

**MASTER'S PROJECT (SUMMER 2016)**

**TOPIC:** *Protecting Data Security and Confidentiality Using Nonlinear Distribution of Cloud Data at Multiple Clouds*

**PRESENTOR:** Vishal Sarode

**ADVISOR:** Dr. Haiping Xu

**DATE & TIME:** Tuesday, August 30, 2016, 1:00 PM

**LOCATION:** Dion 305

**COMMITTEE MEMBERS:** Dr. Iren Valova and Dr. Shelley Zhang

**ABSTRACT**

Cloud services have been widely used for data storage and backup due to their low cost and high availability. However, there are many major concerns while using cloud services for data storage, such as data security, confidentiality and authenticity, as cloud services may be compromised either internally or by cloud hackers. Those issues become very serious when the data contains critical information such as personal information, medical data, or credit card information. In this project, we developed a prototype application to distribute data at multiple clouds for data security. In our approach, we label the data bytes in a block of data using finite numbers, which are considered a finite field called a Galois Field. Then we apply the logarithm function over the Galois Field to shuffle data bytes in each of the data blocks of a user file. After the data shuffling, the user data can be nonlinearly distributed at multiple clouds. When the user data are retrieved from the clouds, the inverse logarithm function over the Galois Field is applied to restore the original user file. With this mechanism, the contents of the user file can be properly protected, and no particular cloud service provider can understand the data content. Comparing with traditional encryption mechanism, this approach provides a simpler and much more efficient way for hiding data contents from cloud service providers. To demonstrate the feasibility of our approach, we use existing cloud services, such as Amazon S3 and Dropbox to simulate multiple clouds. The experimental result shows that user data can be efficiently distributed at multiple clouds and the intended data security can be properly achieved.