Authors: Krutika Patel and An Thai

Computer Science Research

March 26, 2020

**Data Security Approach: Multi-factor Authentication and Scalability**

**Purpose**

Reconstruct a web application by creating a login page with Multi-Factor Authentication and protect client’s data by implementing hashing, encryption, and decryption methods.

**Current Practice**

In the last few years, we have seen an exponential influx in the use of internet based services. With massive amounts of data being generated and collected, comes the responsibility of properly handling user data. As of now most web pages are static and unencrypted. This makes it easier for attackers to access users’ personal information. By having username and password authentication as the sole verification method, we are allowing a gap for attackers to enter through a vulnerable website.

**Proposed Approach**

The approach to this research is to create a web application for users to login using multi-factor authentication and creating a secure database. As a result, there will be a reduction of successful attacks.

**Multifactor Authentication**

Having the ability to authenticate the identity of a user a second time, can be the tipping point that could stop a potential data breach. Multi-factor authentication (MFA) gives us this capability. Once a user signs on to their account, they will be asked to confirm their identity by providing a random token that is sent to their registered email once their credentials are verified. This allows for randomized instantaneous verification.

## **Protecting User Data**

By having functions that include encryption, decryption, and hashing, we are able to reduce the cost of violating privacy rights. Google Cloud instances and mysql databases are independent from one another. Thus, if attackers were planning to attack the system they would have to target both the system instance and mysql database in order to retrieve desired data.