Cloud Data Security and Data Leakage Prevention

Selton Pratheesh Regis

A dissertation submitted in partial fulfilment of the requirement for
Master of Science in Cyber Security and Forensics

Department of Computing
Informatics Institute of Technology, Sri Lanka
in collaboration with
University of Westminster, UK

2020

Abstract

Information Technology is growing exponentially and in this fast-growing technology and faster Internet of things (IOT), data processing devices are being introduced. Data has become an indispensable part of our daily lives in this information age. A mobile application now even handles high processing information software and small microchips can store the complete data of an organization. Therefore, the amount of data which is generated is growing exponentially due to high technological advances. With Internet of things, cloud data security become a question. The survival of many organizations depends on preventing these data from falling into the wrong hands as it could cause serious consequences.

In technology evaluation, cloud computing is the base for IOT and the model in which computing resources such as software, hardware and data are delivered as a service through the internet. In this fast-growing cloud environment, maintaining the security of data is highly important as a small loss in data might create a critical impact in the organization. Hence, preventing the loss of sensitive data became the greatest challenge. Usually organizations implemented methods like framing policies in an organization, implementing control network devices and servers and also endpoints, but still these methods started lagging as technology developed the methodology of data leakage and data theft which attained heights.

Hence, there was a requirement for some system which could prevent the leakage of data in the cloud and this could be done with the help of the cloud access security broker (CASB) or the Data Leakage Prevention system (DLPs). These systems are capable of detecting leakage in data at main states, namely, Data in rest, Data in transit and Data in use, which increase the need of the requirement but still there are some technical gaps we see in this data prevention solution .
With the help of theoretical research this document briefly explains about the various DLPs available, their limitations, providing information about the gaps in security, providing enough awareness to the developers' framework as well as to researchers and professionals for developing a next generation DLP which is capable of cloud data leakage prevention that would be highly beneficial to cloud security.

Keywords: *Data leakage prevention (DLP), Cloud data security, Cloud access security broker (CASB)*