BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu menjadi salah satu acuan penulis dalam pembuatan laporan akhir ini, sehingga penulis dapat memperkaya teori yang digunakan dalam mengkaji penelitian keamanan data dengan menggunakan *JSON Web Token* (JWT).

Rujukan penelitian yang pertama yaitu dari Rohmat Gunawan dan Alam Rahmatulloh dalam Jurnal Edukasidan Penelitian Infromatika (JEPIN) yang berjudul *JSON Web Token* untuk *Authentication* pada Interoperabilitas Arsitektur berbasis *RESTful Web Service*. Dalam penelitiannya, pada aplikasi *blood donors* proses otentikasi dan otorisasi pada *RESTful web service* dikontrol oleh *backend system* yaitu *JSON Web Token*. Setelah proses *login* berhasil *server* memberikan respon berupa JWT token sebagai kunci untuk mengakses sumber daya yang ada di *server* (Gunawan dan Rahmatulloh, 2019 : 76).

Rujukan penelitian selanjutnya yaitu jurnal A.W.P. Putra, A. Bhawiyuga dan M. Data dengan judul Implementasi Autentikasi *JSON Web Token* (JWT) sebagai Mekanisme Autentikasi Protokol MQTT pada Perangkat NodeMCU. Dalam penelitiannya dilakukan pengujian *expiration token* JWT untuk melihat apakah *server* dapat melakukan autentikasi terhadap token yang telah *expired*. Skenario dari pengujian ini adalah ketika *publisher* telah mendapatkan token, maka token tersebut digunakan untuk melakukan komunikasi selanjutnya atau publish ke *broker*. Ketika token telah *expired*, maka *server* akan melakukan autentikasi dan menampilkan pesan *error* (Putra dkk, 2018: 588).

Sedangkan penelitian yang akan dilakukan penulis saat ini tidak jauh berbeda dengan penelitian sebelumnya yaitu implementasi JSON *Web Token* untuk digunakan sebagai kunci oleh *user* untuk melakukan beberapa aktivitas pada sistem.

2.2 Pengertian Sistem

Sistem berasal dari kata Yunani yang artinya kesatuan. Suatu sistem terdiri dari elemen-elemen yang saling berinteraksi untuk mencapai tujuan tertentu. Sistem adalah jaringan kerja yang terdiri dari prosedur-prosedur yang saling berhubungan, berkumpul sama-sama untuk melakukan suatu kegiatan atau menyelesaikan suatu sasaran tertentu. Menurut Jogianto (1995) suatu sistem dapat didefinisikan sebagai satu kesatuan yang terdiri dari dua atau lebih komponen atau subsistem yang berinteraksi untuk mencapai tujuan (Wahyudi, 2015 : 11).

Pengertian sistem secara umum adalah suatu kumpulan objek atau unsur-unsur atau bagian-bagian yang memiliki arti berbeda-beda yang saling memiliki hubungan, saling berkerjasama dan saling memengaruhi satu sama lain serta memiliki keterikatan pada rencana yang sama dalam mencapai suatu tujuan tertentu pada lingkungan yang kompleks. Sedangkan definisi sistem secara singkat adalah sekumpulan benda yang memiliki hubungan di antara mereka.

Menurut KBBI (Kamus Besar Bahasa Indonesia), pengertian sistem adalah sebagai berikut:

1. Perangkat unsur yang secara teratur saling berkaitan sehingga membentuk suatu totalitas.
2. Susunan yang teratur dari pandangan, teori, asas, dan sebagainya.
3. Metode.

Ada beberapa elemen-elemen yang membentuk sistem, yang akan dijelaskan dibawah ini:

1. **Objek**, merupakan bagian, elemen atau variabel. Objek dapat berupa benda fisik, abstrak atau keduanya.
2. **Atribut**, merupakan penentu kualitas atau sifat kepemilikian sistem dan objeknya.
3. **Hubungan internal**, merupakan penghubungan diantara objek-objek yang terdapat dalam sebuah sistem.
4. **Lingkungan**, merupakan tempat dimana sistem tersebut berada.

5. **Tujuan**, Setiap sistem memiliki tujuan dan tujuan inilah yang menjadi motivasi yang mengarahkan sistem.
6. **Masukan**, adalah sesuatu yang masuk ke dalam sistem dan selanjutnya menjadi bahan untuk diproses.
7. **Proses**, Bagian yang melakukan perubahan dari masukan menjadi keluaran.
8. **Keluaran**, adalah hasil dari proses. Pada sistem informasi berupa informasi atau laporan.
9. **Batas**, adalah pemisah antara sistem dan daerah luar sistem (Sumber: www.zonareferensi.com).

2.3 Pengertian Kampus Pintar (Smart Campus)

Kampus pintar atau *smart campus* memiliki artian bahwa fasilitas-fasilitas pendukung semua kegiatan civitas akademika dalam melaksanakan kewajiban Tri Dharma Perguruan Tinggi melibatkan teknologi informasi sebagai tulang punggung pendukung. Penerapan teknologi kampus pintar dapat berupa *smart class room, smart laboratorium, smart department, smart faculty* dan lain-lain (Cordiaz, 2017).

Smart Campus berasal dari bahasa inggris yang artinya Kampus Pintar, untuk konsepnya sendiri merupakan konsep sebuah kampus yang menerapkan dan memadukan sistem pembelajaran dengan penggunaan Teknologi Informasi. Jadi, *Smart Campus* itu intinya adalah untuk mempermudah dalam kegiatan proses belajar-mengajar dengan memanfaatkan Teknologi Informasi. Penerapan Teknologi Informasi dengan menggunakan sistem *Smart Campus ini*, tidak hanya mempermudah dalam proses belajar-mengajar, tapi juga dalam proses untuk kepentingan urusan manajemen kampus, perpustakaan dan lain sebagainya. Sebagai contoh dari penerapan *Smart Campus* adalah dengan penggunaan Sistem Akademik Terintegrasi. Dengan menggunakan Sistem Akademik Terintegrasi yang ada pada *Smart Campus*, pegawai dapat menggunakan data perkuliahan mahasiswa untuk digunakan pada kepentingan sistem yang lainnnya. Misalnya pada sistem Keuangan *(Finance), Library, Smart Cafe, Smart Parking,* Beasiswa dan kepentingan lainnya.

Adapun beberapa kelebihan dalam menggunakan smart campus ini antaranya:

1. Pegawai kampus tidak perlu menginput data mahasiswa yang sama berulang-ulang, cukup sekali input. Inputan data ini juga dapat diambil dari sistem SPMB (Sistem Penerimaan Mahasiswa Baru) yang sebelumnya terlebih dahulu telah diinput sendiri oleh calon mahasiswa yang bersangkutan saat ingin mendaftar di Perguruan Tinggi tersebut sehingga pegawai tidak perlu menginputkannya kembali.
2. Mengurangi duplikasi data. Data merupakan hal yang vital di perguruan tinggi. Bisa dibayangkan, setiap tahun perguruan tinggi akan menerima sekian banyak mahasiswa sehingga semakin lama data pada perguruan tinggi akan semakin meningkat. Jika sistem informasi yang dibuat diperguruan tinggi tersebut tidak dibuat secara terintegrasi antara satu sistem dengan sistem yang lainnya, maka bisa saja akan terjadi duplikasi data dan ini akan membuat sistem informasi pada Kampus bersangkutan menjadi kacau sehingga akan banyak mengeluarkan waktu, uang dan juga tenaga demi mengelola data-data yang ganda. Untuk itulah diperlukan Sistem Informasi Terintegrasi (Sumber: www.garudacyber.co.id).

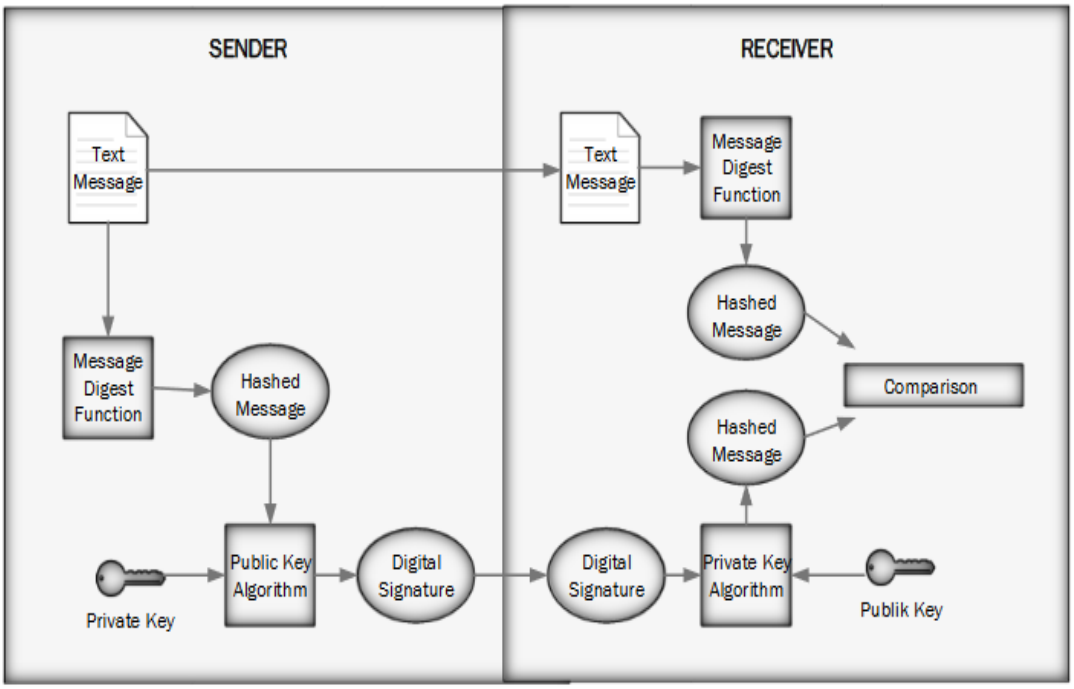
2.4 Pengertian Tanda Tangan Digital

Tanda tangan digital adalah stempel autentikasi elektronik yang dienkripsi pada informasi digital seperti pesan *email,* makro, atau dokumen elektronik. Tanda tangan mengonfirmasi bahwa informasi berasal dari penanda tangan dan bersifat orisinil (Sumber: www.support.microsoft.com).

Perdana (dalam Cahyo, 2017) menjelaskan bahwa salah satu konsep pada kriptografi modern adalah *digital signature*. Cara kerja dan kegunaan *digital signature* mirip dengan tanda tangan dalam versi nyata, yaitu untuk memberikan kepastian keaslian dan persetujuan dokumen oleh penanda tangan. Dalam *digital signature*, “tanda tangan” adalah dalam bentuk digital yang digunakan untuk mensahkan sebuah dokumen digital. Prinsip yang digunakan dalam tanda tangan digital ini adalah dokumen yang dikirimkan harus ditandatangani oleh pengirim dan tanda tangan bisa diperiksa oleh penerima untuk memastikan keaslian dokumen yang dikirimkan. Fungsinya adalah untuk melakukan validasi terhadap data yang dikirim. Tanda tangan digital menggunakan algoritma yang disebut dengan istilah *hashing algorithm*. Fungsi tersebut akan menghasilkan sebuah

kombinasi karakter yang yang unik yang disebut *message digest*. Dengan cara ini pengirim bertanggung jawab terhadap isi dokumen dan dapat di cek keaslian dokumen oleh penerima. Keunikannya adalah jika di tengah perjalanan data mengalami modifikasi, penghapusan maupun di sadap diam-diam oleh *hacker* walaupun hanya 1 karakter saja, maka *message digest* yang berada pada si penerima akan berbeda dengan yang dikirimkan pada awalnya. Keunikan lainnya adalah *message digest* tersebut tidak bisa dikembalikan lagi ke dalam bentuk awal seperti sebelum disentuh dengan fungsi algoritma, sehingga disebutlah sebagai *one-way hash.*

Fungsi utama dari tanda tangan digital pada pada aspek keamanan kriptografi adalah *non-repudiation* atau anti penyangkalan dimana apabila dokumen valid maka pengirim tidak bisa menyangkal bahwa keberadaan dokumen benar dikirim oleh pengirim yang bersangkutan.



Gambar 2.1 Skema *Digital Signature*

Cara kerja *digital signature* seperti yang terlihat pada Gambar 2.1 adalah sebagai berikut:

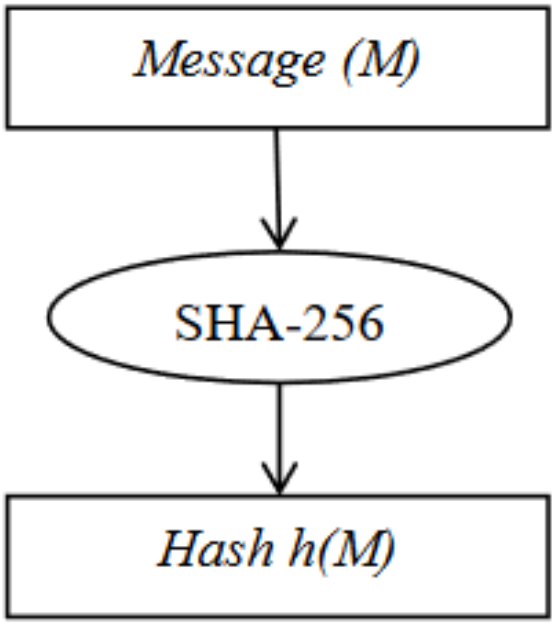
1. *Sender* melakukan proses *hashing algorithm* untuk menghasilkan *message digest* dari sebuah pesan yang terdapat dalam sebuah dokumen yang akan dikirim.
2. Setelah dilakukan *hashing, sender* melakukan *sign* terhadap *message digest* dengan menggunakan kunci publik yang digunakan untuk membentuk *digital signature*.
3. Kemudian *sender* mengirimkan *digital signature* bersama dokumen tersebut kepada *receiver.*
4. *Receiver* merima pesan yang dikirimkan oleh *sender*.
5. Setelah itu *receiver* mengverifikasi pesan yang dikirimkan oleh *sender*.

Pada proses verifikasi tersebut pesan di *hashing* terlebih dahulu sehingga menghasilkan *message digest* dan *digital signature* akan di *unsign* menggunakan *kunci private*. Jika *message digest*-nya sama, maka pesan ini adalah asli dan pesan berasal dari pengirim yang sebenarnya. Bila pesan telah diubah oleh pihak luar, maka *message digest* juga ikut berubah. Proses diatas mampu membuktikan bahwasanya pesan adalah asli (*message authentication*) dan orang yang mengirim adalah orang yang sebenarnya *(user authentication*). Ini berarti *digital signature* memenuhi salah satu syarat keamanan jaringan yaitu *non-repudiation* atau nir penyangkalan (Cahyo, 2017).

2.5 Algoritma HMAC SHA-256

Keyed-Hash Message Authentication Code (HMAC) merupakan metode yang digunakan untuk memastikan integritas serta autentikasi sebuah data melalui algoritma *hash* yang diproses bersama dengan private key. HMAC menjamin autentikasi karena adanya *private key*, sedangkan integritas data diperoleh dari algoritma *hash* yang digunakan,salah satunya SHA-256. Algoritma SHA-256 merupakan algoritma *hash* dari jenis SHA-2 yang menghasilkan *message digest* sepanjang 256 bit. Algoritma SHA-256 dapat digunakan untuk melakukan pengecekan integritas data, pembuatan *digital signature*, dan lain-lain. SHA-256 dapat menerima input pesan hingga 264bit yang akan diproses melalui blok dengan ukuran 512 bit (Anugrah dkk, 2019).

Secure Hash Algorithm-256 adalah salah satu jenis *hash* yang masih umum digunakan. Fungsi ini adalah varian dari SHA-1, SHA-256 dibuat karena telah ditemukan bentrokan dari SHA-1, SHA-1 sendiri adalah pengganti dari SHA-0. Sampai saat ini belum ada yang dapat memecahkan algoritma untuk SHA-256. SHA-256 umumnya digunakan sebagai fungsi antara untuk fungsi lain, termasuk fungsi *hash* MAC, HMAC, dan beberapa fungsi penghasil *digital signature* (Cahyo, 2017). Fungsi utama SHA-256 dapat dilihat pada Gambar 2.2



Gambar 2.2 Fungsi Utama SHA-256

Fungsi utama SHA-256 menerima masukan berupa data atau pesan M dengan panjang sembarang, lalu akan menghasilkan nilai *hash* h(M) dengan panjang 256-bit. SHA-256 mempergunakan 6 fungsi logika, yang setiap fungsi tersebut beroperasi pada 32-bit *words* yang direperesentasikan sebagai x, y, and z. Hasil dari setiap fungsi merupakan sebuah 32-bit *word* baru. Berikut fungsi logika dalam SHA-256:

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\sum_0^{\{256\}}(x) = \mathrm{ROTR}^2(x) \oplus \mathrm{ROTR}^{13}(x) \oplus \mathrm{ROTR}^{22}(x)$$

$$\sum_1^{\{256\}}(x) = \mathrm{ROTR}^6(x) \oplus \mathrm{ROTR}^{11}(x) \oplus \mathrm{ROTR}^{25}(x)$$

$$\sigma_0^{\{256\}}(x) = \mathrm{ROTR}^7(x) \oplus \mathrm{ROTR}^{18}(x) \oplus \mathrm{SHR}^3(x)$$

$$\sigma_1^{\{256\}}(x) = \mathrm{ROTR}^{17}(x) \oplus \mathrm{ROTR}^{19}(x) \oplus \mathrm{SHR}^{10}(x)$$

Keterangan :

ROTR (Right-rotate)

SHR (Right-shift)

2.6 Pengertian Keamanan Data

Keamanan data adalah teknologi standarisasi yang melindungi data dari kerusakan, modifikasi, atau pengunggahan yang dilakukan secara ilegal baik disengaja atau tidak disengaja (Sumber: www.forcepoint.com). Terdapat beberapa aspek pada keamanan data dan informasi, antaranya :

1. *Privacy/Confidentiality* yaitu usaha menjaga data informasi yang bersifat pribadi dari orang yang tidak berhak mengakses.
2. *Integrity* yaitu usaha untuk menjaga data atau informasi tidak diubah oleh yang tidak berhak.
3. *Authentication* yaitu usaha atau metode untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar atau layanan dari *server* yang diberikan benar berasal dari *server* yang dimaksud.
4. Availability berhubungan dengan ketersediaan sistem dan data ketika dibutuhkan (Sumber : bkpsdmd.babelprov.go.id).

Menurut Riyadi Keamanan data terdiri dari beberapa macam, diantaranya "enkripsi, *firewall, secure socket layer, kriptografi dan pretty good privacy*.

1. Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak dapat dimengerti.

2. *Firewall*

Firewall adalah suatu keamanan yang bersifat seperti filter yang bertujuan untuk menjaga sebuah layanan akses dari orang yang tidak berwenang.

3. *Secure Socket Layer*

Secure Socket Layer adalah suatu bentuk penyandian data sehingga informasi rahasia seperti nomor kartu kredit atau kontrol otentikasinya tidak dapat dibaca atau diakses oleh pihak lain selain pemiliknya dan *server* (pemilik servis).

4. Kriptografi

Kriptografi adalah seni menyandikan data, algoritma yang digunakan pada kriptografi berhubungan dengan penyembunyian data.

5. *Pretty Good Privacy*

Pretty Good Privacy adalah salah satu algoritma keamanan komunikasi data melalui internet komunikasi harian semacam *electronic mail*".

Adapun pada sistem JSON *Web Token* (JWT) masuk ke kategori enkripsi, karena proses yang dilakukan JWT yaitu mengubah data atau informasi menjadi kode acak yang tidak dapat dimengerti.

2.7 Pengertian JSON *Web Token*

JSON *Web Token* (JWT) adalah sebuah *random* token berbentuk *string* panjang yang digunakan untuk melakukan sistem otentikasi dan pertukaran informasi. Token yang dihasilkan akan disimpan oleh *user* pada *cookies browser* atau *local storage*, ketika *user* ingin mengakses halaman tertentu maka harus menyertakan token tersebut. Untuk struktur JWT terdiri dari tiga bagian yaitu *header, payload dan signature* (Sumber : www.jwt.io).

1. *Header*

Header biasanya terdiri dari Algoritma HS256 yang digunakan dan tipe JWT sebagai defaultnya.

```
{
        "alg": "HS256",
        "typ": "JWT"
}
```

2. *Payload*

Berisi data atau informasi yang ingin dikirimkan ke *server* JWT misalnya berupa id, nama *user* dan lain lain.

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

3. *Signature*

Hasil gabungan dari *header* dan *payload* yang telah di *encode* serta penambahan kode *secret*nya.

```
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
secret)
```

Dari ketiga bagian tersebut akan digabung dan otomatis di enkripsi menjadi token *string random* panjang seperti dibawah ini :

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM
0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM
5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```