BAB I
PENDAHULUAN

Bab ini menjelaskan bagian pendahuluan penelitian, yang meliputi latar belakang, rumusan masalah, tujuan, ruang lingkup, metode penelitian, tinjauan pustaka, kontribusi penelitian, dan sistematika penulisan.

1.1. Latar Belakang

Teknik keamanan dengan mengubah *password* secara dinamis dinamakan *One Time Password* (*OTP*). *OTP* sendiri merupakan otentikasi dimana *password* dapat digunakan sekali pakai (Janakiraman et al., 2018). Pada umumnya *OTP* digunakan untuk kebutuhan proses autentikasi yang dilakukan antara pihak *server* dan *user*.

HOTP merupakan algoritma pembangkit *OTP* berbasis algoritma *HMAC*. *OTP* dapat dihasilkan dengan *input* pada *n*-digit *integer* yang dapat diatur. *HOTP* menghitung nilai *input* dari *counter* yang nantinya akan di validasi dari pihak *server* kepada pihak *client*, *password* yang diakses pada masing-masing *client* tidak terikat satu sama lain sehingga masing-masing *client* memiliki nilai kunci unik yang tersinkronisasi pada *server* (Fakhrusy, 2016). algoritma *HOTP* dikembangkan menjadi *Time-Based One Time Password* (*TOTP*).

TOTP merupakan algoritma yang berbasis algoritma *HMAC* dikembangkan dengan menggabungkan *secret key* dengan *current timestamp* sehingga dapat men-*generate password* sekali pakai dengan batas waktu (Ungkawa, Dewi, & Putra, 2013). Pembentukan menggunakan fungsi kriptografi *secure hash algorithm* .

Secure Hash Algorithm (*SHA*) merupakan teknik kriptografi yang pada tahun 1993 dikembangkan oleh *National Institute of Standards and Technology (NIST)* dan dipublikasikan sebagai *Federal Information Processing Standards (FIPS 180)*. *SHA* menghitung nilai *hash* pada suatu pesan dengan panjang maksimal 160 *bits* untuk pesan dan hasil keluaran yang dinamakan *message digest* atau *hash code*. Namun ditemukan kelemahan pada algoritma *SHA*-0 sehingga pengembangan algoritma baru dari *SHA*-1 yang merupakan revisi dari *SHA*-0.

Keamanan dari *SHA*-0 dan *SHA*-1 berhasil ditembus dengan *brute attack* sehingga pada tahun 2012 algoritma keccak atau yang dikenal sekarang sebagai

SHA-3 menjadi pemenang pada kompetisi untuk membuat sebuah standar baru yang diadakan oleh *NIST*.

SHA-3 memiliki *input* dengan panjang yang tak terhingga, lalu pada ukuran *output* yang dimiliki *SHA*-3 berukuran beragam, mulai dari 224, 256, 384 dan 512 *bits* (Kurniawan, Kusyanti, & Nurwarsito, 2017). sehingga membuat *SHA*-3 menjadi lebih tahan terhadap serangan *brute attack*.

Sampah adalah benda yang sudah tidak bernilai atau tidak diinginkan yang berasal dari aktivitas manusia dalam kehidupan sehari-hari. Sampah semestinya dibuang pada tempatnya namun di Indonesia khususnya dilingkungan sekitar sudah menjadi hal umum untuk melihat sampah tergeletak dimana-mana, sehingga permasalahan ini adalah masalah yang serius (Ananda, 2019) karena dampak yang ditimbulkan dari pembuangan sampah sembarangan.

Dampak sampah bagi masyarakat terhadap kesehatan dapat berpotensi menimbulkan penyakit ini dikarenakan sampah merupakan tempat yang cocok untuk berkembang biaknya kuman yang dapat menimbulkan penyakit dan dampak sampah terhadap lingkungan dari aspek ekosistem perairan, dari aspek ekosistem daratan akan menimbulkan penyakit terhadap masyarakat yang ada di lingkungan sekitar.

Dengan diberlakukannya *new normal* pada masa pandemi tidak bisa dipungkiri bahwa internet dan *wifi* menjadi suatu kebutuhan khusus untuk melakukan segala aktivitas pekerjaan maupun aktivitas pendidikan secara daring (dalam jaringan). Pada masa sekarang jaringan *wifi* dapat ditemukan pada tempat umum entah itu di kafe, taman, kampus maupun kantor (Dewi, 2020). Pada jaringan *wifi* yang bersifat umum dibutuhkan tingkat keamanan yang tinggi pada *password wifi* dikarenakan pada tempat umum memiliki tingkat kebahayaan yang tinggi ini disebabkan perangkat yang terkoneksi pada jaringan *wifi* melalui gelombang radio maka siapapun dapat terkoneksi pada jaringan tersebut.

Sehingga artinya besar kemungkinan adanya pencurian data yang dilakukan oleh orang yang tidak bertanggung jawab terhadap perangkat lain yang terkoneksi dalam jaringan tersebut (Huseynov & Seigneur, 2016). Maka dibutuhkan teknik

itenas library

keamanan yang dapat meningkatkan kerahasiaan kata sandi pada *password wifi* yang statis menjadi *password wifi* yang dapat mengubah secara dinamis.

1.2. Rumusan Masalah

Pada nilai dari *sequence HOTP SHA*-3 jika *input* diubah pada *byte* awal akan mengalami perubahan drastis namun jika perubahan hanya satu *bit* saja tidak akan mengalami perubahan sama sekali (Fakhrusy, 2016). Sehingga pada sistem *HMAC-SHA*-3 memiliki kekurangan pada hasil *input*-nya.

Implementasi *TOTP* berbasis *SHA*-256 dapat *generate password* tanpa terjadinya pengulangan, namun *password* berpotensi memiliki kemirirpan sebesar 0,03% (Ungkawa et al., 2013). Ini dikarenakan pada *current timestamp* yang menggunakan satuan detik pada implementasi algoritmanya.

Setiap hari sampah selalu diproduksi namun tingkat kesadaran masyarakat untuk membuang sampah pada tempat sampah masih sangat kurang (Maulana, Widyanto, Pratama, & Mutijarsa, 2018). Berdasarkan masalah tersebut maka diperlukan suatu cara agar dapat mengajak masyarakat untuk menjaga lingkungan sekitar dengan cara membuang sampah pada tempatnya yang dikaitkan dengan kebutuhan internet pada masa saat ini.

Dari uraian tersebut maka dapat dirumuskan permasalahan pada penelitian sebagai berikut:

a. Bagaimana cara meningkatkan algoritma *TOTP* dalam upaya meningkatkan pengulangan *password*.
b. Bagaimana meningkatkan kesadaran orang dalam membuang sampah ketempat sampah.
c. Bagaimana media tempat sampah dapat memberikan akses *wifi* dan *password wifi* kepada orang yang membuang sampah pada media tempat sampah.

1.3. Tujuan

Tujuan penelitian dari penelitian ini adalah melakukan implementasi algoritma *TOTP* dengan cara penggabungan *secret key* dengan *current time*. Kemudian dilakukan *hashing* menggunakan algoritma enkripsi *SHA*-3 dalam upaya meningkatkan pengulangan *password* muncul dan tujuan lain dari penelitian lain

melakukan pengujian pada model sistem pengelolaan *password wifi* pada media tempat sampah guna meningkatkan kesadaran orang dalam membuang sampah ketempat sampah. Hal ini dikaitkan dengan kebutuhan orang saat ini sudah tidak dapat terlepas dari memperoleh akses jaringan *wifi*, secara khusus dalam kondisi *new normal* saat ini.

1.4. Ruang Lingkup

Ruang lingkup dalam penelitian ini :

a. Mikrokontroller yang digunakan untuk pengelola *password wifi* adalah *raspberry pi 3* model *B*.
b. Sensor yang digunakan untuk deteksi sampah menggunkan jenis ultrasonic.
c. Pengujian *password* menggunakan aplikasi *brute-force attack*.

1.5. Metode Penelitian

Pada Penelitian ini dilakukan impelementasi algoritma *TOTP* berbasis *SHA*-3 yang dapat meningkatkan kerahasiaan kata sandi pada *password* sekali pakai untuk perorangan, *TOTP* akan memiliki *secret key* yang bersifat dinamis ini dikarenkan *secret key* yang digunakan akan dienkripsi dengan teknik algoritma *caesar* terlebih dahulu yang perhitungannya dipengaruhi waktu. Untuk *current time* akan berdasarkan tanggal sehingga perubahan waktu melibatkan hari. Pada media tempat sampah akan memunculkan *wifi* beserta *password*-nya, tahapan agar *user* dapat mengakses *wifi*. *Password* yang sudah dipakai tidak akan bisa diakses lagi sehingga dibutuhkan *password* baru yang valid dengan cara membuang sampah pada media tempat sampah.

1.6. Tinjauan Pustaka

Dalam penelitian ini melibatkan beberapa pustaka yang berkaitan dengan kegiatan yang akan dilakukan :

(Muhamad Fakhrusy, 2016) pada jurnal "*Implementasi HMAC-SHA-3-Based One Time Password pada Skema Two-Factor Authentication*" pada penelitian ini menjelaskan Algoritma *HMAC-SHA-3* dapat di implementasikan pada *TOTP* dengan memasukan *key* yang nantinya akan menjadi *OTP*, kontribusi

yang diambil dari jurnal ini adalah bagaimana cara kerja algoritma *HMAC-SHA-3* dapat diimplementasikan pada sistem.

(Uung Ungkawa, Irma Amelia Dewi, Kurnia Ramadhan Putra, 2013) pada jurnal "*Implementasi Algoritma TIME-BASED One Time Password Dalam Otentikasi Token Internet Banking*" pada penelitian ini menjelaskan bagaimana mendesain dan meng-implementasikan sistem autentikasi *one time password* untuk kebutuhan *internet banking*, kontribusi yang diambil dari jurnal ini adalah bagaimana cara implementasi *TOTP* dapat dikembangkan untuk mengingkatkan keamanan pada autentikasi *server* dan *client*.

(Taufik Ramadhany, 2016) pada jurnal "*Keyed-hash Message Authentication Code(HMAC)*" pada penelitian ini menjelaskan bagaimana cara kerja algoritma *HMAC* untuk sistem kemanan dengan proses autentikasi , kontribusi yang diambil dari jurnal ini adalah memahami cara kerja dari algoritma *HMAC* untuk mengamankan pesan yang dapat diketahui oleh pengirim dan penerima.

(Firlhi Kurniawan, Ari Kusyanti, Heru Nurwarsito, 2017) pada jurnal "*Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost*" pada penelitian ini perbandingan implementasi pada algoritma *SHA*-1 dengan *SHA*-2 pada sistem autntikasi garuda *traning cost*, kontribusi yang diambil dari jurnal ini adalah memahami perbedaan *SHA*-1 dan *SHA*-3 dari cara kerja hingga perbandingan hasil berdasarkan pengujian perbandingan.

(Herry Adi Chandra, Yusup Indra Wijaya, Haldi Budiman, 2019) pada jurnal "*Algoritma One Time Password Pada Sistem Informasi Penerimaan Siswa Baru Online SMP H.A Johansyah.A Banjarmasin*" pada penelitian ini menjelaskan bagaimana mendesain dan meng-implementasikan *one time password* berbasis *web* untuk melakukan validasi proses pendaftaran siswa baru yang dilakukan secara *online*, kontribusi yang diambil dari jurnal ini adalah bagaimana *OTP* dijadikan suatu teknik kemanan pada tiap-tiap *user*.

(Chinmay Kolhatkar ,Bhavesh Joshi, Prachi Choudhari,Dhruvin Bhuva, 2018) pada jurnal "*Smart E-dustbin*" penelitian ini menjelaskan tentang membangun sistem manajemen sampah.dan memnampilkan informasi ke *LCD*

berupa penuh atau tidaknya tempat sampah, kontribusi yang diambil dari jurnal ini adalah pada tempat sampah dapat dikembangkan menjadi sesuatu yang lebih bermanfaat dengan memanfaatkan *IoT* untuk pengelolaannya.

(Anuraj Singh, Sumit Raj, 2019) pada jurnal "*Securing Password Using Dynamic Password Policy Generator Algorithm*" pada penelitian ini menjelaskan tentang membangun sistem *generator password* untuk keperluan *user* agar dapat mendapat *password* secara dinamis dan terhindar dari serangan *hacker*, kontribusi yang diambil dari jurnal ini adalah memahami bagaimana *generator password* menjadi salah satu teknik keamanan yang memiliki tingkat sekuritas yang tinggi terhadap serangan *hacker*.

(Willy Sudiarto Raharjo, Ignatia Dhian E.K.Ratri, Henry Susilo, 2017) pada jurnal "*Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login*" pada penelitian ini menjelaskan tentang membangun sistem *login* dengan menerapkan autentikasi *one time password* agar meningkatkan sekuritas pada sistem, kontribusi yang diambil dari jurnal ini adalah bagaimana autentikasi dua arah yang dilakukan untuk melakukan tahap *login*.

(Chandramohan Sudar ,S K Arjun, L. R. Deepthi, 2017) pada jurnal "*Time-based one-time password for Wi-Fi authentication and security*" pada penelitian ini menjelaskan tentang membangun sistem autentikasi akses ke *access point* menggunakan *OTP* yang terintegrasi dengan *server* dan aplikasi *android* sehingga *output* dari sistem menampikan *barcode*, kontribusi yang diambil dari jurnal ini adalah bagaimana cara *OTP* dapat diimpelmentasikan pada keamanan *password wifi*.

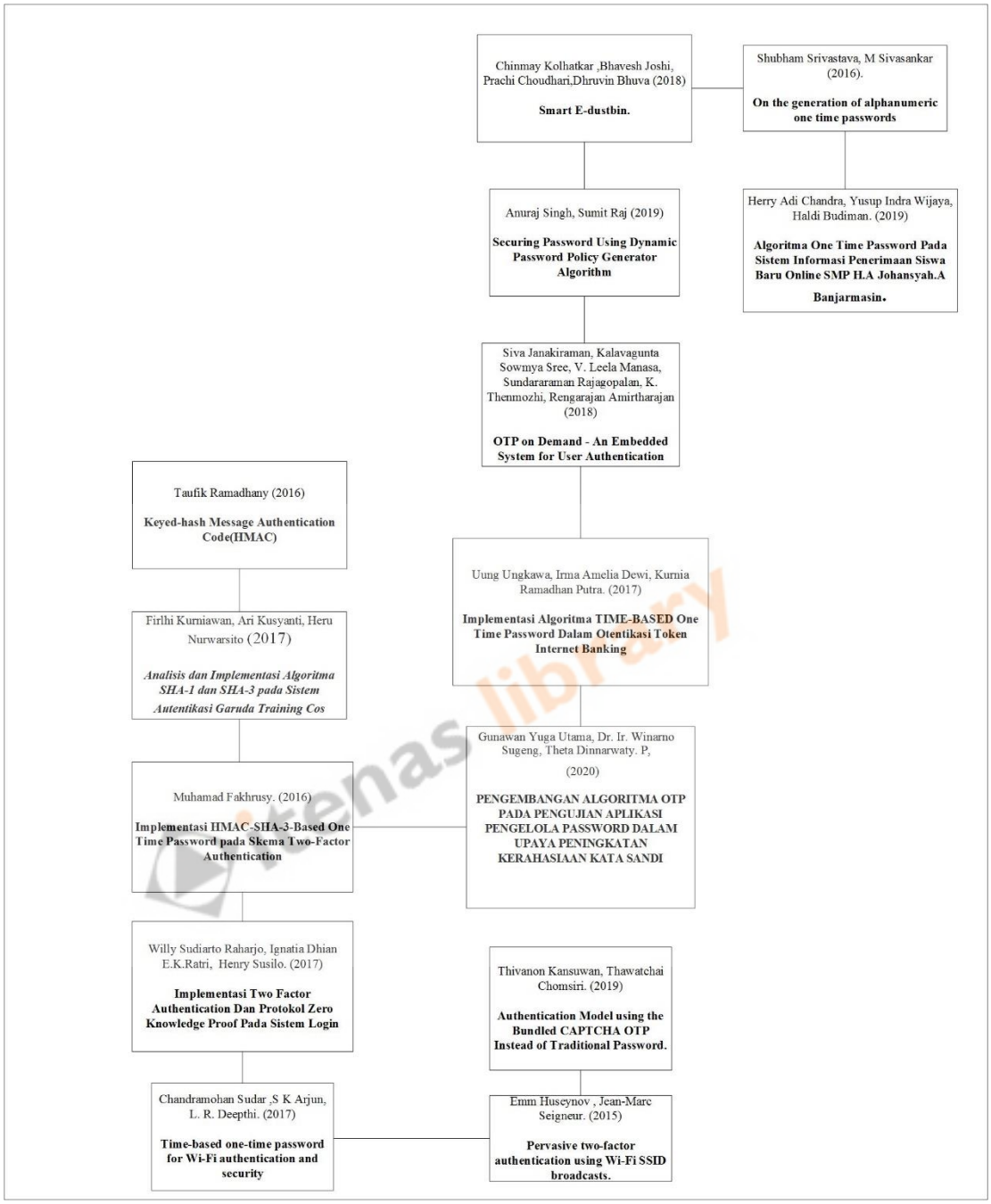
(Siva Janakiraman, Kalavagunta Sowmya Sree, V. Leela Manasa, Sundararaman Rajagopalan, K. Thenmozhi, Rengarajan Amirtharajan, 2018) pada jurnal "*OTP on Demand - An Embedded System for User Authentication*" pada penelitian ini menjelaskan tentang membangun sistem *request OTP* via sms menggunakan *AVR ATmega8* yang terintegrasi dengan modul *GSM*, kontribusi yang diambil dari jurnal ini adalah bagaimana cara kerja dari *OTP* untuk kepentingan proses autentikasi.

(Emm Huseynov , Jean-Marc Seigneur, 2015) pada jurnal "*Pervasive two-factor authentication using Wi-Fi SSID broadcasts*" pada penelitian ini menjelaskan bagaimana membangun sistem *OTP* pada *password Wi-Fi* yang berbasis *web*, sehingga *request OTP* yang dilakukann oleh *user* harus *login* dengan memasukan *username password* maka *access point* terintegrasi dengan *web server* yang dapat men-*generate password* baru, kontribusi yang diambil dari jurnal ini adalah bagaimana *OTP* dapat diimplemenetasikan untuk *password wifi* untuk peroangan *user*.

(Shubham Srivastava, M Sivasankar, 2016) pada jurnal *"On the generation of alphanumeric one time passwords*" pada penelitian ini menjelaskan bagaimana membuat sistem *OTP* dengan gabungan *alphabet* dan *numeric*, kontribusi yang diambil dari jurnal ini adalah *OTP* dapat dikembangangkan pada hasil keluaran berupa *alphabet* dan *numeric*.

Penelitian-penelitian tersebut digambarkan keterhubungannya melalui pemetaan pustaka pada Gambar 1.1 berikut.

itenas library



Gambar 1.1 Peta tinjauan pustaka

1.7. Kontribusi Penelitian

Kontribusi penelitian ini menyesuaikan target kontribusi program studi yatu *smart city*, dalam penelitian ini mengambil topik *smart trash can* yang merupakan bagian dari *smart city*.

1.8. Sistematika Penulisan

Laporan ini disusun berdasarkan sistematika sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan pendahuluan pada Implementasi Algoritma *TOTP SHA*-3 Untuk Pengelolaan *Password Wifi* Pada Media Tempat Sampah.

BAB II LANDASAN TEORI

Bab ini menjelaskan mengenai teori-teori dasar yang digunakan pada penelitian Implementasi Algoritma *TOTP SHA*-3 Untuk Pengelolaan *Password Wifi* Pada Media Tempat Sampah.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai perancangan dari penelitian Implementasi Algoritma *TOTP SHA*-3 Untuk Pengelolaan *Password Wifi* Pada Media Tempat Sampah.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan mengenai implementasi dari perancangan yang telah dilakukan dan pengujian sesuai dengan implementasi yang dikerjakan.

BAB V PENUTUP

Bab ini menjelaskan mengenai kesimpulan, kendala serta saran yang direkomendasikan untuk tahap pengembangan selanjutnya.

itenas library