daily basis. The use of internet is growing rapidly from devices, appliances and Enterprise Cloud computing, which has emerged to address a cost-effective solution for businesses. However, security is the most common security concerns of all. Therefore, security for Enterprise Cloud computing is the main aim of this chapter. The everyday Enterprise Cloud applications and apps can be protected using commonly available anti-security software packages. However, it is harder to protect us from security related attacks which emerges unexpectedly and are often hard