Kemacetan merupakan hal umum yang dijumpai didalam kota kota besar, kemacetan ini memberikan dampak yang sangat besar baik di dalam segi perekonomian maupun dalam segi lingkungan [1]. Managemen lalu lintas merupakan solusi yang harus dilakukan. Hal yang umum digunakan sebagai pengatur lalu lintas adalah lampu lalu lintas, yang biasa digunakan di persimpangan jalan. Selain itu penempatan petugas pada titik titik rawan kemacetan merupakan hal umum yang digunakan untuk mengatasi kemacetan lalu lintas, namun hal ini juga merupakan tidakan yang tidak efektif dari sisi tenaga maupun sumber daya manusia yang terlibat didalam melakukan pengaturan secara manual [2]. Penerapan Teknologi IoT (Internet of Thing) pada lampu lalu lintas (traffic light) dapat membantu mengurai kemacetan lalu lintas [4]. Namun terdapat beberapa permasalahan yaitu bagaimana cara memenejemen lalu lintasnya dan bagaimana mengamankan lampu lalu lintas (traffic light) tersebut dari peretasan.

Untuk manajemen lalu lintasnya dapat menggabungkan teknologi IOT dengan RFID yang merupakan teknologi yang kompetitif dan mampu memberikan solusi tentang permasalahan tersebut [1] dimana dengan teknologi ini memungkinkan dapat memperoleh data tentang kecepatan rata- rata pada suatu titik kemacetan, waktu lama kemacetan, serta memperoleh data banyak mobil maupun motor yang terjebak didalam kemacetan. Selain itu metode ini memungkinkan dapat mengidentifikasi kendaraan kendaraan khusus seperti ambulan dan kendaraan militer, sehingga metode ini dapat memperioritaskan kendaraan tersebut [3]. Pengolahan data dapat dilakukan dengan beberapa metode yang ada2dan dikomunikasikan dengan IOT. Dengan pengolahan data yang terpusat, diperoleh hasil untuk melakukan optimasi waktu dan jalur lampu lalu lintas yang akan dilakukan perubahan. Dengan hal ini lampu lalu lintas akan memiliki kontrol terpusat dan terintegrasi dengan lampu lalu lintas yang berada di area tersebut [3].

* Algoritma antrian dinamis lampu lalu lintas menggunakan RFID

Metode ini memiliki topologi wireless yang dikomunikasikan dengan pengolah data pusat. Input data diperoleh dari sensor RFID yang ditempatkan pada titik-titik tertentu. Seluruh lampu lalu lintas terintegrasi dengan sistem tersebut sehingga memungkinkan diperoleh data secara realtime dan akurat. Prinsip utama dari metode ini adalah hasil input akan diolah pada pusat sistem. Dynamic Traffic Sequence Algorithm digunakan sebagai prinsip utama metode ini. Algoritma ini dapat melakukan control perubahan waktu antrian lampu lalu lintas [2]. Data yang digunakan diperoleh dari sensor RFID.Gambar 2 merupakan sensor RFID yang terpasang pada titik lampu lalu lintas. Sensor yang ditempatkan pada lalu lintas memiliki beberapa titik yang berfungsi sebagai data perhitungan.

* Kontrol lampu lalu lintas dengan RFID dan Neural Network

Metode ini menggunakan RFID sebagai alat input dalam melakukan automasi lampu lalu lintas, didalam metode ini ditambahkan neural network sebagai metode kalkulasi dan pengolahan data hasil input. Terdapat dua database dimana database knowledge base sebagai data hasil yang sudah diolah dari database input. Metode ini memungkinkan menyimpan data dari RFID yang sudah dibaca sebelumnya. Sehingga untuk permasalahan khusus metode ini dapat memberikan prioritas pada angkutan tertentu seperti angkutan militer maupun ambulan [3].

Untuk proteksi dari peretasan dapat menggunakan dua metode untuk melindungi data yang dikirimkan dari perangkat IoT ke jaringan komunikasi publik.

* Metode proteksi berbasis pada penggunaan algoritma enkripsi hybrid

Algoritma ini (misalnya, RSA-512 dan AES-128) memerlukan kemampuan komputasi yang relatif besar, metode ini melibatkan langkah-langkah berikut [5]:

Langkah 1. Pembuatan kunci public dan private pada server untuk organisasi enkripsi asimetris (misalnya RSA).

Langkah 2. Pembuatan kunci public dan private untuk mikrokontroller dan menyimpannya ke memori perangkat IoT.

Langkah 3. Kunci public ditukarkan antara server dan perangkat IoT.

Langkah 4. Perangkat IoT dengan sekumpulan karakter acak membuat kunci untuk enkripsi simetris (misalnya DES).

Langkah 5. Kunci enkripsi simetris yang telah dibuat di enkripsi dengan kunci public dan dikirim ke server.

Langkah 6. Decoding dijalankan pada server dan kunci simetris disimpan di ROM dengan menggunakan kunci private.

Langkah 7. Semua data berikutnya yang dikirim dari perangkat IoT dienkripsi menggunakan kunci simetris yang tersedia di server.

Langkah 6. Langkah 4-7 harus di ulang selama waktu yang telah di tetapkan tergantung pada kompleksitasnya.

* Metode proteksi berdasarkan penciptaan pola unik (unique pattern) untuk lalu lintas jaringan internet perangkat IoT.

Metode ini membuat perubahan acak dalam stuktur pertukaran informasi antara prangkat IoT dan server cloud, metode ini melibatkan langkah-langkah berikut [5]:

Langkah 1. Melakukan hashing pada semua data yang tersimpan dalam field data dari semua paket yang dikirim ke prangkat IoT.

Langkah 2. Menambahkan random delay sebelum siklus pengiriman data selanjutnya.

Langkah 3. Menggunakan server-side multiple IP addresses untuk menerima data.

Langkah 4. Menggunakan metode "port knocking" sebelum setiap data di transmisikan.

Langkah 5. Membuat data stream palsu.

Daftar Pustaka

[1] N. Choosri, Y. Park, S. Grudpan, P. Chuarjedton, and A. Ongvisesphaiboon, ―IoT-RFID Testbed for Supporting Traffic Light Control,‖ International Journal of Information and Electronics Engineering, Vol. 5, No. 2, March 2015

[2] K. A. Al-Khateeb, J. A. Johari, and W. F. Al-Khateeb, "Dynamic traffic light sequence algorithm using RFID," Journal of Komputer Science,vol. 4, no. 7, 2008.

[3] W. Wen, "An intelligent traffic management expert sistem with RFID technology," Expert Sistems with Applications, vol. 37, no. 4, pp.3024-3035, 2010.

[4] Shubham N. Mahalank, Keertikumar B. Malagund, R. M. Banakar, “IoT Based Dynamic Road Traffic Management for Smart Cities” 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies, Islamabad, 2015.

[5] Ruslan Kirichek, Vyacheslav Kulik, Andrey Koucheryavy, “False Clouds for Internet of Things and Methods of Protection” 18th International Conference on Advanced Communication TechnologyRussia, 2016.