Implementasi Aplikasi Pembuat One Time Password (OTP) dengan Pemulihan dan Salinan Cadangan yang Terdesentralisasi = Implementation of a One Time Password (OTP) Generator Application With Recovery and Decentralized Backup

Prajna, author

Abstrak

Autentikasi multi faktor adalah upaya untuk memperkuat autentikasi. Saat ini, penggunaan one time password (OTP) masih menjadi salah satu faktor autentikasi yang digunakan pada aplikasi di Internet. Salah satu jenis OTP adalah yang dibuat menggunakan aplikasi yang dipasang pada perangkat pengguna. Aplikasi tersebut dibuat oleh banyak pengembang dan mengimplementasikan algoritma yang sama. Pada saat ini, yang banyak diimplementasikan adalah algoritma TOTP, yang membutuhkan sebuah kunci rahasia untuk membuat OTP. Apabila pengguna kehilangan perangkatnya, kunci rahasia tersebut tidak bisa diakses lagi dan pengguna berisiko kehilangan akses ke akun-akunnya karena OTP tidak bisa didapatkan kembali. Untuk mencegah hal tersebut, aplikasi-aplikasi di luar sana memiliki metode pemulihan. Namun, aplikasi-aplikasi tersebut menyimpan salinan cadangan pada peladen yang terpusat untuk mendukung pemulihan OTP. Selain cara tersebut, terdapat pendekatan lain untuk melakukan pemulihan dengan penyimpanan salinan cadangan yang terdesentralisasi yang diusulkan oleh Conor Gilsenan, Noura Alomar, Andrew Huang, dan Serge Egelman. Ide tersebut juga sudah diimplementasikan oleh mereka dalam aplikasi Blues 2FA. Namun, aplikasi tersebut belum dirilis ke masyarakat umum. Tugas akhir ini berisi implementasi versi penulis dari spesifikasi yang dibuat oleh mereka, serta analisis dan evaluasi terhadap implementasi tersebut.
.....Multi factor authentication is a way to make authentication more secure. One time password (OTP) is one of the commonly used multi factor authentication method on the Internet. Users can get OTP from an OTP generator application in their devices. There are many such applications out there, but they use one same algorithm to generate the OTP. Nowadays, the popular algorithm used by those applications is TOTP, which needs a secret key to generate OTP. If users lose their devices, then the secret key will also gone and they may not be able to access their account again because they cannot generate their OTP anymore. As a preventive measure, some applications offer recovery and backup methods with centralized backup. As an alternative, Conor Gilsenan, Noura Alomar, Andrew Huang, and Serge Egelman proposed an idea to make decentralized backup. They already developed an application with their method, named Blues 2FA. But, it is not publicly available yet. This work implements my own version of application based on the requirements from the previous work. Some analyses and evaluations about the implementation also shown in this work.