Problem Statement: Privacy-Preserving Cloud, Email, and Password Systems

Scott Merrill

October 10, 2017

Cloud-based storage services have become a necessity in a world where the demand for cell phones is smaller, faster, and larger storage capabilities. Using the cloud instead of physical space on the system frees up space for data and programs that cannot be stored on the cloud. The major concern with this is privacy. Not all cloud based servers are to be trusted with recent news like the hack on Yahoo to reinforce the point. Basic encryption techniques can be used to prevent these sorts of attacks on personal data, but makes it impossible for users to send queries into the data. Searchable encryption data techniques can help to prevent this and allow users to send queries, such as searching, to the data, without the data being viewable by external sources.

Having your data encrypted so that a sever or anyone who can gain access to a server is one way to prevent your data from being taken against your will. Unfortunately, there are some major drawbacks to encrypted data. Inherently encrypted data is unable to be read, this prevents the user from doing queries like search or sort operation on the data. Dynamically Searchable Symmetric Encryption (DSSE) tries to solve this problem. DSSE schemes are designed to allow the user to access this data and search on it by creating a data structure (liked a hash table) to link encrypted keywords to associated encrypted files. This data has already been created, but there are significant tradeoffs. Performing these data queries takes much more time than a normal search and the data structures used to create the relationship between encrypted keywords and encrypted files can be large.

The goal of this project is to implement these data schemes (specifically David Cashs DSSE scheme) on structures such as: Cloud-based systems, Email servers, and Password Managers and discover if they can be used at a consumer level. Metrics used to determine success of these implementations include:

- Correctness - being able to reliably search for keywords contained in files and deliver these results to the user.
- Efficiency - optimize implementation to reduce the amount of time (measured in ms) it takes to perform queries on the system.

- Usability - Determine if the data queries are efficient enough to be used at the consumer level for each of the different structures: Cloud-based systems, Email serves, and Password managers.

Searchable encryption on cloud based systems such as Google Drive, DropBox, etc., is important to protect your sensitive data. By using DDSE schemes we hope to be able to implement a service where a user can encrypt and upload their files and then be able to fetch back the location of files when searched for with specific keywords. This is a privacy vs. utilization problem as the fetch time needs to be quick enough that it is usable by the consumer as well as efficient enough to support scaling so that the severs can support this server on multiple clients.

Almost everyone uses email for both important and mundane tasks. As it stands right now these email services can access and read your data on the servers that they provide. This may not be a concern for you with some data, but sensitive personal emails and private corporate information correspondence may be something you do not want others to have access to. The solution to that now is to encrypt the entire files and then to decrypt them when needed. This is entirely inefficient and is not only slow by also very resource intensive. By implementing a DSSE scheme we hope to be able to maintain the security that encryption offers and allow the user to perform keyword search over those files in a more efficient manner.

Password managers are designed to help users remember password in a world where almost every digital service requires a user to have an account and a unique password to access their system. You want the password manager to protect not only the account and password, but also when you try to access them. Searchable encryption will allow you to do this and in the process, increase your privacy and the security of you data from potential adversaries.

Since this is a research project there will not necessarily be a product that we are developing to show for at the end. Instead we are more focused on the results we generate for our experiments and the implementation of our Dynamic Searchable Symmetric Encryption schemes on each of the different platforms.

What we hope to accomplish is: we will implement searchable encryption schemes, that we already developed, on a public cloud system, like Dropbox, Google drive, or amazon cloud; which will achieve higher performance than current implementations and that offers better security and is easy for users to implement. Develop a privacy-preserving email system on a public cloud system like, Google mail, which automatically crawls the personal emails from public an email provider, performs encryption and enables searchable encryption techniques on these encrypted emails. Develop a highly secure password management system, which stores a bunch of user passwords in an encrypted database and apply searchable encryption and ORAM techniques to retrieve the passwords on user request. All of these projects will be implemented as a system service that for a client-side application that interacts with a server-side system. Mobile and desktop versions should both be developed to test the usage of these services on the most commonly used platforms for the consumer.