

ABSTRAKSI

Nama : Nizar
Program Studi : Teknik Informatika, FSTI, ISTN
Judul : Implementasi Sistem Registrasi Dengan Verifikasi Email Atau Token OTP Berbasis Android

Sistem login yang baik adalah sistem yang dapat mengamankan data pengguna dan mengetahui dengan benar apakah data pengguna itu benar adanya atau tidak. Karena dijamin sekarang ini banyak *tools* atau *software* yang bisa digunakan untuk mencari celah-celah password pengguna yang dilakukan oleh orang-orang yang tidak bertanggung jawab. Pada kesempatan kali ini penulis tertarik menerapkan tentang aplikasi login yang dapat memverifikasi data pengguna yang didaftarkan dan mengamankan password dengan *hash bcrypt* atau dengan token otp. Pada penelitian ini, penulis ingin membuat 2 pilihan login yang bisa dilakukan oleh pengguna. Yang pertama bisa dengan menggunakan email atau dengan nomor ponsel. Untuk pendaftaran data akun pengguna penulis membuat sistem verifikasi yang bisa dilakukan otomatis oleh sistem untuk membuktikan bahwa benar data tersebut yang diinputkan atau didaftarkan oleh pengguna. Lalu dengan keamanan password sistem login berbasis email ini penulis memanfaatkan fungsi *hash bcrypt* yang berada di password hash parameters *Firebase BaaS (Backend as a Service)*. *Bcrypt* adalah algoritma *hashing* satu arah yang berarti penyerang tidak dapat mengambil kata sandi teks biasa tanpa sudah mengetahui *salt* dan *password* itu sendiri. *Password hash parameters* disini digunakan untuk menyamarkan kata sandi pengguna didalam aplikasi yang saya buat. Didalam fungsi *hash bcrypt* ini juga terdapat *salt*, *salt* adalah data acak yang digunakan sebagai input tambahan untuk fungsi satu arah yang digunakan untuk *hash* data seperti kata sandi, atau data penting lainnya agar sulit di didekripsi. Pilihan login kedua yang dibuat penulis adalah dengan mengirimkan kode token otp bila pengguna ingin login dengan memasukan nomor ponselnya. Dengan penelitian ini penulis memberikan kesimpulan bahwa sistem login yang baik dapat memverifikasi data pengguna yang didaftarkan dan menjaga kerahasiaan password dengan fungsi *bcrypt* atau dengan token otp untuk menyulitkan penyerang

Kata Kunci : sistem login, *firebase*, *bcrypt*, *hash*, *salt*, kata sandi, token otp

ABSTRACT

*Name : Nizar,
Study Program : Informatics Engineering, FSTI, ISTN
Judul :Registration System Implementation With Android-Based Email
Or Token Verification*

A good login system is a system that can secure user data and know correctly whether the user's data is true or not. Because today there are many tools or software that can be used to find user password gaps that are carried out by irresponsible people. On this occasion the author is interested in applying about a login application that can verify user data that is registered and secure passwords by hashpt hashes or with otp tokens. In this study, the author wants to make 2 login options that can be done by users. The first can be by using email or by cellphone number. For the registration of user account data the author creates a verification system that can be done automatically by the system to prove that the data is actually entered or registered by the user. Then with the security of this e-mail-based login system password the author uses the bcrypt hash function which is the parameter hash parameter Firebase BaaS (Backend as a Service) password. Bcrypt is a one-way hashing algorithm which means the attacker cannot retrieve a plain text password without knowing the salt and password itself. Hash password parameters here are used to disguise the user's password in the application I made. In the bcrypt hash function there is also a salt, salt is random data that is used as an additional input for one-way functions used to "hash" a data such as a password (password), or other important data so that it is difficult to decrypt. The second login option that the author makes is to send an otp token code if the user wants to log in by entering his cellphone number. With this study the authors conclude that a good login system can verify user data registered and maintain password confidentiality with bcrypt functions or with otp tokens to make it difficult for attackers

Keywords: login system, bcrypt, hashing and salting, password, otp token