

PERANCANGAN SISTEM KEAMANAN APLIKASI PADA LEMARI BRANKAS DENGAN MENGGUNAKAN METODE OTP

DESIGN OF APPLICATION SECURITY SYSTEM ON SAFE CLOTHERS USING OTP METHOD

Aslam Afif¹, Tito Waluyo Purboyo², Randy Erfa Saputra³

^{1,2,3} Universitas Telkom, Bandung

aslamafif@student.telkomuniversity.ac.id¹, titowaluyo@telkomuniversity.ac.id², resaputraa@telkomuniversity.ac.id³

Abstrak

Tingkat kriminalitas yang cukup tinggi khususnya dalam pencurian uang mendorong adanya pembuatan alat yang disebut brankas. Brankas merupakan tempat penyimpanan yang dianggap praktis tetapi memiliki resiko yang tinggi, karena memungkinkan mudahnya brankas dibobol tanpa sepengetahuan pemiliknya.

Dengan adanya hal tersebut, maka diperlukan system keamanan aplikasi rangkaian berbasis mikrokontroler. Pada penelitian ini akan dibuat sebuah keamanan system aplikasi berbasis android untuk menunjang keamanan pada lemari brankas menggunakan metode OTP.

Berdasarkan hasil analisis dan pengujian yang telah dilakukan, sistem keamanan brankas pada penelitian ini dapat bekerja secara optimal. Aplikasi android yang digunakan dapat mempermudah pengguna untuk mengakses kode OTP yang telah dikirim. Metode OTP (*One Time Password*) yang digunakan pada penelitian cocok untuk digunakan pada lemari brankas pada saat ini, sehingga dapat menambah sistem keamanan yang ada.

Kata Kunci: *OTP (one time password), mobile applications, ESP8266.*

Abstract

The high level of criminality, especially in the theft of money, encourages the manufacture of a tool called a safe. Safe is a storage place that is considered practical but has a high risk, because it allows the safe to be broken into without the knowledge of the owner.

With this in mind, a microcontroller-based circuit application security system is needed. In this study, an Android-based application system security will be made to support security in safe cabinets using the OTP method.

Based on the results of the analysis and testing that has been done, the safe system in this study can work optimally. The android application used can make it easier for users to access the OTP code that has been sent. The OTP (One Time Password) method used in this study is suitable for use in safe cabinets at this time, so that it can add to the existing security system.

Keywords: *Blockchain, KIR, Smart Contract, IoT.*

1. Pendahuluan

1.1 Latar Belakang

Pencurian merupakan suatu tindakan kejahatan yang seringkali terjadi di masyarakat khususnya pada lemari Brankas. Maraknya pencurian yang terjadi menimbulkan keresahan bagi para penggunanya. Keresahan yang muncul bukan tanpa alasan, hal ini disebabkan oleh intensitas tindakan kejahatan pencurian yang begitu tinggi. Kejahatan yang berkembang di masyarakat itu dapat terjadi di mana saja, kapan saja, dan dalam bentuk atau jenis kejahatan yang beragam, dan dilatarbelakangi oleh faktor-faktor yang memiliki keterkaitan dengan tempat, waktu dan jenis kejahatan tersebut.

Brankas adalah suatu tempat yang disediakan untuk menyimpan suatu benda yang berharga seperti dokumen penting, perhiasan, uang dan barang berharga lainnya. Pada saat ini brankas masih menggunakan sistem penguncian semi otomatis yaitu dengan menggunakan kunci kombinasi.

Penggunaan kunci kombinasi kurang efisien karena pengguna brankas mudah lupa pin dari kunci kombinasi brankas serta kunci kombinasi juga mudah dibobol oleh pencuri.

Dengan adanya hal tersebut, maka diperlukan aplikasi rangkaian berbasis mikrokontroler. Pada penelitian akan dibuat sebuah sistem keamanan buka tutup kunci brankas menggunakan Node MCU yang terkoneksi dengan ESP8266. Sistem ini dibuat dengan menggunakan metode OTP (*one time password*) pada *Mobile Application*. Serta fitur tambahan yang akan dibuat pada brankas.

1.2 Rumusan Masalah

Permasalahan yang menjadi objek pada penelitian ini adalah sistem pengunci apakah yang cocok digunakan pada lemari brankas pada saat ini dan bagaimana membuat kunci pengamanan pada lemari brankas berbasis *Mobile Application* ?

1.3 Batasan Masalah

Dalam memfokuskan penelitian Tugas Akhir ini, maka diberikan beberapa batasan masalah sebagai berikut: Node MCU yang terkoneksi dengan ESP8266 yang dipasangkan pada lemari brankas akan disambungkan dengan sistem android. Aplikasi melakukan kontrol dan monitoring terhadap brankas sebagai keamanan brankas. Target sasaran untuk perusahaan yang mempunyai dokumen penting berbentuk *Hard copy* yang harus disimpan secara aman.

1.4 Tujuan

Berikut merupakan beberapa tujuan yang mendasari dilakukannya penelitian ini, antara lain: Lebih meyakinkan pengguna bahwa metode OTP (*One Time Password*) pada *Mobile Application* dapat meningkatkan sistem keamanan pada lemari brankas. Serta mampu meningkatkan sistem keamanan pada lemari brankas.

2. Dasar Teori

2.1 Internet Of Things

Teknologi *Internet of Things* (IoT) termasuk salah satu perkembangan terbaru dalam dunia teknologi, namun perkembangannya relatif cepat. *ABI Research* memprediksi bahwa di tahun 2026, koneksi dan teknologi berbasis IoT akan melebihi 23 milyar koneksi jumlahnya dengan pasar-pasar IoT yang terus berkembang pesat. (*ABI Research*, 2020). Dengan berkembangnya bidang teknologi ini, kita diperhadapkan dengan tantangan untuk mengamankan servis-servis IoT dari serangan siber (*cyber-threats*), yang tentunya juga ikut berevolusi seiring dengan bertambahnya kecanggihan dan kompleksitas IoT.

Salah satu tantangan terbesar untuk menghadapi berkembangnya IoT adalah bagaimana mengembangkan opsi-opsi sekuritas digital untuk memproteksi servis-servis dan aset-aset yang terhubung dengan IoT, terutama dengan prediksi bahwa servis IoT yang berhubungan dengan autentikasi dan sekuritas digital lainnya akan menjadi bisnis yang menghasilkan untung US\$8.4 milyar di tahun 2026. *Value chain* dari sebuah bisnis keamanan dan autentikasi IoT dapat memanfaatkan layanan-layanan seperti penerbitan identitas IoT, penyedia layanan IoT (*provisioning*), autentikasi, management kunci enkripsi *lifecycle*, management akses, dan pembuktian digital (*attestation*). Layanan-layanan ini merupakan bentuk masa depan dari model-model monetisasi IoT.

Oleh karena bahaya-bahaya yang bisa ditimbulkan dari kurangnya keamanan perkembangan teknologi IoT, maka salah satu cara terbaik untuk meningkatkan keamanan adalah dari authentication perangkat. Otentikasi perangkat yang kuat untuk teknologi IoT memastikan bahwa perangkat-perangkat yang terhubung dapat dipercayai untuk melakukan aktivitas sesuai dengan program mereka. Selain itu, setiap perangkat IoT membutuhkan identitas yang unik dan bisa diotentikasi ketika perangkat tersebut berusaha untuk membuat koneksi ke sebuah *gateway* atau server pusat. Dengan ID yang unik, sistem administrator IT dapat melacak setiap perangkat setiap saat, berkomunikasi secara aman dengan perangkat tersebut, dan mencegah apabila perangkat tersebut berpotensi untuk melakukan proses yang berbahaya di sistem. Apabila perangkat tersebut tiba-tiba melakukan tindakan yang mencurigakan (diluar *programmingnya*),

orang administrator bisa langsung mengambil hak privilegenya melalui otentikasi ini. (Internet of Things – F.A.Q, 2020)

2.2 Bahasa Pemrograman

Bahasa yang dipakai untuk menginstruksikan komputer disebut bahasa pemrograman. Ada 2 jenis bahasa pemrograman terdiri dari bahasa tingkat tinggi & bahasa tingkat rendah. Kita kenal diantaranya: Basic, Algol, Cobol, Pascal, PL- 1, RPG, SNOBOL, APL, LISP, GPSS, ADA, DEAL dan sebagainya yang merupakan bahasa tingkat tinggi.

Bahasa yang dimengerti oleh mesin komputer adalah intruksi dalam bahasa mesin (Machine Language) yang merupakan bahasa tingkat rendah, jadi bahasa tingkat tinggi yang kita sebutkan diatas agar dapat dimengerti oleh komputer haruslah diterjemahkan lebih dahulu oleh kompilator.

2.3 API (Application Programming Interface)

Application programming interface (API) merupakan suatu dokumentasi yang terdiri dari interface, fungsi, kelas, struktur dan sebagainya untuk membangun sebuah perangkat lunak. Dengan adanya API ini, maka memudahkan programmer untuk “membongkar” suatu software, kemudian dapat dikembangkan atau diintegrasikan dengan perangkat lunak yang lain. API dapat dikatakan sebagai penghubung suatu aplikasi dengan aplikasi lainnya yang memungkinkan programmer menggunakan sistem function. Proses ini dikelola melalui sistem operasi. Keunggulan dari API ini adalah memungkinkan suatu aplikasi dengan aplikasi lainnya dapat saling berhubungan dan berinteraksi. [4]

2.4 Web Server

Web server adalah sebuah *software* (perangkat lunak) yang memberikan layanan berupa data. Berfungsi untuk menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrome, Firefox*). Selanjutnya ia akan mengirimkan respon atas permintaan tersebut kepada *client* dalam bentuk halaman web.

teknologi yang satu ini berfungsi menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrome, Firefox*). Ia juga akan mengirimkan respon atas permintaan kepada client dalam bentuk halaman web yang umumnya HTML.

Web Server memiliki peran dalam memproses berbagai data yang diminta oleh klien (web browser). Kemudian ia memberikan hasil atau jawaban berupa dokumen, video, foto, atau beragam bentuk berkas lainnya.

2.5 Android Studio

Android Studio adalah *Integrated Development Environment* (IDE) resmi untuk pengembangan aplikasi Android, yang didasarkan pada [IntelliJ IDEA](#). Selain sebagai editor kode dan fitur developer IntelliJ yang andal, Android Studio menawarkan banyak fitur yang meningkatkan produktivitas Anda dalam membuat aplikasi.

Setiap project di Android Studio berisi satu atau beberapa modul dengan file kode sumber dan file resource. Jenis modul meliputi modul aplikasi android, modul library dan modul google app engine.[5]

2.6 OTP (One Time Password)

OTP atau *One-time Password* adalah sebuah kode yang biasanya dikirimkan lewat email juga SMS, hal ini merupakan langkah dalam memperkuat autentikasi ketika memasukkan ID dan *Password*. Saat ini, OTP juga digunakan di setiap aplikasi dan yang paling sering kita temukan di aplikasi dompet digital hal

ini dilakukan demi mencegah tindak kejahatan dan tindakan kriminal yang dapat merugikan pihak tertentu.

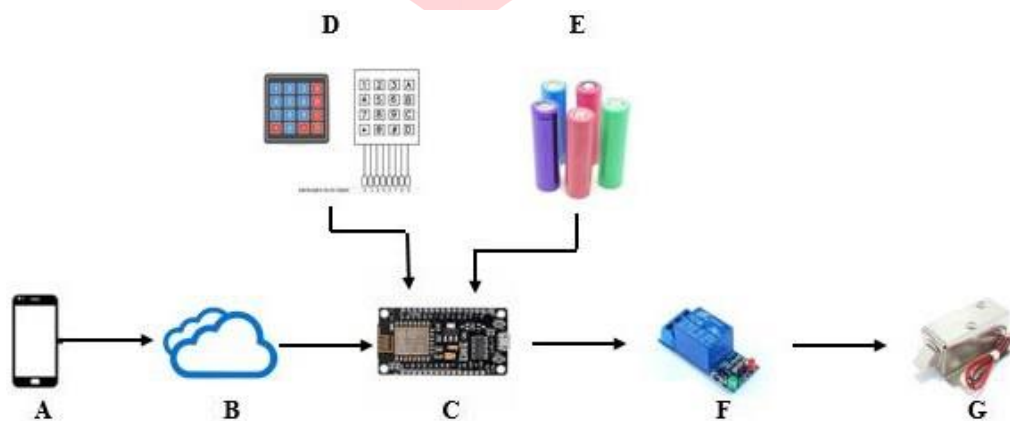
Sumber dari Detik menjelaskan bahwa *One-time Password* pertama kalinya diterapkan oleh sebuah bank yang ada di Indonesia dalam memperketat keamanan pada data. Kemudian OTP selalu digunakan dalam setiap transaksi dan setiap aktivitas umum di masyarakat yang dengan demikian banyak masyarakat yang semakin familiar dengan kode OTP ini.

One-time Password umumnya digunakan hampir disemua aplikasi. Hal ini berguna dalam menjaga para penggunanya dari masalah, misalnya pencurian dan penyalahgunaan atas akun tersebut. Kode OTP biasanya terdiri dari 4 – 6 digit angka, Kode tersebut akan dikirim ke nomor yang telah didaftarkan lalu dikirim melalui SMS atau email.[6]

3. Pembahasan

3.1 Gambaran Umum Sistem

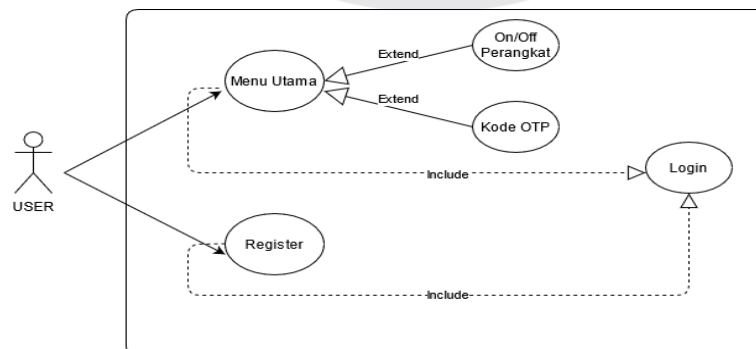
Perancangan yang dilakukan dalam penelitian ini adalah perancangan sistem keamanan yang dapat mengendalikan system buka tutup pada lemari brankas.menggunakan kode OTP . Berikut arsitektur sistem yang dibuat.



Gambar 3.1. Gambaran Umum Sistem.

Sistem terdiri dari beberapa bagian sebagai berikut : Aplikasi android, cloud, Node MCU, Keypad, Baterai, Relay, dan Selenoid.

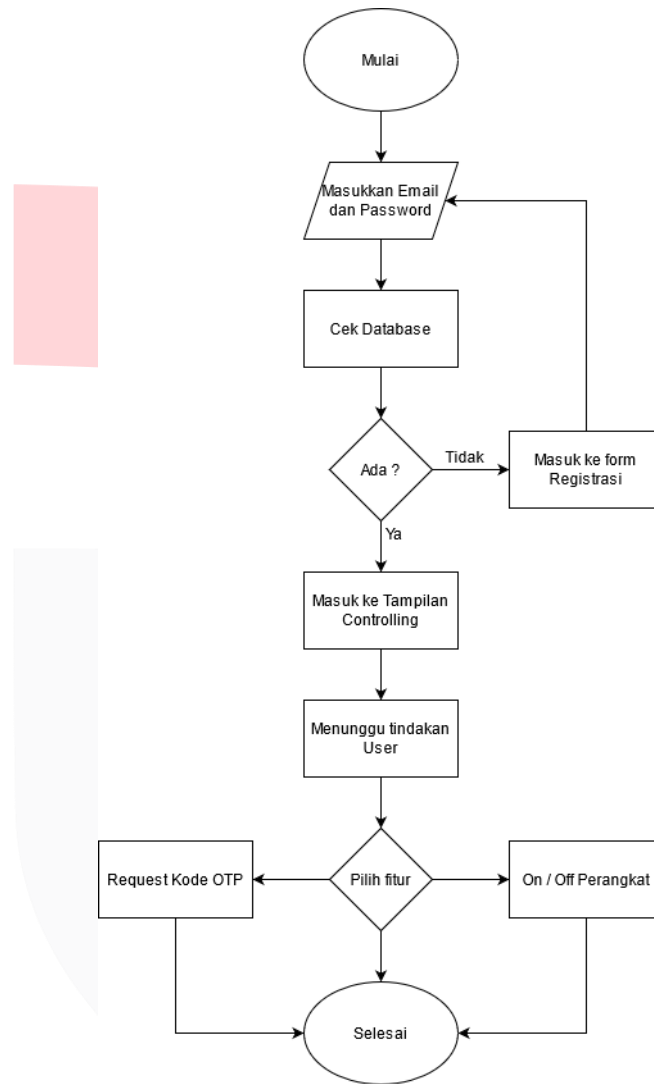
3.2 Use Case Diagram



Gambar 3.2 Use Case Diagram

Pada gambar 3.2 ini adalah *use case diagram user*. Dapat dijlaskan pada aplikasi android Brankas ini terdapat dua menu yang dapat user gunakan, yaitu menu request kode OTP dan On/Off alat. pada menu request kode OTP user dapat meminta kode terbaru jika kode OTP yang lama telah expired. user dapat melakukan on atau off sistem pada lemari brankas jika sedang tidak digunakan. Selain itu juga terdapat fitur login untuk masuk kedalam akun pengguna, jika belum memiliki user dapat registrasi akun terlebih dahulu.

3.3 Flowchart Aplikasi Android

**Gambar 3.3 Flowchart Aplikasi Android**

Pada Gambar 3.9 *Flowchart Aplikasi*, dimulai dengan user melakukan login yaitu dengan memasukkan *username* dan *password*, data yang sudah dimasukkan akan dilakukan proses *check* dengan data yang ada di database. Apabila data yang dimasukkan terdaftar di database maka akan lanjut ke halaman *controlling*, jika *username* yang dimasukkan belum terdaftar di database, maka *user* harus melakukan registrasi terlebih dahulu agar *username* bias terdaftar di database. Pada menu tampilan *controlling* user dapat melakukan tindakan untuk merequest kode OTP, serta dapat melakukan on/off pada sistem aplikasi jika sedang tidak digunakan.

3.4 Pengujian

Pada tahapan ini dilakukan pengujian *Post Data* sebagai berikut :

Tabel 3.1. Tabel Pengujian *Post Data*

Waktu	Aktifitas Pengujian	Hasil Pengujian	Kesimpulan
28-07-2021 14:00	Masukkan halaman awal	Terhubung dengan web server (muncul halaman login)	Berhasil
28-07-2021 14:00	Masukkan email dan password	Muncul halaman controlling	Berhasil
28-07-2021 14:00	Masukkan email dan password yang belum teregistrasi dihalaman login	Gagal masuk ke halaman controlling	Berhasil
28-07-2021 14:00	Muncul halaman registrasi, diminta memasukkan fullnama, email, password	Muncul halaman registrasi	Berhasil
28-07-2021 14:00	Klik tombol refresh kode OTP	Kode OTP baru didapatkan	Berhasil
28-07-2021 14:00	Klik tombol On / Off pada	Sistem aplikasi dapat di non aktifkan	Gagal

	halaman controlling		
29-07-2021 20:00	Klik tombol On / Off pada halaman controlling	Sistem aplikasi dapat di non aktifkan	Berhasil

4. Kesimpulan

4.1 Kesimpulan

Setelah melakukan pengujian pada penelitian tugas akhir ini, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi android untuk sistem keamanan pada lemari brankas berfungsi untuk menambah sistem keamanan pada lemari brankas agar tidak mudah dibobol. Dengan tingkat keberhasilan 95%.
2. Komunikasi antara perangkat *real – time* yaitu aplikasi android yang terhubung dengan *web server* yang berupa perintah data dan pengambilan data yang terhubung pada lemari brankas. Dengan delay antara 5 – 10 detik pada kecepatan internet 34-56 Kbps.
3. Metode OTP (*one time password*) merupakan salah satu metode yang sangat cocok digunakan untuk lemari brankas saat ini, serta dapat menambah nilai keamanan pada lemari brankas.
4. Pengimplementasian pada aplikasi android ini dapat menambah sistem keamanan pada lemari brankas agar tidak mudah di bobol.

4.2 Saran

Berdasarkan penelitian tugas akhir ini, maka saran yang dapat diberikan sebagai berikut.

1. Aplikasi android dapat dikembangkan menjadi aplikasi yang lebih kompleks dengan cara menambahkan fitur-fitur baru dan inovasi baru.
2. Dapat menambahkan enkripsi/dekripsi untuk menambah sistem keamanan yang sudah ada
3. Menambahkan beberapa sensor keamanan pada lemari brankas seperti *Buzzer*

REFERENSI

- [1] Setiadi. D, Muhaemin, M. N. A. 2018. PENERAPAN *INTERNET OF THINGS* (IoT) PADA SISTEM MONITORING IRIGASI (SMART IRIGASI), vol. 3
- [2] Juansyah, A. 2015. PEMBANGUNAN APLIKASI *CHILD TRACKER* BERBASIS *ASSISTED – GLOBAL POSITIONING SYSTEM* (A-GPS) DENGAN PLATFORM ANDROID, vol. 1, pp. 2089 – 9033.
- [3] Binarso, Y. A, Sarwoko. E. A, Bahtiar. N. 2012. PEMBANGUNAN INFORMASI ALUMNI BERBASIS WEB PADA PROGRAM STUDI TEKNIK INFORMATIKA UNIVERSITAS DIPONOGORO. Vol. 1, pp. 72-84.
- [4] Beni Adi Pranata, Astria Hijriani, Akmal Junaidi. 2018. Perancangan Application Programming Interface (API) Berbasis Web Menggunakan Gaya Arsitektur Representational State Transfer (REST) Untuk Pengembangan Sistem Informasi Administrasi Pasien Klinik Perawatan Kulit. Vol. 6, No 1
- [5] Madhya Pradesh. 2018. Development of Native Mobile Application Using Android Studio for Cabs and Some Glimps of Cross Platform Apps. Volume 13, Number 16
- [6] Christian Hadi Wijaya, Ade Hendri Hendrawan, Andik Eko K.P, Arief Gueritno. 2017. Implementasi Sistem One Time Password (OTP) Sebagai Kay Penggerak Pintu Berbantuan Arduino UNO. ISSN 2085-4218.
- [7] Narzisca Angga Dewy. 2018. KONTROL AKSES PINTU RUMAH MENERAPKAN KONSEP OTP (ONE TIME PASSWORD) UNTUK MENINGKATKAN KEAMANAN DENGAN IMPLEMENTASI IOT (Internet Of Things). Vol. 2 No. 1
- [8] N. Anusha, A. Darshan Sai, B. Srikar. 2017. LOCKER SECURITY SYSTEM USING FACIAL RECOGNITION AND ONE TIME PASSWORD. *IEE*, vol. 24. No 1.