CERIAS

The Center for Education and Research in Information Assurance and Security

Confidentiality Guidelines for Cloud Storage

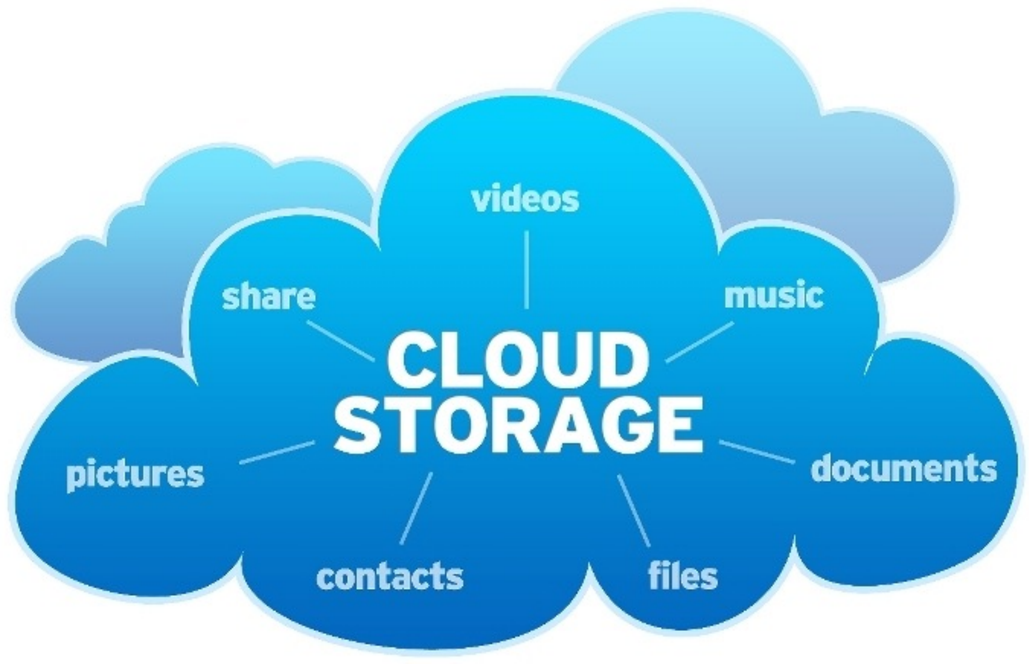
Joseph Beckman, Matthew Riedle, Hans Vargas

beckmanj, mriedle, hvargas [@purdue.edu]

Prof. Brandeis Marshall

ABSTRACT

As cloud computing is becoming more popular among the average user, and even governments, the question arises of how secure is the data stored in the cloud. Guidelines have been established by FedRAMP that evaluate certain security protocols for cloud providers like Google Drive and Amazon Web Services. This project will examine the confidentiality and access control guidelines for Amazon's S3 data storage, and will check if they are sufficient for current and future markets.



PREVIOUS WORK:

Fall2012 NSA sponsored class: 'Unclassified' problems. Public Cloud Providers: Security Controls to address Risk (Amazon, Microsoft, Google). There is a variety of resources in the form of research papers, book chapters, and other publications that address general concepts related to cloud security, some others are related to Confidentiality or authentication within the IaaS model, and there are a few related specifically to Amazon as our CSP. The lack of abundant material related to our research is challenging, but also a great opportunity to further explore.

PURPOSE:

The aim of this project is to bring a greater level of security to information and processes performed in the cloud. Increasing the level of security in the cloud is an important act to the field of information security, and to anyone who uses cloud services. Measuring the impact of this project might be difficult to quantify, but nevertheless we know that it is a relevant issue for a fast growing sector of cloud customers.

EXPECTATIONS:

The project seeks to produce the following solutions:

1. Evaluation of the confidentiality of Amazon S3 cloud service against a wider range of security control guidelines.
2. Suggestions for the improvement of security within the S3 cloud services with regard to the Confidentiality in a IaaS framework.
3. Based on our evaluation of the S3 cloud services, produce a list of recommendations to improve information security practices for cloud services.

OUTCOMES:

Report containing the following sections:

1. Description of the evaluation methods of Amazon S3 services with reference to the FedRAMP guidelines which relate to Confidentiality.
2. Report of results from evaluation and testing of Amazon S3 against FedRAMP guidelines.
3. Present suggested guideline improvements towards better cloud services security for Amazon S3.

FUTURE WORK:

- Confidentiality is only one aspect of information security. Future research directions may include analysis of the integrity and availability aspects
- Research into the confidentiality, integrity, and availability of other aspects of cloud services such as Software as a Service (SaaS), and Platform as a Service (PaaS).
- Research possibilities also exist regarding the efficacy of the application of FedRAMP guidelines to specific needs of individual United States federal, state, and local agencies.

PURDUE UNIVERSITY