

**IMPLEMENTASI KEAMANAN BERBAGI ASET SANDI WIFI
DENGAN METODE ONE WAY HASH SHA-256 DAN QR CODE**

SKRIPSI

**Disusun sebagai salah satu syarat untuk memperoleh Gelar Sarjana Teknik
Pada Program Studi Teknik Informatika Universitas Sangga Buana YPKP**

Disusun oleh:

DEDE SUDIRMAN

2113181091



FAKULTAS TEKNIK

**PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS SANGGA BUANA YPKP**

2022

LEMBAR PERSEMBAHAN



Ucup Syukur kepada *Allah SWT* yang telah memberikan kesempatan dan kekuatan dalam menjemput keberkahan menuntut ilmu. Karunianya tiada kira yang membukakan jalan yang mudah untuk menyelesaikan skripsi ini. Shalawat dan salam selalu terlimpahkan curahkan kepada baginda *Rasulullah Muhammad SAW*.

Kupersembahkan karya sederhana ini untuk orang terkasih, tersayang dan dihormati.

Ibunda dan Ayahanda Tercinta

Sebagai tanda bakti, hormat dan rasa terimakasih yang amat besar kupersembahkan kepada Ibunda (Rumyati) dan Ayahanda (Jaenal Aripin) yang tiada henti memberikan kasih sayang, ridho, dan dukungan moral maupun materi, semoga senantiasa terus dalam lindungan dan karunia Allah SWT.

Keluarga dan Orang Terdekat

Sebagai tanda terimakasih kupersembahkan kepada keluarga kandung terdekat Kakak (Arif permana) adik pertama (Muhammad yusuf) dan adik kedua (Alwi Mubrom) yang selalu memberikan semangat, untuk teman-teman seperjuangan di Universitas Padjadjaran (Yudi, Fahri, Gery, Fajar serta teman *FrontEnd*, dan *Backend* lainnya) yang memberikan koreksi, pandangan, simulasi sidang, pengalaman dan berbagi ilmu. Tak tertinggal untuk orang spesial yang mau direpotkan ketika sedang sibuk (Aisyah Nurjanah, S.Pd.) yang memberikan koreksi dan semangat untuk cepat lulus.

Dosen Pembimbing

Dr. Teguh Nurhadi Suharsono, ST., M.T selaku Dosen pembimbing, Terimakasih banyak terucap atas bimbingan,waktu, dukungan, nasihat, pengajaran dan pengertian yang luar biasa sehingga skripsi ini dapat diselesaikan.

PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama: DEDE SUDIRMAN

NIM: 2113181091

Menyatakan dengan sebenar-benarnya bahwa laporan Skripsi saya yang berjudul:

**IMPLEMENTASI KEAMANAN BERBAGI ASET SANDI WIFI DENGAN
METODE ONE WAY HASH SHA-256 DAN QR CODE**

Adalah hasil karya sendiri dan bukan jiplakan hasil karya orang lain.

Demikian pernyataan ini saya buat dengan sebenar-benarnya. Jika dikemudian hari terbukti bahwa laporan Skripsi saya merupakan hasil jiplakan, maka saya bersedia menerima sanksi apapun yang diberikan.

Bandung, 05 Juni 2022



Dede sudirman

LEMBAR PERSETUJUAN DAN PENGESAHAN TUGAS AKHIR

NPM : 2113181091
Nama : Dede Sudirman
Program Studi : Teknik Informatika
Judul : **IMPLEMENTASI KEAMANAN BERBAGI ASET SANDI WIFI DENGAN METODE ONE WAY HASH SHA-256 DAN QR CODE**

Telah dipertahankan pada sidang Tugas Akhir Semester Genap Tahun Ajaran 2022 dihadapan para penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik (S.T) pada Fakultas Teknik Program Studi S1 Teknik Informatika Universitas Sangga Buana YPKP.

Bandung, 10 Agustus 2022

Menyetujui
Pembimbing,



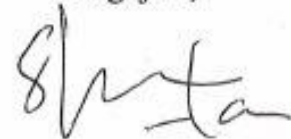
Dr. Teguh Nurhadi Suharsono, ST., M.T.
NIDN. 0021077101

Penguji I,



Riffa Haviani Laluma, S.Kom., MT.
NIDN. 0011067301

Penguji II,



Gunawan, ST., M.kom
NIDN. 0404027604

Mengetahui
Ketua Program Studi Teknik Informatika,



Riffa Haviani Laluma, S.Kom., MT.
NIDN. 0011067301

KATA PENGANTAR

Puji dan Syukur kehadiran Allah SWT, atas rahmat dan karunianya penelitian dalam skripsi yang berjudul “**IMPLEMENTASI KEAMANAN BERBAGI ASET SANDI WIFI DENGAN METODE ONE WAY HASH SHA-256 DAN QR CODE**” dapat terselesaikan. Penelitian ini menyajikan model Hash yang diimplementasikan dalam sandi *WiFi*. Adapun maksud dan tujuan dari penulisan skripsi ini adalah untuk memenuhi syarat mengikuti sidang skripsi, Jurusan Teknik Informatika Universitas Sangga Buana YPKP.

Selama penelitian dan penyusunan skripsi banyak sekali hambatan yang ditemui, namun berkat bantuan serta dorongan dari berbagai pihak, akhirnya skripsi dapat terselesaikan.

Persembahan skripsi ini merupakan karya terbaik yang dapat disajikan, namun tetap disadari didalamnya terdapat kekurangan-kekurangan, oleh karenanya kritik dan saran membangun sangat terbuka untuk perbaikan dimasa yang akan datang. Akhir kata, semoga skripsi ini dapat bermanfaat bagi penyusun dan khususnya bagi para pembaca.

Bandung, 05 Juni 2022

Penulis,



Dede Sudirman

ABSTRAK

Penelitian ini dilakukan untuk memodelkan aset sumber daya sandi WiFi dalam sebuah platform yang dapat dibagikan dan berkolaborasi secara publik dengan aman serta mendukung perubahan data yang dinamis dengan pintasan repositori online yang terdokumentasikan dalam dukungan akses melalui mesin pencari khusus dan QR CODE. Dalam penelitian ini menggunakan 3 metode, yaitu fungsi HASH SHA-256 satu arah yang di formulasi dengan penambahan teknik penaburan dan teknik pembalik sehingga menghasilkan String panjang yang diberi nama Keycode, Metode kedua menggunakan teknik kriptografi modern yaitu Digital Siganature, yang menghimpun keycode dalam Path identitas dari aset sumber daya, dan yang terakhir adalah QR CODE digunakan sebagai pintasan akses yang menghimpun data akses Digital signature. Dalam penelitian ini menggunakan data testing dari kontributor aplikasi pembandingan yaitu wifimap.io secara acak yang selanjutnya hasil formulasi di dibongkar dengan teknik brute force menggunakan HASHCAT. Hasil penelitian data sandi dari sumber daya berhasil diformulasikan menjadi kombinasi String dengan kerahasian tinggi yang tidak bisa dibongkar ke data aslinya, namun tetap dapat diakses oleh pemilik dan pemegang keycode yang di imbangi dengan batasan kontrol aksesnya.

Kata Kunci: Hashing, SHA-256, WiFi, Jaringan Komputer, Digital Signature, QR CODE.

ABSTRACT

The study was conducted to model Wi-Fi password resource assets in a platform that can be shared and collaborated publicly securely and support dynamic data changes with online repository shortcuts documented in access support via dedicated search engines and QR CODE. This study uses 3 methods, namely the one-way SHA-256 HASH function which was formulated with the addition of sowing techniques and reversing techniques so as to produce a long String named Keycode, the second method uses modern cryptographic techniques, namely Digital Signature, which collects keycodes in Path the identity of the resource asset, and the last one is a QR CODE used as an access shortcut that collects digital signature access data. This study used testing data from comparator application contributors, namely wifimap.io randomly, the results of which the formulation results were then disassembled using the brute force technique using hashcat. The results of the research of password data from resources were successfully formulated into a combination of Strings with high confidentiality that cannot be disassembled to the original data but are still accessible to the owner and holder of the keycode that is balanced with the limitations of access control.

Keywords: Hashing, SHA-256, Wi-Fi, Computer Network, Digital Signature, QR CODE.

DAFTAR ISI

LEMBAR PERSEMBAHAN.....	ii
PERNYATAAN.....	.iii
LEMBAR PERSETUJUAN DAN PENGESAHAN TUGAS AKHIRiv
KATA PENGANTAR.....	v
ABSTRAK	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiv
BAB I.....	1
PENDAHULUAN.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Maksud dan Tujuan Penelitian.....	3
1.2.1. Maksud Penelitian	3
1.2.2. Tujuan Penelitian.....	3
1.3. Metode Penelitian	4
1.3.1 Analisis Penelitian.....	4
1.3.2 Metode Pengumpulan data	6
1.4. Ruang Lingkup.....	6
1.4.1. Perumusan Masalah	6
1.4.2. Batasan Masalah	7
BAB II	9
LANDASAN TEORI.....	9
2.1. Kajian Pustaka	9
2.1.1. Jaringan Komputer	9
2.1.2. Keamanan Jaringan Komputer.....	11

2.1.3 Wi-Fi (Wireless Fidelity)	13
2.1.4. Password	15
2.2. Dasar Program	15
2.2.1 Python Programming	15
2.2.2. Flask Framework	16
2.2.3. MySQL Database	19
2.2.4. Front End (Pengkodean Bagian Depan)	20
2.2.5. DevOps (<i>Development</i> dan <i>Operation</i>)	20
2.3. Rujukan Penelitian	22
2.3.1 Kajian Metodologi yang digunakan	23
BAB III	26
PERANCANGAN	26
3.1. Software Arsitektur	26
3.2. Bisnis Proses	28
3.2.1 Wireframe	29
3.2.2 Komponen Diagram	30
3.2.3 Use Case Diagram	31
3.2.4 Database	35
3.2.5 Sequence Diagram	37
3.3. Struktur Logika Utama	42
3.4. Sistem Kendali	42
BAB IV	44
IMPLEMENTASI	44
4.1. Implementasi Sistem	44
4.1.1. Informasi Sistem	44
4.1.2. Tampilan Sistem	46
4.2. Data Testing	67
4.3. Keycode One Way Hash Testing	68
BAB V	71
PENUTUP	71

5.1. Kesimpulan	71
5.2. Saran	72
DAFTAR PUSTAKA	74
Lampiran 1 Listing program	77
Lampiran 2. Dokumentasi konfigurasi Virtual Private Server	81
Lampiran 3. Bimbingan	82

DAFTAR GAMBAR

Gambar 2.1. Implementasi Hash satu arah.....	24
Gambar 2.2 dokumentasi QR CODE.....	25
Gambar 3.1. ECSA Software Arsitektur.....	26
Gambar 3.2. Wireframe depan.....	29
Gambar 3.3. Wireframe hasil transaksi kode.....	30
Gambar 3.4. Komponen diagram.....	30
Gambar 3.5. aktivitas pengguna pada platform ECSA.....	31
Gambar 3.6. Interaksi utama pengguna dengan sistem ECSA.....	34
Gambar 3.7. Relasi antara tabel.....	35
Gambar 3.8. Struktur database.....	36
Gambar 3.9. Sequence diagram registrasi pengguna.....	38
Gambar 3.10. Sequence diagram login pengguna.....	39
Gambar 3.11. Sequence diagram menambah sumber daya.....	40
Gambar 3.12 Sequence diagram menambah grup kolaborasi.....	41
Gambar 4.1. Tampilan depan.....	46
Gambar 4.2. Tampilan Login Pengguna.....	47
Gambar 4.3. Dark Mode Login Pengguna.....	47
Gambar 4.4. Tampilan Pendaftaran Akun.....	48
Gambar 4.5. DarkMode Pendaftaran Akun.....	49
Gambar 4.6. Tampilan Lupa Sandi.....	49
Gambar 4.7 DarkMode Lupa Sandi.....	50
Gambar 4.8. Dashboard.....	50

Gambar 4.9. DarkMode Dashboard	51
Gambar 4.10. Verifikasi Pin Akses.....	52
Gambar 4.11. Verifikasi Pin DarkMode	52
Gambar 4.12. Membuat pin keamanan	53
Gambar 4.13. DarkMode pin keamanan	53
Gambar 4.14. Tampilan MyAssets.....	54
Gambar 4.15. DarkMode MyAsets	54
Gambar 4.16. Tampilan QR Code.....	55
Gambar 4.17. DarkMode QR CODE	55
Gambar 4.18. Tampilan cetak QR CODE.....	56
Gambar 4.19. Tampilan Redeem Keycode	56
Gambar 4.20. DarkMode Redeem Keycode	57
Gambar 4.21. Tampilan pembaruan sumber daya	57
Gambar 4.22. DarkMode pembaruan sumber daya	58
Gambar 4.23. Tampilan Kolaborasi	58
Gambar 4.24. DarkMode Kolaborasi	59
Gambar 4.25. Tampilan Aset Grup.....	59
Gambar 4.26. DarkMode Aset Grup.....	60
Gambar 4.27. Menambahkan grup.....	60
Gambar 4.28. DarkMode menambah grup.....	61
Gambar 4.29. bergabungkolaborasi	61
Gambar 4.30. DarkMode bergabung kolaborasi	62
Gambar 4.31. Halaman Bantuan	62
Gambar 4.32. Data tidak ditemukan	63

Gambar 4.33. Aktivasi akun berhasil.....	64
Gambar 4.34. Token Kadaluarsa.....	64
Gambar 4.35. generate token aktivasi.....	65
Gambar 4.36. peringatan kombinasi user pengguna tidak sesuai.	65
Gambar 4.37. peringatan akun sudah terdaftar	66
Gambar 4.38. peringatan Email tidak ditemukan.....	66
Gambar 4.39. Required Form isian	67
Gambar 4.40. Data kontributor Wifimap.io	68
Gambar 4.41. keycode testing.....	69
Gambar 4.42. Implementasi sistem Versi 3.0	70

DAFTAR TABEL

Tabel 1.1. Fungsi Hash	5
Tabel 2.1. Contoh baris code di flask sederhana.....	17
Table 2.2 struktur Flask pada umumnya	18
Tabel 2.3. MySQL config di flask	20
Tabel 3.1. keamanan aplikasi tambahan	28
Tabel 3.2. Testing Code logika Utama	42
Tabel 3.3. Tabel kendali sistem ESCA	43
Tabel 4.1. Informasi Program	44