1. Pendahuluan

Latar Belakang

Penempatan parkir kendaraan telah menjadi masalah umum di kota-kota metro, terutama di mal mereka. Peningkatan polusi udara juga mengikuti karena lamanya waktu yang dibutuhkan pengemudi hanya untuk berkendara di sekitar area tersebut. Dengan kesadaran akan masalah tersebut, ide sistem parkir pintar mulai muncul di sekitar para peneliti. Tujuan sistem ini adalah untuk membantu pengemudi menemukan tempat kosong yang tersedia untuk ditempati tanpa harus berkeliling area parkir.

Sistem yang diusulkan berbasis komputasi awan untuk mengolah data mentah, aplikasi web API untuk mengolah data, aplikasi mobile untuk pengguna berinteraksi dengan sistem, dan database untuk menyimpan informasi tempat parkir dan data pengguna.

Terlepas dari manfaat yang diperoleh oleh sistem parkir pintar, ada juga beberapa tantangan keamanan yang harus dihadapinya. Sebagian besar sistem parkir pintar memiliki sistem terpusat, di mana jenis sistem tersebut umumnya rentan dan terutama sistem terpusat berisiko mengalami kegagalan satu titik yang dapat memengaruhi keseluruhan sistem.

Untuk mengatasi risiko kegagalan titik tunggal yang dapat mempengaruhi seluruh sistem sistem terpusat, mekanisme paling populer yang diusulkan peneliti adalah blockchain. Pasalnya, teknologi blockchain dikenal sebagai model terdesentralisasi yang juga memberikan jaminan integritas data. Pada tahun 2020 Waheed A. mengusulkan penggunaan kerangka biometrik dan blockchain pada sistem parkir pintar.

Metode sebelumnya hanya menjelaskan penggunaan blockchain dalam sistem parkir pintar, mekanisme untuk memverifikasi keaslian setiap transaksi tidak dibahas. Dalam tulisan ini, mekanisme blockchain digabungkan dengan tanda tangan digital berbasis RLWE untuk memverifikasi keaslian setiap transaksi. Ring Learning With Errors pertama kali diusulkan oleh Lyubashevsky et al. Skema kriptografi berbasis kisi adalah keluarga yang paling menjanjikan dalam skema tahan kuantum karena keserbagunaan dan kinerjanya yang unggul. Hyeongcheol dkk. menyatakan bahwa tanda tangan digital berbasis RLWE memiliki ukuran tanda tangan yang lebih kecil dan kompleksitas waktu yang paling kecil dibandingkan dengan kriptografi tahan kuantum lainnya.

Topik dan Batasannya

Berdasarkan latar belakang yang ada, rumusan masalah yang dapat dari metode sebelumnya yaitu penggunaan sistem terpusat yang rentan terhadap kegagalan titik tunggal yang dapat memengaruhi keseluruhan sistem. Batasan dari penelitian ini adalah penggunaan RLWE hanya dalam bentuk tanda tangan digital.

Tujuan

Tujuan dari penelitian ini adalah untuk memperkuat keamanan dari sistem parkir cerdas dengan menggunakan blockchain dan tanda tangan digital berbasis RLWE. Pemilihan RLWE didasari dengan kelebihan dari skema tersebut dimana skema RLWE dapat bertahan melawan penyerangan komputer kuantum.