Chapter 41
Better Security and Encryption Within Cloud Computing Systems

K. Y. B. Williams
Walden University, USA

Jimmy A. G. Griffin
NETE Solutions, USA

ABSTRACT

Better security and encryption is necessary with regard to all forms of Cloud Computing, Cloud Infrastructure, and Cloud Storage. Areas that are affected the hardest by security breaches include: retail/e-commerce, communications, transportation, and banking. Illustrated within this article are ways that companies such as Walmart, Verizon, Wells-Fargo, and BWM would be affected by a lapse in security and/or a breach in their Cloud Infrastructure. In this article issues that can magnify these breaches and data loss is discussed as it relates to Cloud Structure and Cloud Services based on known vulnerabilities and lack of product testing. This article concludes with why it is necessary to have Public Policies as part of the governing system on Cloud Computing, Cloud Infrastructure, and Cloud Storage

INTRODUCTION

Security has always been an issue with any type of new innovation. Whether securing the information, technology, design details, or schematics of the newly developed innovation (from the public) before initial release to the public, to securing the new innovation, technology, design details, schematics, and/or information once it has been released, to securing the next updates and improvements on existing technology and improvements on the technology, security at each stage of development is necessary and important. With any lapse of security at any of these stages the results can range from financial loss to loss of intellectual property as a whole. It is not surprising that any lapse in security on any of these levels will result in law suits from one company claiming another company had infringed upon their intellectual property, trade secrets, or may have engaged in espionage (corporate and/or cyber) to gain

DOI: 10.4018/978-1-5225-8176-5.ch041

an advantage that they could only have gotten from looking at the existing or new technology from the company and/or from the company's prior innovations, design details, schematics, and/or proprietary information. Therefore, it is imperative that security measures are built into ever level of the process: from design to production, and even after the technology is obsolete.

Once the technology is considered obsolete, it is usually decommissioned, even if the technology has been decommissioned, the need for storage of that information in the form of Data Storage is still needed. An old design can still produce a wealth of information on how to improve on the existing technology, and also on how to think about new forms of innovation based off older designs. Therefore, securing the designs is important, as the designs and design concepts can lead to new ideas and lead to new innovations, and these new innovations can result in new forms of technology based on one concept (resulting in intellectual property). Therefore, security at the storage level is just as important as securing the designs of the developed technology and when transporting the information to/from/and within the data storage facility.

When transporting information from one facility to another, any and all researchers will state that once the amount of data reaches a certain level, it becomes necessary to move large volumes of data via external hard drives as communication networks and file transfer protocols will be slowed based on the sheer volume of data. Although it is possible to send the data via a secured network, the reliability that all the data will be captured and received within a reasonable and suitable timeframe may be a concern for any company that is transmitting any proprietary form of technology. Therefore, encryption of the information when in transit is essential, whether via network transport over a secured system connection or via external hard drive.

Encryption has become the solution for many security issues as it has advantages that allows the user of the system to get around various security issues that can be found within computing systems, and within the products that they are used on a daily basis. However, it is not impossible to get the information once it is encrypted, but it does make it more difficult to get to the actual information once it is encrypted. By using encryption methods, it allows the company, security team, system administration, and user to have a sense of feeling protected and viewing the data as being unreadable and possibly "irretrievable" in an encrypted form. However, encryptions can be broken and the information can be retrieved given enough skill, computing time, and processers.

Therefore, better security and encryption methods is necessary at all stages of development and in the processing, transport, and storage of information within all forms of computing systems especially on-demand systems such as Cloud Systems.

Within this article, a discussion on security, encryption, and how to improve on the current forms of security and encryption is discussed. Within this article, it will be necessary to look at some of the major companies in various markets to illustrate, discuss, and speculate on the effect that an unwanted intrusion would have on the company. The discussion and speculation will focus on: the reputation of the company, customer base, and their system design if their systems were penetrated. For illustrative purposes, the companies that will be used include: Walmart, Verizon, Wells Fargo and BMW. In the illustrations, the view point that will be used is based on the vulnerabilities that exists within the infrastructure of Cloud Systems.