BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi kian bergerak mengikuti kebutuhan manusia modern yang merambah di berbagai sektor kehidupan, baik bisnis, kesehatan, gaya hidup, seni budaya, pendidikan, dan sektor vital lain yang turut terlibat. Perkembangan selalu menghadirkan buah pembaruan yang cukup nyata dalam wujud infrastruktur, konektivitas, pengelolaan data, keamanan dan sumber daya manusia yang terus menyumbangkan masalah dalam tata kelola teknologi informasi yang rinci, oleh karenanya kesiapan pada berbagai lini menjadi masalah tersendiri untuk mulai mengadopsi model teknologi informasi yang lebih baik.

Model teknologi yang dibangun sejatinya harus dapat mengakomodasi kebutuhan proses bisnis antara pemilik dengan target pengguna, tidak hanya berbicara dalam segi kualitas transaksi di dalamnya, namun lebih awal pada pintu gerbang utama, dalam hal ini akses dan konektivitas menjadi bagian besar topik yang akan dilirik, tentunya akses yang baik akan memberikan pengalaman pengguna yang menyenangkan dan secara tidak langsung dapat menaikan kesempatan adanya perputaran transaksi yang lebih besar. Penting adanya konsep perencanaan pada permasalahan akses sebagai landasan terdepan yang dapat mempresentasikan kesiapan dari fitur teknologi yang akan ditawarkan, sebagai jembatan yang dapat menyuplai sumber daya sekarang maupun di masa yang akan datang.

Pada akses penyebaran konektivitas dalam jaringan WiFi (*Wireless Fidelity*), pengguna cukup familiar dengan proses autentikasi sandi keamanan atau beberapa pengguna mengenalnya sebagai *user login* untuk dapat menikmati sebuah layanan, baik akses pengguna dari perangkat seluler, laptop atau personal komputer yang dibekali dengan adapter tambahan. Pada praktek dan penyebarannya sangat jarang

administrator atau pemilik menerapkan keleluasaan pada akses publik untuk dapat dengan mudah memperoleh akses secara langsung, kebanyakan pengguna yang ingin terhubung ke suatu jaringan harus bertanya pada *super user* (pemilik) atau delegasinya sebagai prosedur keamanan yang selalu menjadi isu tersendiri, misalnya ancaman keamanan yang cukup terkenal yaitu *WannaCry,* atau *Brute force Attack* dalam sebuah penelitian mengenai penetrasi jaringan yang mengangkat topik *Brute Force*, membongkar kata kunci dari keamanan *WiFi* secara acak untuk mendapatkan sandi yang pas berdasarkan *wordlist* yang memuat ribuan kata kunci [1] . Serangan yang memanfaatkan *vulnerable port* seperti *WannaCry* bisa saja terjadi lagi, terutama pada jaringan publik seperti publik *WiFi* yang sering dijumpai di cafe, restoran, hotel maupun *airport* [2].

Terdapat kelebihan tersendiri ketika masalah keamanan turut diperhatikan namun beberapa hal terkadang menyulitkan ketika proses penerapannya tidak sesuai dengan kebutuhan atau berlebihan. Pengguna publik dengan ruang lingkup akses yang berbeda di setiap waktunya akan kesulitan untuk menikmati layanan dan cenderung untuk tidak menggunakannya, sehingga mendapatkan kesan negatif yang dapat berdampak pada perputaran bisnis, di mana sebelumnya layanan internet hanya sebagai fasilitas tambahan namun beralih inti dari layanan yang sangat diharapkan oleh penggunanya.

Fasilitas akses konektivitas pada layanan publik dalam ruang lingkup internal seperti restoran, cafe, sarana hiburan, atau fasilitas umum lainnya dapat menjadi nilai tersendiri dalam meningkatkan keuntungan bisnis ketika mampu dikelola dengan tepat, berangkat dalam permasalahan tersebut penelitian **IMPLEMENTASI KEAMANAN ASET SANDI WIFI DENGAN METODE ONE WAY HASH SHA-256 dan QR CODE**, dapat menjadi jawaban dalam meningkatkan ketersediaan koneksi yang fleksibel serta aman di area publik atau lingkungan internal. Selain itu sebagai pembeda pada penerapan layanan konektivitas dengan ketersediaan, seperti model terintegrasi atau menjadi anggotanya terlebih dahulu untuk mendapatkan layanan.

1.2. Maksud dan Tujuan Penelitian

1.2.1. Maksud Penelitian

Penelitian ini mempunyai titik berat pada pengelolaan aset sandi *Wifi* sebagai repositori publik yang dapat diakses dengan pengenal aset digital yang sebagai kode uniknya, dipersembahkan untuk pemilik jaringan agar mempermudah pengelolaan aset sumber daya, pelaku bisnis atau instansi yang memiliki kontrol pada fasilitas publik untuk dapat meningkatkan layanan, serta para pengguna yang tidak mudah menukar informasi pribadinya untuk fasilitas layanan internet *WiFi* sekali pakai yang mengharuskan untuk terdaftar sebagai anggota terlebih dahulu.

1.2.2. Tujuan Penelitian

Adapun tujuan penelitian dalam dokumentasi pada permasalahan yang diangkat adalah sebagai berikut:

1. Menyederhanakan proses akses layanan internet *WiFi* publik tanpa harus melibatkan *super user* atau administrator dan delegasinya secara langsung.
2. Memberikan hak Privasi kepada pengguna tanpa mengurangi layanan fasilitas yang diterima.
3. Sebagai wadah Repositori induk yang menjadi pendoman dalam penggunaan berulang secara dinamis.
4. Mengkolaborasikan model keamanan kriptografi modern dalam konektivitas jaringan *WiFi* dengan peran *Digital Signature*.
5. Mengkolaborasikan pengembang aplikasi yang masuk pada ranah jaringan komputer dengan sajian model keamanan yang bervariasi.
6. Mempermudah cakupan berbagi aset sandi dengan fitur kolaborasi antar pengguna secara aman.
7. Membuat model akses dengan *QR Code* yang dapat dimanipulasi data di dalamnya tanpa harus merubah struktur dari *QR Code* yang telah ada sebelumnya, sehingga cukup satu kali cetak secara fisik sebagai pintasan.

1.3. Metode Penelitian

1.3.1 Analisis Penelitian

Metode analisis penelitian dalam menunjang permasalahan penelitian ini menggunakan tiga metode yaitu penerapan Hash satu arah, *Digital Signature* dan *QR Code* :

1. Kriptografi Satu Arah Atau One Way HASH

Algoritma Kriptografi terdiri dari enkripsi yang dapat merubah pesan (*plain text*) menjadi pesan yang sulit untuk dibaca atau dimengerti (*cipher text)* dan deskripsi digunakan untuk mengembalikan pesan tersebut ke bentuk awalnya, dalam penelitian ini yang akan digunakan adalah metode enkripsi yang menjadi pengenal unik untuk setiap aset perangkat *WiFi* yang berisi identitas, sandi dan informasi perangkat lainnya, tanda tangan digital menjadi bagian dalam model kriptografi modern yang dapat memberikan kepastian dalam isi dokumen didalamnya. Fungsi *hash* satu arah menggambarkan model fungsi kode alfanumerik yang panjang dan bekerja dalam satu arah, dimana data yang sudah diubah tidak dapat dikembalikan lagi kesemula.

Jenis kriptografi yang digunakan yaitu teknik *HASH SHA-256* yang dipadukan dengan teknik penaburan yang sering dikenal *SALT* yang ditambah dengan metode pembalik atau *reverse* sebagai tambahan keamanan dalam dokumentasi aksesnya, dimana setiap aset yang telah ditambahkan dapat memiliki pengenal keamanannya tersendiri yang secara otomatis dikirim oleh sistem. Model sistem yang dikembangkan dapat berupa akses publik yang memiliki ketetapan *Digital signature* dan *Private* yang dapat berubah serta tidak bisa diakses oleh sembarang user.

Tabel 1.1. Fungsi *Hash*

Algoritma	Ukuran Message Digest(bit)	Ukuran Blok Pesan	Kolisi
MD4	128	512	Hampir
MD5	128	512	Ya
SHA-256/224	256/224	512	Tidak
SHA-512/384	512/384	1024	Tidak

Tabel 1.1. Fungsi *Hash* diatas menjelaskan bagaimana beberapa fungsi *hash* yang berkembang dan sering digunakan misalnya yang cukup familiar yaitu *MD5,* namun penelitian ini akan membahas secara khusus penggunaan fungsi *hash SHA-256*. *SHA-256* dianggap lebih aman karena didesain sedemikian rupa sehingga tidak memungkinkan mendapat pesan yang berhubungan dengan *message digest,* atau untuk menemukan dua pesan yang berbeda yang menghasilkan *message digest* yang sama [3] .

2. Digital Signature

Digital Signature atau tanda tangan digital digunakan untuk autentikasi pada data aset yang di akses merupakan data sebenarnya, jika tidak sesuai dengan ketersediaan sumber daya, maka data tidak akan dapat disajikan. Tanda tangan digital menjadi salah satu model teknik kriptografi modern yang sering dipakai, misalnya untuk sertifikasi tanah, bangunan, dokumen aset, dimana cara kerja dan kegunaan *Digital signature* mirip dengan tanda tangan dalam versi nyata, yaitu untuk memberikan kepastian, keaslian dan persetujuan dokumen oleh penanda tangan [4].

Tanda tangan digital dengan konsep kriptografi model *One way hash* bekerja dengan prinsip enkripsi satu arah yang nilainya tidak dapat dapat dikembalikan namun akan diterjemahkan langsung oleh *database* ketika tersedia dan menampilkan informasi sumber daya kepada pengakses.

keuntungan menerapkan model *digital signature* yaitu memiliki tingkat keamanan yang lebih kuat, sehingga menambah rasa aman pada sumber data agar tidak diakses ilegal.

3. QR Code

QR Code atau *Quick Response Code* menjadi metode interaksi yang digunakan untuk mempermudah akses aset data yang berisikan informasi sandi *WiFi* menjadi lebih mudah, kombinasi *string* rumit dan panjang pada digital signature yang dihasilkan dari metode *one way hash* pada setiap aset dapat dibungkus dengan *QR Code* yang dapat mengubah data tertulis menjadi 2 dimensi kedalam gambar yang lebih ringkas. *QR code* sendiri adalah matrik dua dimensi (*barcode*) dengan pembacaan yang cepat dan kapasitas penyimpanan karakter yang lebih besar [5].

1.3.2 Metode Pengumpulan data

Adapun metode pengumpulan data yang digunakan yaitu dengan melalui serangkaian data yang ditambahkan oleh partisipasi pengguna secara dinamis dan realtime serta adanya data *default* yang ditambahkan oleh pemilik sebagai acuan.

1.4. Ruang Lingkup

Lingkup masalah selalu menjadi titik temu dalam perumusan dan batasannya, dalam hal ini beberapa poin yang mendukung hal tersebut adalah sebagai berikut:

1.4.1. Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas, penelitian ini merumuskan berbagai masalah, diantaranya adalah sebagai berikut:

1. Bagaimana menyajikan akses koneksi yang mudah, aman serta mampu mendukung pembaruan dokumentasi kata sandi yang dinamis?
2. Bagaimana menyajikan layanan akses internet yang dapat dimanfaatkan kapanpun untuk akses publik, tanpa harus menanyakan informasi sumber daya dan sandi pada pemilik secara langsung?

3. Bagaimana membangun sebuah sistem konektivitas tanpa harus melibatkan data keanggotaan pengguna yang cukup sensitif atau perlu upaya lebih.
4. Bagaimana membangun layanan modern dan *user Friendly* pada akses berbagi koneksi internet?
5. Bagaimana membuat fasilitas akses layanan internet menjadi daya tarik yang dapat meningkatkan peluang terjadinya transaksi bisnis?
6. Bagaimana mempermudah dokumentasi administrator jaringan ketika menangani sumber daya yang banyak, tanpa harus mengingat setiap kombinasi sandi akses secara khusus.
7. Bagaimana menyajikan dokumentasi aset yang dapat digunakan kembali tanpa harus merubahnya secara fisik data *Real Time*.

1.4.2. Batasan Masalah

Berikut adalah batasan masalah dalam merumuskan dokumentasi pada permasalahan yang diangkat, diantaranya sebagai berikut:

1. Merancang sebuah sistem yang menjadi wadah untuk menyimpan aset data *WiFi*, baik *SSID*, *password* dan deskripsi pendukung lain yang dibangun dengan model Web Aplikasi agar dapat diakses di berbagai perangkat, dimana Bahasa pemrograman yang digunakan yaitu *python* dengan *Framework FLASK*.
2. Proses Keamanan pada berbagai *password* dibuat dalam dua model, yaitu akses *public* dan *private*.
3. Disajikan fitur kolaborasi group yang dapat terpublikasi dan tidak terpublikasi.
4. Model kriptografi yang disajikan tersaji pada kombinasi perubahan string karakter yang menjadi link akses serta keamanan tingkat lanjut pada Web aplikasi.
5. Model keamanan yang diterapkan dalam metode membahas lebih mengenai *digital signature*, Enkripsi satu arah (*One way hash*) yang tidak bisa dikembalikan ke nilai semula dengan *SHA-256* dan Basis keamanan tambahan.

6. Model *Digital signature* disajikan sebagai bentuk akses pada aset data dengan penambahan unik karakter *HASH* dan *SALT*.
7. Model *QR Code* tersaji sebagai pintasan untuk mengakses aset dengan pengenal unik yang terenkripsi dengan fungsi kriptografi *hash* yang cukup panjang dan rumit.