View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Sheffield Hallam University Research Archive

# Secure Information Systems in the Age of Cloud Computing

**Marcos A Rodrigues**

GMPR-Geometric Modelling and Pattern Recognition Group

Sheffield Hallam University, Sheffield, UK

m.rodrigues@shu.ac.uk

Recent revelations by Edward Snowden speak volumes about the need to protect sensitive data to comply with privacy regulations worldwide. The Cloud Computing paradigm in which servers, storage and applications are delivered to an organization's computers and devices through the Internet is here to stay. The benefits of this mode is that it enables data centres to be accessed and shared as virtual resources in a secure and scalable manner. For businesses, this is a very attractive model as services can expand or shrink as needs change. For information systems stored in the cloud to comply with EU data protection and privacy regulations, both the stored data and the connection between provider and customer need to be adequately protected against all known security risks. Recent reports indicate that 82% of cloud providers encrypt data in transit, protecting against man-in-the-middle attacks as data are transmitted. However, only 9.4% of cloud providers encrypt data once stored in the cloud, for file sharing convenience. This is a serious issue leaving the cloud vulnerable to data breaches and unauthorized access. In this paper, we will review security threats to cloud computing and present a solution based on our unique patented compression-encryption method. We focus on threat prevention through cryptographic methods that, when properly implemented, are virtually impossible to break directly. Our solution compresses data in a unique way tackling security, performance, data protection, privacy and cost issues. A unique, data-dependent symmetric key is generated as a side effect to the compression method. Without the key, the data cannot be decompressed. It is also important to realise that not all data in the cloud need to be encrypted, and not all data should be encrypted in the same way. For instance, images and video may be encrypted by a lossy method while text and other documents need to be lossless. Our algorithms cover both lossless and lossy requirements giving the user full control over what and where it is compressed-encrypted, either at the local machine or in the cloud. We highlight the benefits of the solution concerning less bandwidth requirements, faster data transmission and response times, less storage space, and less energy consumption. Finally, we consider that data protection and privacy legislations are not similar across the globe. It is demonstrated that our solution addresses security and privacy concerns according to current European legislation on data protection whether the servers are located or not in the EU.