MIND (Multimedia Artificial Intelligent Networking Database) Journal

MIND Journal | ISSN (p): 2528-0015 | ISSN (e): 2528-0902 | Vol. 5 | No. 1 | Halaman 1 - 13
DOI : https://doi.org/10.26760/mindjournal.v5i1.1 Juni 2020

Tempat Sampah Pengelola Password Wifi dengan Algoritma TOTP SHA-3

THETA DINNARWATY PUTRI, WINARNO SUGENG, GUNAWAN YUGA UTAMA

Program Studi Informatika Institut Teknologi Nasional Bandung
Email : theta@itenas.ac.id

Received 12 Maret 2020 **|** *Revised* 30 April 2020 **|** *Accepted* 25 Mei 2020

ABSTRAK

Algoritma Time-Based One Time Password (TOTP) merupakan algoritma yang berfungsi menghasilkan password untuk satu kali pemakaian. Password yang dihasilkan memiliki batas waktu tertentu dan akan selalu berubah secara dinamis dalam periode tertentu. Algoritma TOTP menggabungkan secret key dengan current time yang kemudian dilakukan hashing menggunakan algoritma enkripsi SHA-3. Pada penelitian ini TOTP diaplikasikan untuk pengelolaan password wifi pada media tempat sampah dimana keterkaitan user dan kebutuhan mengakses wifi. TOTP akan menghasilkan password wifi untuk user jika user melakukan kegiatan membuang sampah pada media tempat sampah. Pada secret key dilakukan enkripsi menggunakan algoritma caesar terlebih dahulu sebelum dilakukan tahap hashing, ini agar membuat secret key dinamis sehingga variasi password menjadi lebih banyak dan dapat meningkatkan keamanan dari password. Dari hasil pengujian keluaran password tidak muncul secara berulang namun memiliki tingkat kemiripan sebesar 0,02%.

Kata kunci: *Internet Of Thing*, *TOTP, SHA*-3, Tempat sampah

ABSTRACT

The Time-Based One Time Password (TOTP) algorithm is an algorithm that produces a password for only one use. A password that is produced has a limited time and always changed dynamically in a specific period. The TOTP algorithm combines a secret key with a current time which is then hased with an encryption algorithm SHA-3. In this experiment the TOTP is applied for managing a wifi password for a user, when the user is throwing a trash at a particular bin. The secret key will be encrypted used a caesar algorithm before the hashing process, so that a secret key become dynamic and the password multiplied, and the security level will be higher. In this experiment the password output has not produced periodically but has a 0.02% simillarity.

***Keywords**: Internet Of Thing, TOTP, SHA-3,Trashbin*

1. PENDAHULUAN

Teknik keamanan dengan mengubah *password* secara dinamis dinamakan *One Time Password* (*OTP*) **(Chandra, Wijaya, & Budiman, 2019)**. *OTP* sendiri merupakan otentikasi dimana *password* dapat digunakan sekali pakai **(Janakiraman, Sree, Manasa, & Rajagopalan, 2018)**. Pada umumnya *OTP* digunakan untuk kebutuhan proses autentikasi yang dilakukan antara pihak *server* dan *user*.

HMAC based One Time Password (HOTP) merupakan algoritma pembangkit *OTP* berbasis algoritma *HMAC*. *OTP* dapat dihasilkan dengan *input* pada *n*-digit *integer* yang dapat diatur **(Ramadhany, 2016)**. *HOTP* menghitung nilai *input* dari *counter* yang nantinya akan divalidasi 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)**. Pembentukannya 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*) **(Singh & Raj, 2019)**. *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, & Nurwasito, 2017)**, sehingga membuat *SHA*-3 menjadi lebih tahan terhadap serangan *brute attack*.

Pada masa sekarang jaringan *wifi* dapat ditemukan pada tempat umum seperti di kafe, taman, kampus maupun kantor **(Andriani, 2020)**. Pada jaringan *wifi* yang bersifat umum dibutuhkan tingkat keamanan yang tinggi pada *password wifi* dikarenakan pada tempat umum memiliki tingkat kebahayaan yang tinggi, hal ini disebabkan perangkat yang terkoneksi pada jaringan *wifi* melalui gelombang radio sehingga siapapun dapat terkoneksi pada jaringan tersebut. Dengan hal tersebut maka keamanan data yang terkoneksi pada jaringan tersebut menjadi hal yang rentan **(Kolhatkar, Joshi, Choudhari, & Bhuva, 2018)**.

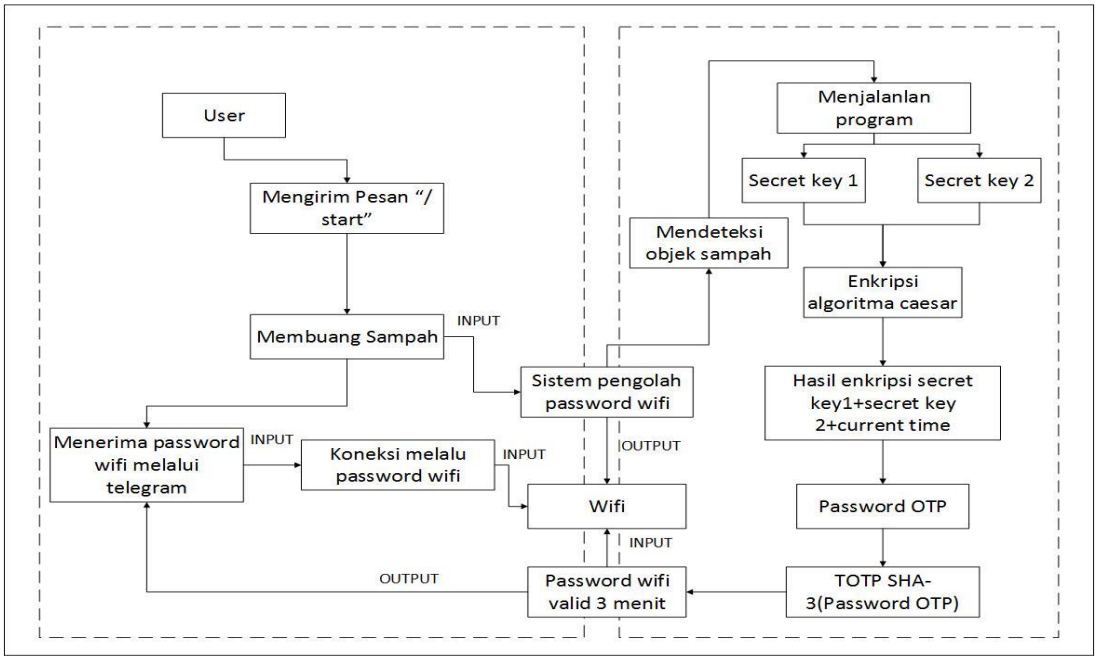
Besar kemungkinan adanya pencurian data yang dilakukan oleh orang yang tidak bertanggung jawab terhadap perangkat lain yang terkoneksi dalam jaringan tersebut **(Huseynov & Seigneur, 2016)**. Dengan hal tersebut maka penelitian ini membangun teknik keamanan yang dapat meningkatkan kerahasiaan kata sandi pada *password wifi* yang statis menjadi *password wifi* yang dapat mengubah secara dinamis untuk meminimalisir pencurian data dengan menggunakan algoritma *TOTP SHA*-3*.*

2. METODE PENELITIAN

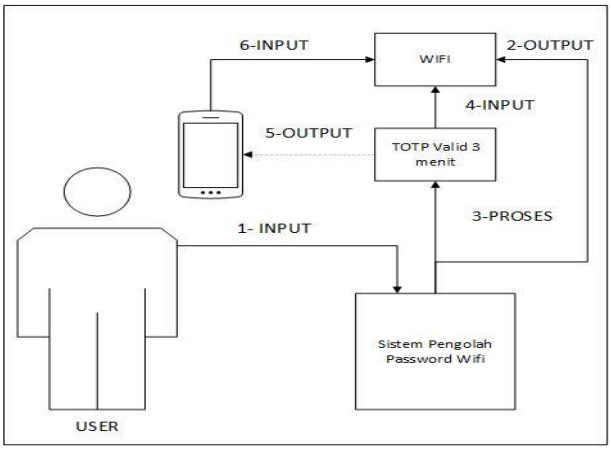
Metode proses pembuatan sistem dalam penelitian ini menggunakan model *prototype*. Dasar dari metode penelitian adalah dengan melakukan implementasi algoritma *TOTP* berbasis *SHA*-3 yang dapat meningkatkan kerahasiaan kata sandi pada *password* sekali pakai untuk perorangan. *TOTP* memiliki *secret key* yang bersifat dinamis, hal tersebut dikarenakan *secret key* yang digunakan akan dienkripsi dengan teknik algoritma *caesar* terlebih dahulu yang perhitungannya dipengaruhi waktu. *Current time* dilakukan berdasarkan tanggal sehingga perubahan waktu melibatkan hari. Media tempat sampah akan memunculkan *wifi* beserta *password* 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 tersebut.

Penelitian ini bertujuan untuk melakukan implementasi algoritma *TOTP* dengan cara penggabungan *secret key* dengan *current time*. Kemudian dilakukan *hashing* menggunakan algoritma enkripsi *SHA*-3 dalam upaya meningkatkan pengulangan kemunculan *password* yang sama dengan melakukan pengujian pada model sistem pengelolaan *password wifi* pada media tempat sampah.

Perancangan sistem akan ditujukan dengan skema *mindmapping* yang berisikan bagaimana cara kerja antara *user* dengan sistem saling berkaitan, skema apa yang akan dilakukan *user* terhadap sistem, respon apa yang dilakukan oleh sistem dan bagaimana perancangan *TOTP SHA*-3 diimplementasikan ke media tempat sampah yang ditujukan pada Gambar 1.



Gambar 1. *Mind Mapping* Proses Kerja Sistem yang Dibangun

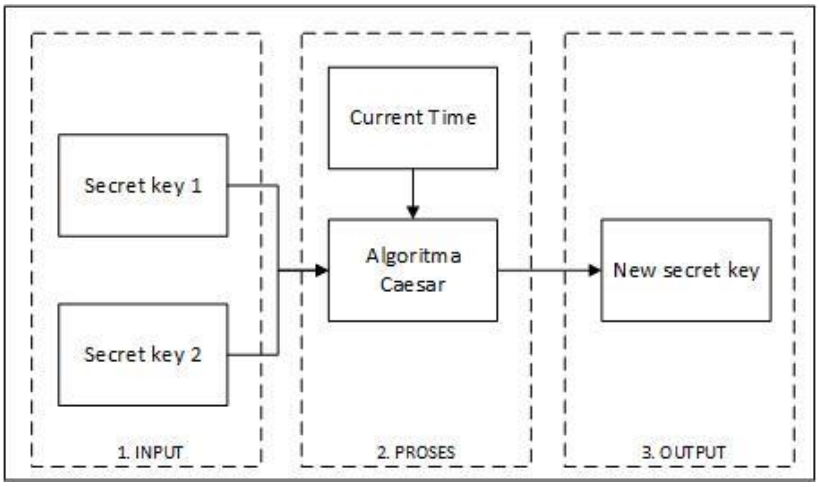


Gambar 2. Skema Umum Perancangan Sistem Pengolah *Password Wifi*

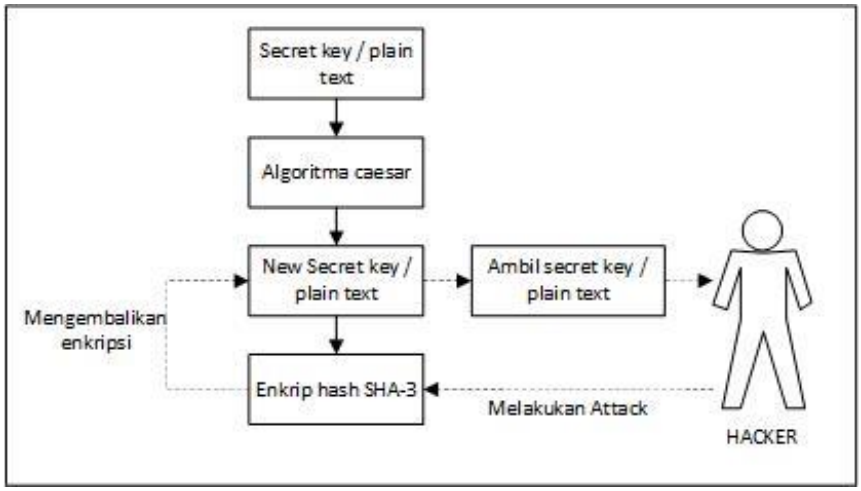
Berikut adalah penjelasan tahapan skema perancangan yang ditujukan pada Gambar 2 :

1. *User* melakukan aktivitas berupa membuang sampah pada media tempat sampah dianggap sebagai nilai *input*.
2. Media tempat sampah menyediakan *wifi* sebagai *output*.
3. Media tempat sampah akan men-*generate* atau melakukan proses *TOTP* yang dapat diakses selama 3 menit.
4. Hasil *generate TOTP* di *input* ke *settingan wifi* sebagai *password wifi*.
5. Hasil *output generate TOTP* dikirim ke *user*.
6. *User* dapat mengakses *wifi* dengan melakukan *input password wifi* dari *TOTP* yang telah diterima.

Penerapan *TOTP* selain menggunakan teknik *hash SHA*-3 juga menggunakan teknik enkripsi algoritma *caesar*, tujuan penerapan algoritma *caesar* yaitu untuk meningkatkan varian *password* dan meningkatkan keamanan. Algoritma *caesar* akan digunakan untuk mengenkripsi *secret key* pada kasus ini *secret key* akan dibagi menjadi dua *secret key* skema implementasi algoritma *caesar* yang ditujukan pada Gambar 3.



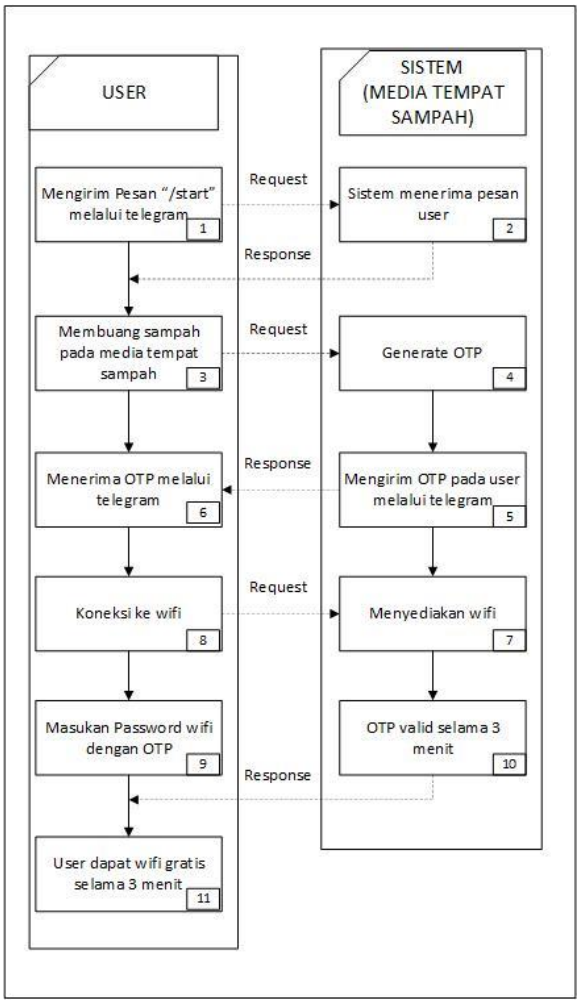
Gambar 3. Penerapan Algoritma *Caesar*



Gambar 4. Skema *Hacker*

Pada Gambar 4 ditujukan bagaimana jika suatu waktu *SHA*-3 berhasil diretas dan *secret key* atau *plain text* berhasil dicuri oleh *hacker*, namun *secret key* atau *plain text* yang dicuri merupakan hasil enkripsi berdasarkan algoritma *caesar* yang sudah diproses sebelum melakukan tahap enkripsi algoritma *SHA*-3. Meskipun untuk saat ini *SHA*-3 belum berhasil diretas namun penerapan dengan cara ini menjadi jalan alternatif untuk meningkatkan keamanan kerahasiaan pada *password*, *secret key* atau *plain text*. Gambar 5 menunjukkan blok diagram dari sistem yang akan dijelaskan sebagai berikut :

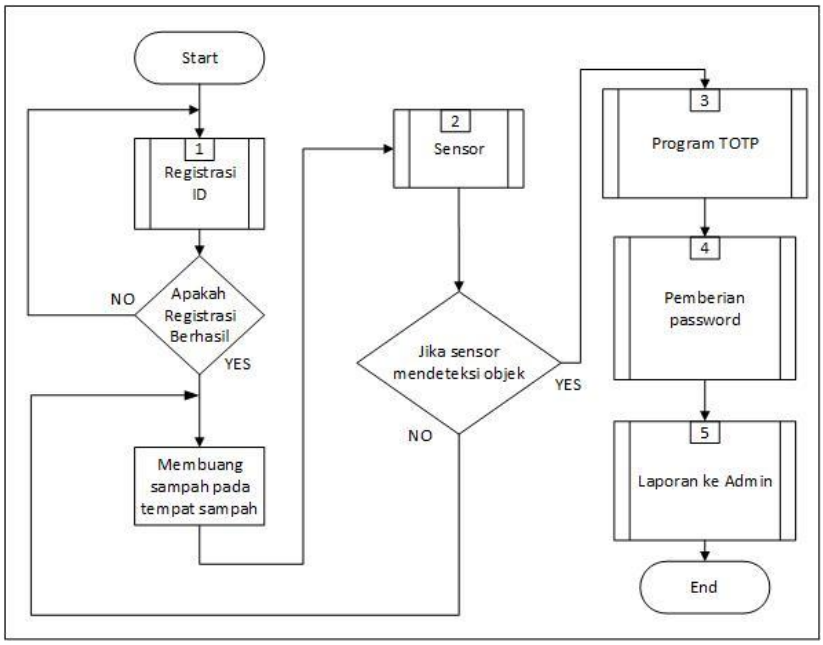
1. *User* mengirim pesan "/*start*" ke sistem melalui *telegram*.
2. Sistem menerima pesan dari user agar dapat memulai program untuk mendeteksi objek sampah sebagai nilai *input*.
3. *User* membuang sampah pada media tempat sampah.
4. Sistem mendeteksi objek sampah lalu men-*generate OTP*.
5. *OTP* yang telah di*generate* akan dikirim oleh sistem ke *user* melalui *telegram*.
6. *User* akan menerima *OTP* dari sistem melalui *telegram*.
7. Sistem menyediakan *wifi* untuk *user*.
8. *User* melakukan tahap koneksi ke *wifi* dari media tempat sampah.
9. User memasukan *password wifi* dengan *OTP* yang telah diterima sebelumnya.
10. *OTP* bisa diakses selama 3 menit.
11. *User* dapat melakukan aktivitas melalui *internet* yang terkoneksi ke *wifi* selama 3 menit.



Gambar 5. Blok Diagram Sistem Media Tempah Sampah *Wifi*

Seperti pada Gambar 6 terdapat beberapa tahapan dalam melakukan pengolahan pada penelitian ini. Berikut merupakan penjelasan-penjelasan dari *flowchart* pada Gambar 6 tersebut :

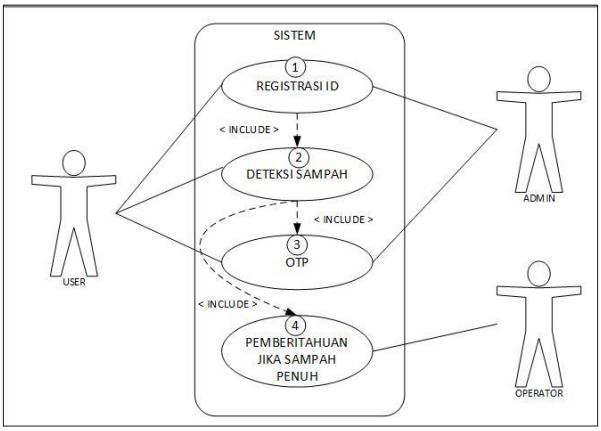
1. **Registrasi *ID* :** pada tahapan ini dilakukannya registrasi agar sistem dapat mengirim *password* yang valid kepada *client* sehingga orang yang membuang sampah dan mendapatkan *wifi* adalah orang-orang yang sudah terdaftar *password* akan dikirim via *telegram* dan untuk registrasi dilakukan secara *private*, data yang isi berupa informasi pribadi dan *token telegram*.
2. **Sensor :** tahapan ini bertujuan untuk mendeteksi objek atau sampah ketika masuk sehingga dapat memberikan kondisi agar sistem dapat memproses atau menjalankan program namun jika sensor terus menerus mendeteksi objek maka sistem akan memberitahu pihak operator bahwa tempat sampah telah penuh dan menghentikan sistem.
3. **Program *TOTP* :** adalah tahapan untuk *generate TOTP* untuk pengelolaan pada *password wifi*, sehingga *password* berubah secara dinamis berdasarkan *TOTP SHA*-3.
4. **Pemberian *Password* :** Bertujuan untuk pemberian *password* yang sudah di-*generate* oleh program akan dikirim via *telegram* kepada *client* yang sudah terdaftar pada *telegram*.
5. **Laporan Ke *Admin* :** setiap laporan atau *log* dari sistem akan dikirim ke *Admin* yang nantinya *Admin* akan menerima laporan atau log tersebut via *e-mail*.



Gambar 6. *Flowchart* Sistem Pengelolaan *Password* pada Media Tempat Sampah *Wifi*

Pada *use case* yang ditujukan pada Gambar 7 terdapat tiga *actor* yaitu *user, admin* dan operator, serta beberapa fungsionalitas pada sistem. Berikut adalah penjelasan dari masing-masing fungsionalitas :

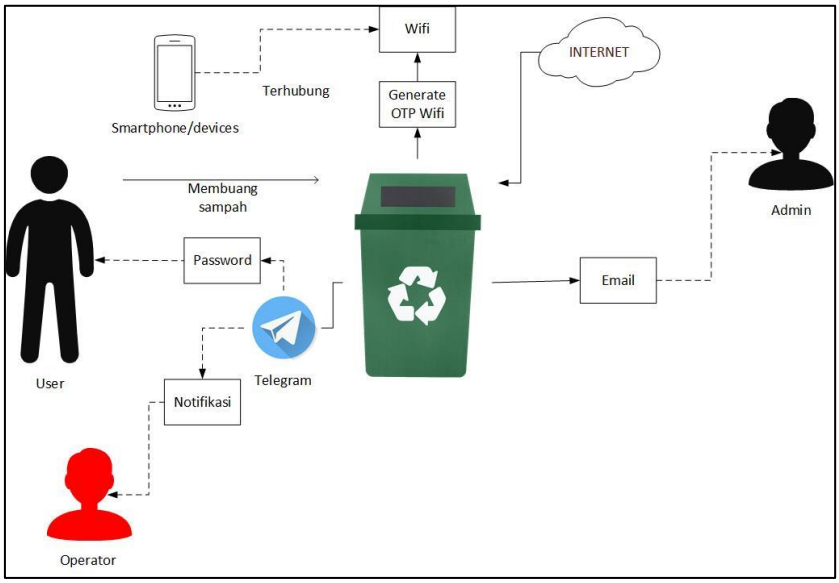
1. Fungsionalitas registrasi *id*, pada fungsionalitas ini *user* pertama kali melakukan tahap registrasi kepada pihak *admin* sehingga *admin* akan mendaftarkan *user* dengan memasukan *token telegram* milik *user* pada sistem, sehingga *user* memiliki akses untuk mendapatkan akses *wifi* dan *password wifi*.
2. Fungsionalitas deteksi sampah, pada fungsionalitas ini merupakan kegiatan *user* memasukan objek sampah pada media tempat sampah.
3. Fungsionalitas *OTP*, pada fungsionalitas ini merupakan *generate OTP* berdasarkan *TOTP SHA*-3 pada *password wifi* yang akan dikirim ke *user* untuk mengakses *wifi* selama 3 menit dan dikirim ke pihak *admin* sebagai laporan *log* atau aktivitas dari media tempat sampah.
4. Fungsionalitas pemberitahuan jika tempat sampah penuh, pada fungsionalitas ini merupakan pemberitahuan kepada pihak operator jika tempat sampah harus segera dikelola, lalu sistem akan berhenti beroperasi.



Gambar 7. *Use Case Diagram* Fungsional Sistem Keseluruhan

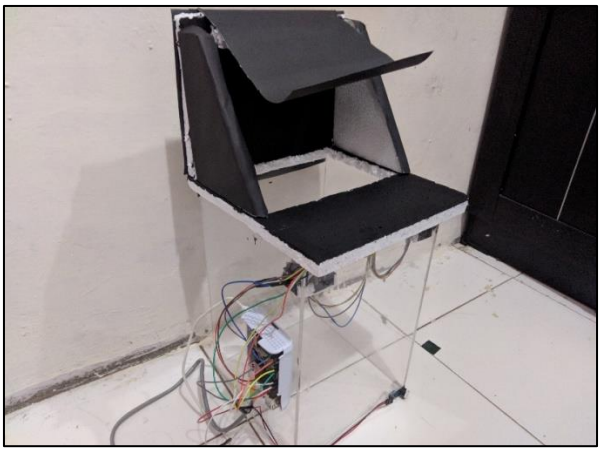
3. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan ini dibahas mengenai bagaimana *TOTP SHA*-3 dapat diimplementasikan untuk pengelolaan *password wifi* pada sistem tempat sampah *wifi* dan dapat men-*generate password wifi* untuk sekali diakses dalam batas waktu yang ditentukan. Berikut adalah blok diagram umum bagaimana sistem bekerja dan saling berhubungan yang ditujukan pada Gambar 8.



Gambar 8. Implementasi Sistem Pengelolaan *Password* pada Sistem Tempat Sampah *Wifi*

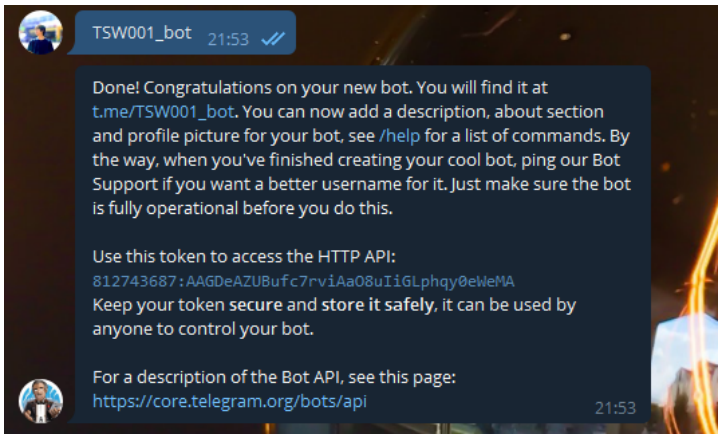
Pada Gambar 9 ditunjukan hasil dari perancangan seluruh *hardware* dari *prototype* tempat sampah dan perancangan alat.



Gambar 9. Implementasi *Hardware Prototype* Sistem

Subsistem *telegram* memanfaatkan *Internet of thing* sebagai suatu inovasi dimana mesin dapat berkomunikasi dengan manusia secara mandiri dan tidak ada campur tangan dari manusia, selama *raspberry pi* terhubung ke *internet* maka opsi fitur komunikasi yang akan digunakan cukup banyak salah satunya aplikasi *chatting telegram* sehingga pemanfaatan *internet* yang mana adalah inti dari *IoT* dapat diimplementasikan pada sistem dengan menggunakan *bot telegram* pada *python raspberry*, *bot telegram* akan memiliki dua akun yang dapat berkomunikasi dengan *raspberry pi* yaitu *User* dan *Operator*, *User* berperan

sebagai penerima *password wifi* yang nantinya akan dikirim melalui *telegram* dari sistem sedangkan *Operator* berperan me-*manage* kapasitas sampah jika penuh dan memberi perintah untuk menjalakan sistem jika tempat sampah sudah siap beroperasi.

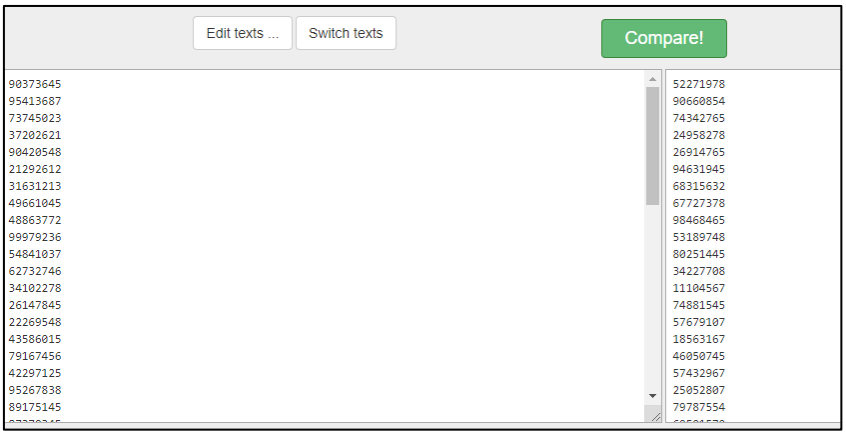


Gambar 10. *Bot Telegram*

Berikut ini merupakan pengujian kemiripan hasil keluaran *TOTP* dengan skenario sebagai berikut :

Skenario Awal : Hasil keluaran di-*generate* dalam dua waktu yang berbeda.
Tujuan : Membandingkan kemiripan dari kedua hasil *generate* .
Waktu Pengujian : 21-09-2020 pada pukul 15:30

Pengujian dilakukan dengan mencetak 50 *password* dalam dua waktu yang berbeda, hasil keluaran dibandingkan dengan menggunakan *tool* yang bernama *text compare*. Perbandingannya ditunjukan pada Gambar 11 sebagai berikut.



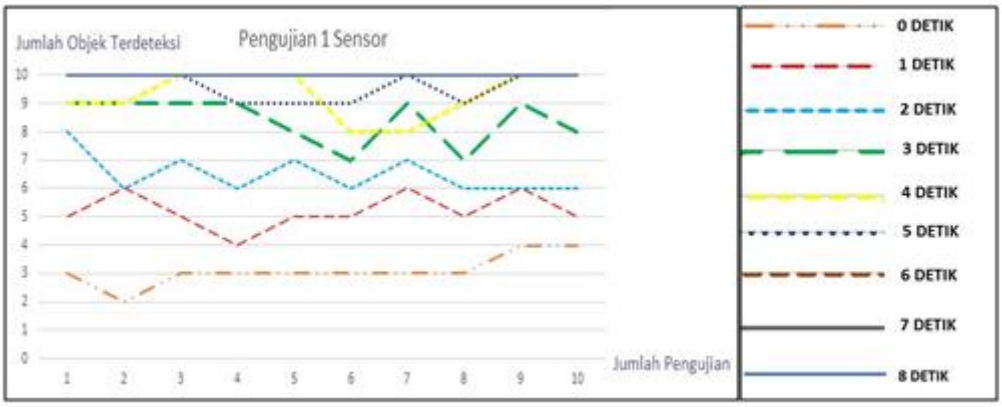
Gambar 11. Komparasi *OTP*

Saat dibandingkan terdapat satu *password* yang memiliki tingkat kemiripan yang tinggi, seperti yang ditujukan pada Gambar 12 sebagai berikut.

Gambar 12. Kemiripan *TOTP*

Dari 50 *password* terdapat kemiripan *password* dengan jumlah digit 5 berupa deretan angka "94563" pada kedua hasil keluaran *password,* sehingga presentase dengan tingkat kemiripan

sebesar $\frac{01}{50}$ = 0,02%. Pada hasil pengujian didapatkan perolehan jumlah objek terdeteksi dengan hasil sebesar 100% pada jeda 6 detik untuk pengujian *alpha* satu sensor.

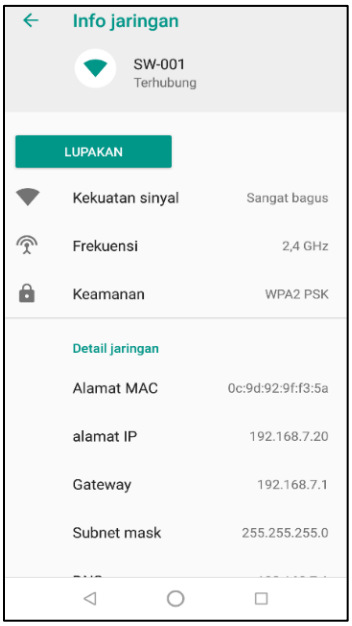


Gambar 13. Grafik Pengujian *Alpha* Satu Sensor

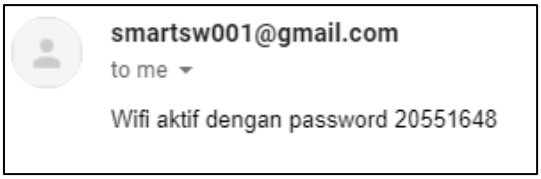
Berikut ini merupakan pengujian *Beta* implementasi *Hardware* yang terdapat pada Gambar 14. Pada saat kertas atau objek sampah dimasukan ke tempat sampah dengan posisi horizontal dan diagonal akan terdeteksi oleh dua sensor ultrasonik yang sebelumnya sudah dijalankan oleh *operator* melalui *telegram*, sensor ultrasonik akan mendeteksi objek jika terjadi perubahan deteksi jarak, ketika adanya perubahan maka perubahan tersebut akan dijadikan suatu nilai analog dan men-*trigger* untuk menjalankan sistem.

Gambar 14. Pengujian Buang Sampah

Gambar 15 menunjukkan hasil uji konektivitas dari *smartphone*, hasil yang didapat adalah *smartphone* dapat terkoneksi dengan *wifi*, secara otomatis *smartphone* mendapatkan *ip dhcp* dan mendapatkan akses *internet.*



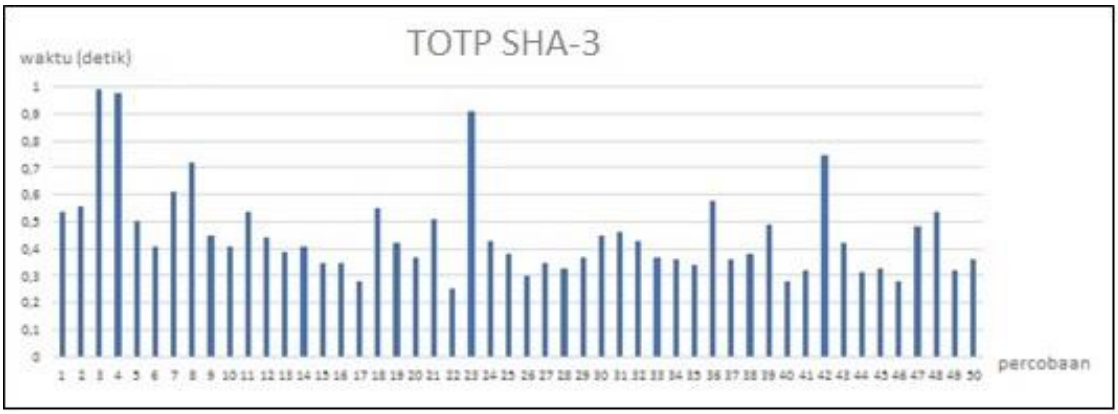
Gambar 15. Pengujian Konektivitas



Gambar 16. Pengujian *Email* Diterima *Admin*

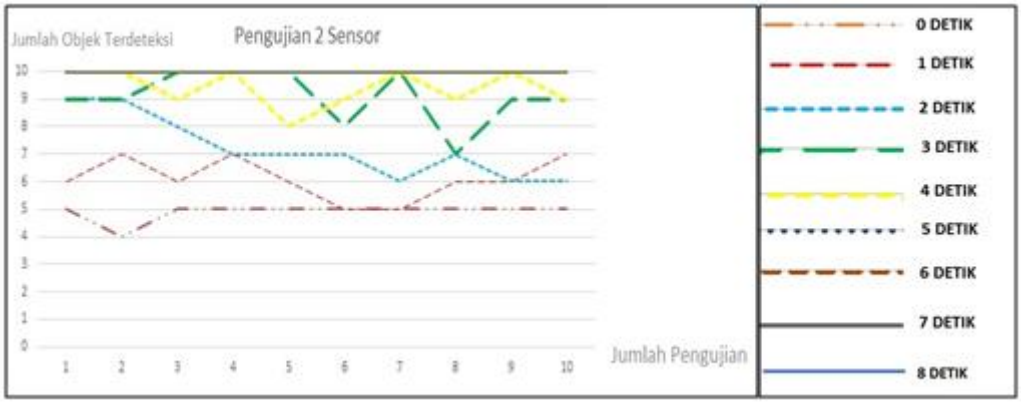
Gambar 16 menunjukkan bahwa *admin* secara otomatis mendapatkan *email* dari tempat sampah mengenai aktivitas saat *WiFi* aktif beserta *password WiFi* yang *valid*.

Gambar 17 menunjukan grafik dari pengujian *beta*, implementasi algoritma *TOTP SHA*-3 pada sistem sampah *wifi* menunjukan berapa perolehan waktu dalam detik yang didapat saat sistem mendeteksi objek sampah dan mengirim *password wifi* ke *telegram*, perolehan rata-rata waktu yang didapat adalah 0,45 detik.



Gambar 17. Pengujian *Beta* Algoritma *TOTP SHA-3*

Pada Gambar 18 didapatkan perolehan jumlah objek terdeteksi dengan hasil sebesar 100% pada jeda 5 detik untuk pengujian *beta* dua sensor.



Gambar 18. Grafik Pengujian *Beta* Dua Sensor

4. KESIMPULAN

Kesimpulan yang didapat pada penelitian algoritma *TOTP SHA*-3 untuk pengelolaan *password wifi* pada media tempat sampah ini adalah penerapan enkripsi *SHA*-3 dapat menjaga kerahasiaan *password* yang telah diuji dengan *brute attack*, penerapan algoritma *caesar* pada *TOTP* membuat variasi *password* yang banyak dan meningkatkan kerahasiaan *password* sebagai lapis keamanan kedua. Pada pengujian jeda waktu dengan 1 sensor diperoleh presentase 100% pada jeda waktu 6 detik dan dengan 2 sensor diperoleh presentase 100% pada jeda waktu 5 detik sehingga sensor dapat mendeteksi objek dengan baik jika ada waktu jeda untuk merespon selama 5 detik. Dari hasil pengujian keluaran *password* tidak terdapat kemunculan *password* yang berulang namun memiliki tingkat kemiripan *password* sebesar 0,02%.

Sistem tempat sampah *wifi* digunakan sebagai implementasi sistem dengan hasil pengujian sistem mampu mengidentifikasikan akun telegram yang teregistrasi dengan menggunakan *token*, mendeteksi objek dengan sensor ultrasonik, menghasilkan password *wifi* berbasis *TOTP SHA*-3, mengirim *password wifi* melalui *telegram* dan mencatat laporan ke *admin* melalui *e-mail*.

DAFTAR RUJUKAN

Andriani, D. (2020). *Perlunya Tingkatkan Jaringan Internet di Masa New Normal*. Diambil kembali dari https://teknologi.bisnis.com/read/20200805/84/1275606/perlunya-tingkatkan-jaringan-internet-di-masa-new-normal

Chandra, H. A., Wijaya, Y. I., & Budiman, H. (2019). Algoritma One Time Password pada Sistem Informasi Penerimaan Sistem Baru Online SMP H.A Johansyah A Banjarmasin. (hal. 207-211). Technologia.

Fakhrusy, M. (2016). Implementasi HMAC-SHA-3-Based One Time Password pada Skema Two-Factor Authentication. 1-6.

Huseynov , E., & Seigneur, J.-M. (2016). WiFiOTP : Pervasive two-faktor Autentication using Wi-Fi SSID Broadcasts. *Proceedings of the 2015 ITU Kaleidoscope : Trust in the Information Society, K-2015-Academic Conference.*

Janakiraman, S., Sree, K. S., Manasa, V. L., & Rajagopalan, S. (2018). *2018 International Conference on Computer Communication and Informatics (ICCI)*, (hal. 1-2).

Kolhatkar, C., Joshi, B., Choudhari, P., & Bhuva, D. (2018). Smart E-dusbin. *International Conference on Smart City and Emerging Technology, ICSCET*, (hal. 1-3).

Kurniawan, F., Kusyanti, A., & Nurwasito, H. (2017). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 803-812.

Ramadhany, T. (2016). *Authentication, K.M., & Hmac, C. (n.d).Keyed-has Message Authentication Code (HMAC).*

Singh, A., & Raj, S. (2019). Securing Password using Dynamic Password Policy Generator Algorithm. *Journal of King Saud University - Computer and Information Sciences*.

Ungkawa, U., Dewi, I. A., & Putra, K. R. (2013). Implementasi Algoritma Tme-Based One Time Password dalam Otentikasi Token Internet Banking. *Teknik Informatika Fakultas Teknologi Industri Institut Teknologi Nasional Bandung*, 2-11.