PhD – Patient health Database

Fachgebiet: Informatik
Betreuer: Prof. Dr. Emmanuel Benoist
Experte: Prof. Dr. Andreas Spichiger

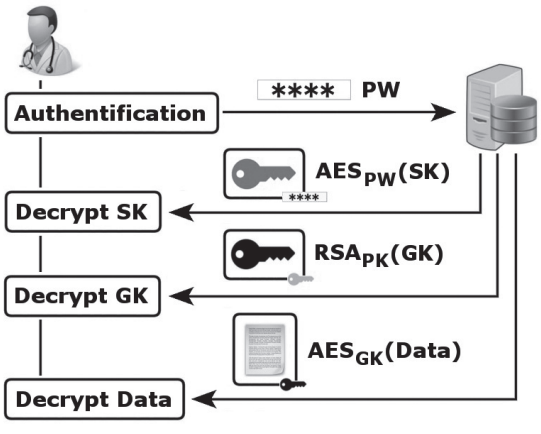
Damit die Qualität und Quantität von Behandlungen im medizinischen Bereich erfasst werden kann, werden Anwendungen entwickelt, welche die Behandlungsdaten von Patienten, z. T. in verschlüsselter Form abspeichern. Unsere Anwendung soll die Handhabung der Daten für die Doktoren vereinfachen, indem die verschlüsselten Daten benutzerübergreifend genutzt werden können. Ausserdem sollen die Behandlungsdaten für Statistiker in anonymisierter Form zugänglich gemacht werden können.

Einleitung

Mit unserer Arbeit wollen wir Handhabung von medizinischen Daten so vereinfachen, dass ein möglichst einfaches System entsteht, welches sicherheitstechnisch überzeugen kann und den Datenschutz der Patienten bewahrt. Um dies zu erreichen, haben wir eine auf JSF basierende Webapplikation entwickelt, in welcher die Behandlungsdaten aller Krankenhäuser in einem einzigen System erfasst und anschliessend weiterverarbeitet werden können. Die gespeicherten Daten bestehen aus den sensiblen Patientendaten, welche verschlüsselt werden müssen und nur den Doktoren zur Verfügung stehen und den Behandlungsdaten, welche unverschlüsselt bleiben und für statistische Zwecke genutzt werden können.

Konzept Datenverschlüsselung

Das Konzept der Datenverschlüsselung nutzt eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Jeder Benutzer besitzt einen Benutzernamen und ein Passwort für die Authentifizierung auf der Webseite. Dieses Passwort muss ausreichend stark sein, da es für die weitere Verschlüsselung von Nöten ist. Ausserdem bleibt es als Einziges im physischen Besitz des Benutzers. Weiterhin wird für jeden Doktor ein Schlüsselpaar erzeugt, bestehend aus einem Public Key und Private Key, wobei der Private Key mit dem Passwort des Doktors verschlüsselt wird. Bei der Kreation einer neuen Gruppe wird zusätzlich ein Group Key erzeugt, welcher zuständig ist für die Ver- und Entschlüsselung der Patientendaten. Der Group Key kann durch asymmetrische Verschlüsselung mit dem Public Key eines Doktors an diesen bzw. das System übertragen werden.



Verschlüsselungskonzept (PW=Passwort, PK=Public Key, SK=Secret Key, GK=Group Key)

Client side Encryption

Eine Schwierigkeit lag darin, bestimmte kryptografische Operationen auf den Clientcomputer zu verlagern. Da einige Daten in verschlüsselter Form vorliegen, können diese nicht direkt auf dem Client dargestellt werden, sondern müssen zuerst aufbereitet werden. Die Aufbereitung der Daten erfolgt in zwei Schritten. Zuerst werden die Daten mit dem Group Key entschlüsselt. Der erhaltene JSON String muss nach dem Entschlüsseln geparst werden, wobei die erhaltenen Key-Value Paare wieder den entsprechenden Feldern (Vorname, Nachname etc.) zugeordnet werden können. Sobald alle benötigten Felder vorhanden sind, können sie im Webbrowser dargestellt werden. Da die Patientendaten aus mehreren Teilen (Vorname, Nachname, etc.) bestehen, wurden diese beim Verschlüsseln erst in einen JSON String umgewandelt. Somit erspart man sich die Verschlüsselung jedes einzelnen Feldes und es wird lediglich eine Verschlüsselungsoperation pro Patient durchgeführt.

Patientendaten und Anonymisierung

Alle gespeicherten Fragebögen können von den Doktoren für die Behandlung eines Patienten ausgefüllt werden. Damit die Statistiker nur Zugang zu anonymisierte Daten erhalten, werden ihnen nur die Behandlungsdaten zur Verfügung gestellt, ohne die dazugehörigen Personalinformationen der Patienten. Eine enthaltene ID dient lediglich dazu, die Behandlungsdaten einer anonymen Person zuzuordnen. Die Zugänglichkeit der anonymisierten Behandlungsdaten erfolgt direkt auf der Webseite, wo sie als Ganzes in einem CSV Format heruntergeladen werden und anschliessend in andere Programme importiert und ausgewertet werden können.

Tino Kobler
+41 79 945 36 63
tinokobler@gmail.com

Michael Leiser
+41 78 843 29 04
michael.leiser@gmx.net