Privacy-Preserving Cloud, Email and Password Systems

Scott Russell's Problem Statement

October 10, 2017

Project Team:
Scott Russell
Scott Merrill
Andrew Ekstedt
Andrew (TA)

Cleint:
Attila Yavuz
Thang Hoang (Client TA)

Class: CS 461 (Fall 2017)

Date of Change: October 10, 2017

Version: 1.0

Abstract:

Searchable Encryption is a powerful way to allow databases to be stored on the cloud while still having secure access by users. Currently algorithms to process searchable encryption are very slow, such as Oblivious RAM (ORAM) and Fully Homomorphic Encryption. They provide excellent security but lack the efficiency that any large Cloud system would require. This project focuses on researching Dynamic Searchable Symmetric Encryption (DSSE) through papers and abstracts of our client, Atilla Yavuz, as well as other key researchers in this field. After having a strong grasp on DSSE through these papers we will implement our own Searchable Encryption Algorithm. Work done by David Cash will provide a strong basis for our understanding of DSSE. Evaluation of DSSE is based on a few key factors including Performance, Security, and Correctness. (Specific parameters for evaluation will be added as details of metrics are discussed with client) Using our implementation of a DSSE we will set up a cloud database server, an email client as well as an ORAM password-manager. This project is heavily focused on the research aspect of DSSE and deadlines for specific implementations will change dynamically based on our progress.

Introduction to Project:

The challenge between privacy and data utilization; this is the dilemma of trying to achieve Dynamic Searchable Symmetric Encryption. With data being outsourced to storage on the cloud how can we, as developers, guarantee the same level of encryption and security while obtaining efficiency and speeds that our clients want. The motivation behind the use of cloud storage is twofold. Firstly, the need for global access. As communication and networking between companies becomes more digital, rather than physical, there is a need for data to be accessible by multiple parties quickly and securely. This is where Yavuz, along with other key researchers, come into play. Over the past few years Attila Yavuz has implemented a new DSSE scheme that achieves this. privacy-preserving data outsourcing for computing clouds Our scheme achieves these desirable properties with a very simple data structure that enables efficient yet secure search/update operations on it. [1]. The objective of this project is to establish our own DSSE scheme based on the research of David Cash. After we will use this scheme to create an email server where we can test the efficiency and usability of our DSSE. Finally, we will create a password manager using this encrypted data cloud structure. This project will involve a heavy use of research of previous implementations of DSSE to inform our team about the specifics of the process.

Problems with current Security on Cloud Databases:

Security is the primary concern with the implementation of this project. There are currently faster cloud storage implementations but not with the ability to carry out this searchable encryption. There are tested and strong forms of encryption, for example we could use an AES Block Cipher to encrypt the data on the Cloud. The problem comes when we want to query and get data back from the cloud. Standard encryption would not allow the user to search for a file, since even with the same name sending two separate signals to the server will have completely different hashes and direct comparison will not be feasible. Professor Boldyreva explains the difficulties of current security schemes in her presentation Introduction to Searchable Encryption [2]. Specifically, we want to preform searches on a database that are faster than a linear search. If we must do a linear search on the data base it will take an extremely long time to get any queries back from the Cloud, especially with the massive scale that cloud storage can obtain. There are existing solutions to this idea of searchable encryption such as Oblivious RAM and Fully Homomorphic Encryption. In these methods, we have the security strength that we are looking for but lack the efficiency that we want for any modern Searchable Encryption scheme.

Conclusion:

From researching what is currently available in the market we can create a searchable encryption scheme with sound security, however we are lacking the efficiency and speed that any modern system with a huge database would need to run in any applicable manner. This is the foundation for this project. To research current solutions for DSSE, specifically that of David Cash, and then implement our own. Metrics for success are based on using sound security principles as well as specific efficiency benchmarks. Finally, we will apply our implementation to an email service and a password-manager service. With time permitting we will improve the usability of our implementation through a UI.

References:

[1]. A. A. Yavuz, Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware, pp. 122, 2015.

[2]. Alexandra Boldyreva, Order-Preserving Encryption, Georgia Tech, January 2016.