1. Pendahuluan

Latar Belakang

Meningkatnya teknologi pada area internet mengakibatkan peningkatan jumlah aplikasi yang beredar.. Perkembangan ini memberikan kemudahan untuk menjangkau keinginan kedua sisi pembuat dan pengguna aplikasi. Aplikasi yang beredar saat ini memiliki tujuan yang beragam dari sosial media, gaya hidup, perbankan, dan lainnya. Banyak aplikasi menggunakan sistem autentikasi sebelum dapat diakses dan digunakan, ini bertujuan untuk memberikan keamanan dan kenyamanan sehingga tidak terjadi bentuk akses yang tidak sah.

Autentikasi memiliki beragam cara untuk mengidentifikasi, umumnya dibagi menjadi 3 faktor berbasis pengetahuan, kepemilikan, dan biometrik [1]. Faktor autentikasi yang berlaku memfokuskan kepada hal yang terdapat pada individu untuk memvalidasi akses. Penggunaan informasi individu untuk melakukan akses memiliki masalah pada sisi privasi jika informasi tersebut tersebar diluar sistem autentikasi. Penerapan sistem autentikasi yang memfokuskan kepada kenyaman pengguna dengan melakukan autentikasi secara pasif, memperlihatkan permasalahan pada privasi individu [2], Adapun bentuk lain sistem autentikasi yang berfokus dalam menjaga privasi dengan menggunakan informasi disekitar individu seperti lokasi, agar menjaga kerahasiaan informasi yang bersifat individual [3]. Permasalahan ini menjadi lebih serius dengan adanya penyerangan Man-in-the-middle atau serangan MITM yang dapat menyadap serta memanipulasi jalur komunikasi [4], [5].

Zero Knowledge Proof atau ZKP merupakan sebuah cara untuk menyembunyikan informasi yang bersifat sensitif dalam jalur komunikasi. Pengamanan dilakukan dengan mengubah data yang memiliki informasi sensitif pengguna dalam autentikasi, menjadi bentuk nilai ZKP sebagai autentikasi. Bentuk penerapan ZKP dalam autentikasi web [6] dan autentikasi data pada perangkat IoT [7] yang menyembunyikan data sensitif dalam proses autentikasi pengguna.

Penerapan keamanan ZKP pada privasi data membantu mencegah terjadinya kebocoran informasi, namun perlu diperhatikan bahwa sistem keamanan perlu memanfaatkan sumber daya dengan baik agar berjalan secara efesien dan efektif. Dalam penelitian berfokus kelayakan implementasi ZKP dalam bentuk autentikasi data dari penggunaan CPU dan Memori yang dipergunakan pada perangkat.

Topik dan Batasannya

Bentuk dari autentikasi data merupakan pengujian kredensial pada setiap pesan yang dikirimkan dari salah satu pihak dalam proses komunikasi. Pengujian kredensial ditujukan untuk memastikan bahwa pesan yang diterima berasal dari pihak yang benar dan sah dalam proses komunikasi yang dilakukan. Penerapan *zero knowledge proof* di dalam autentikasi data adalah pengujian kredensial yang disematkan dalam sistem autentikasi. Pihak yang sedang berkomunikasi dapat saling bertukar informasi tanpa menampilkan informasi yang bersifat sensitif.

Batasan dari sistem yang dibangun yaitu penggunaan bahasa pemrograman Python dalam pengembangan sistem karena kemudahan dalam pembuatan sistem namun memiliki kekurangan dalam segi efektivitas waktu proses sistem serta manajemen memori[8][9]. Pengujian yang digunakan dalam pengukuran sistem hanya dari pemanfaatan penggunaan CPU dan memori. Dikarenakan keterbatasan perangkat, sistem hanya berjalan pada satu perangkat dengan client berjalan menggunakan sistem operasi Windows dan server berjalan menggunakan virtual machine dengan sistem operasi Linux.

Tujuan

- Memberikan kinerja dari *zero knowledge proof* dalam sistem autentikasi data dari segi komputasi penggunaan CPU dan Memori.
- Pengujian keamanan sistem pada sisi kredensial dalam skenario uji yang diberikan.

Organisasi Tulisan

Bagian Studi Terkait melakukan pembahasan teori/studi/literatur yang menunjang dalam pencapaian tujuan dari topik pada penelitian ini. Dalam bagian sistem yang dibangun berisikan bentuk sistem, alur kerja sistem, dan bentuk pengujian sistem. Bagian berikutnya yaitu evaluasi pemaparan hasil pengujian serta analisis. Bagian terakhir kesimpulan memuat saran juga kesimpulan dari hasil pengujian serta analisis pengujian.