BAB I
PENDAHULUAN

1.1. Latar Belakang

Di era digital seperti sekarang ini, tentu data merupakan hal yang tidak asing lagi. Data selalu berhubungan dengan segala aspek kehidupan manusia. Misalnya, setiap mendaftar pada suatu situs atau melakukan selancar menggunakan mesin pencari, dapat dipastikan bahwa akan selalu berhubungan dengan data.

Data merupakan suatu informasi, terutama fakta atau angka yang dikumpulkan untuk diolah serta digunakan untuk membantu pengambilan keputusan atau informasi dalam bentuk elektronik yang dapat disimpan dan digunakan oleh komputer [1]. Menurut Tata Sutabri (2016), data yaitu suatu istilah majemuk yang berarti fakta atau bagian dari fakta yang mengandung arti yang dihubungkan dengan kenyataan, simbol-simbol, gambar-gambar, angka-angka, huruf atau simbol yang menunjukkan suatu ide, objek, kondisi, atau situasi [2]. Sedangkan Menurut Canggih Ajika Pamungkas (2017), data merupakan nilai yang merepresentasikan deskripsi dari suatu objek atau kejadian [3]. Berdasarkan pengertian data menurut para ahli diatas, dapat disimpulkan bahwa data merupakan suatu fakta atau angka yang dapat dapat diolah menjadi suatu informasi.

Pengguna internet di Indonesia dalam beberapa tahun terakhir mengalami peningkatan yang cukup signifikan. Dikarenakan kemudahan dalam memperoleh informasi melalui internet menjadi penyebab peningkatan jumlah pengguna [4]. Namun, hal tersebut tentunya harus diikuti dengan keamanan data. Keamanan dan kerahasiaan data menjadi hal yang sangat penting karena data tersebut bisa digunakan oleh orang yang tidak bertanggung jawab untuk berbuat kejahatan. Hal tersebut tentunya akan berakibat fatal bagi pemilik data apabila terjadi penyalahgunaan data. Untuk meningkatkan keamanan data, ada beberapa aspek yang perlu diperhatikan,

antara lain *privacy* (kerahasiaan), *integrity* (konsisten), *authenticity* (keaslian), *availability (*ketersediaan), dan *access control* [5]**.**

Menurut Harun Mukhtar (2019), *privacy* adalah kerahasiaan terhadap data agar tidak diketahui orang lain. *Integrity* dapat digunakan untuk menjamin bahwa data yang digunakan benar-benar asli yang dikirimkan oleh orang yang benar. *Authenticity* merupakan keaslian data yang diterima oleh penerima informasi. *Availability* merujuk pada ketersediaan data dan informasi dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Sedangkan *access control* berkaitan dengan pengaturan hak akses informasi pada suatu sistem komputer. Meskipun semua aspek diatas penting, namun yang harus mendapat perhatian khusus yakni pada aspek *authenticity* dan *access control*. Karena kedua aspek tersebut sering mendapatkan ancaman keamanan, maka diperlukan proses *authentication* dan *authorization* [5].

Di dalam membangun suatu sistem, tentunya keamanan sistem menjadi hal utama yang perlu diperhatikan. *Authentication* (autentikasi) dan *authorization* (otorisasi) akan sangat berpengaruh dalam menjaga hak akses dari pengguna serta mencegah terjadinya berbagai aktivitas peretasan yang umum dilakukan, yakni *MITM* (*Man In The Middle*) *Attack*. Maka dari itu, demi meningkatkan keamanan pada data akademik, maka juga ditekankan penggunaan algoritma *HMAC* (*Hash-Based Message Authentication Code*) untuk meningkatkan keamanan sistem dari sisi *authentication* dan *authorization* [6].

Fakultas Teknik, merupakan salah satu fakultas yang ada di Universitas Muhammadiyah Ponorogo yang menerapkan sistem pengelolaan perkuliahan berupa praktikum dan PKN (Praktek Kerja Nyata) berbasis digital. Namun, implementasi keamanan data akademik yang disimpan pada sistem tersebut masih kurang karena hanya menerapkan *basic authentication* (autentikasi dasar). *Basic authentication* merupakan skema paling sederhana dalam menerapkan autentikasi di *HTTP*. Pasalnya, kita cukup memberikan identitas *Basic user:password* yang telah di *encode* menggunakan *base64 string* pada

header authorization request HTTP untuk membuktikan bahwa kita adalah pengguna yang autentik [7]. *Basic authentication* memiliki keamanan yang kurang baik karena *base64 string* dapat di-*decoded* secara mudah tanpa ada pengamanan apa pun. Dalam hal ini, keamanan data akademik merupakan hal yang perlu diperhatikan, mengingat data tersebut sangat penting dan bisa saja terjadi manipulasi data.

Sebagai solusi keamanan, dapat menggunakan *JWT* (*JSON Web Token*). *JWT* adalah format token yang banyak digunakan pada *Token-Based Authentication*. *JWT* juga menjadi standar yang terbuka (*RFC 7519*) sebagai format dalam transaksi data *JSON* secara aman dalam bentuk token [8]. Selain itu, penggunaan *JWT* bisa dikombinasikan dengan algoritma *HMAC* untuk membuat dan memvalidasi keaslian token. Token *JWT* terdiri dari *header, payload*, dan *signature* yang di-*hash* dan divalidasi menggunakan algoritma *HMAC*, sehingga penerapan *JWT* dapat meningkatkan keamanan sistem apabila dibandingkan dengan *basic authentication*.

Dari permasalahan yang telah diuraikan diatas, maka diambil penelitian dengan judul "Implementasi *Authentication* & *Authorization* Berbasis *JWT* Pada Sistem Pengelolaan Perkuliahan Menggunakan Algoritma *HMAC*". Dengan demikian, penulis akan mengimplementasikan keamanan sistem dari sisi *authentication* dan *authorization* berbasis *JWT* menggunakan algoritma *HMAC* pada sistem pengelolaan perkuliahan di Fakultas Teknik Universitas Muhammadiyah Ponorogo. Sehingga nantinya bisa dihasilkan perangkat lunak yang teruji baik dari sisi fungsionalitas maupun keamanan sistem.

1.2. Perumusan Masalah

Dari latar belakang yang telah diuraikan diatas, maka rumusan masalah yang dapat diambil yaitu:

Bagaimana mengimplementasikan *authentication* dan *authorization* berbasis *JWT* pada sistem pengelolaan perkuliahan menggunakan algoritma *HMAC*?

1.3 Tujuan Penelitian

Tujuan diadakannya penelitian ini adalah:

Mengetahui cara implementasi keamanan sistem di sisi *authentication* dan *authorization* berbasis *JWT* menggunakan algoritma *HMAC*.

1.4 Batasan Masalah

Agar penelitian ini lebih terarah serta sesuai target, maka diperlukan batasan masalah sebagai berikut:

1. Sistem atau aplikasi berjalan di lingkup Fakultas Teknik Universitas Muhammadiyah Ponorogo.
2. Penelitian pada sistem ini lebih fokus kepada proses *authentication* dan *authorization*.

1.5 Manfaat Penelitian

Dari penelitian ini, diharapkan dapat memberikan berbagai manfaat, diantaranya:

1. Meningkatkan keamanan sistem pada sisi *authentication* dan *authorization* pada sistem pengelolaan perkuliahan di Fakultas Teknik Universitas Muhammadiyah Ponorogo.
2. Menanggulangi terjadinya penyalahgunaan kontrol akses pada sistem.
3. Token *JWT* bersifat *stateless* (tanpa harus disimpan pada basis data), sehingga cocok digunakan pada arsitektur *monolithic* maupun *microservices*.
4. Mengurangi latensi jaringan karena sifat *JWT* yang *stateless*.