BAB I

PEDAHULUAN

1.1 LATAR BELAKANG

Teknologi perangkat medis kini terhubung melalui jaringan yang dikenal dengan *Internet of Medical Things* (IoMT), mempercepat kemajuan era digital, khususnya di sektor kesehatan. IoMT merupakan salah satu aplikasi *Internet of Things* (IoT) . Sistem IoMT harus mengintegrasikan keselamatan dan keamanan perangkat medis [1]. elain itu, proses kesehatan seperti penanganan pasien, pemantauan, pemberian diagnosis, dan pemberian alat bantu ketika melakukan terapi pada pasien menggunakan IoMT dalam penanganannya [2]. Kemudian, IoMT juga digunakan pada saat krisis waktu untuk menghubungan antara penyedia layanan kesehatan dan pasien dalam peningkatan perawatan pasien yang membutuhkan diagnosis secara *real-time* [3]. Contoh teknologi IoMT adalah konsultasi dan pengobatan jarak jauh, *smart beds*, *Smart diagnostic tools*, *smart patient monitoring tools*, *smart pill bottles*, dan lain sebagainya [4]. Salah satu protokol komunikasi yang paling banyak digunakan di lingkungan IoMT adalah (MQTT), sebuah protokol yang dirancang untuk mengirimkan pesan dalam jaringan.

Protokol *Message Queue Telemetry Transport* (MQTT) yang sesuai dengan penerapan konsep IoMT, dan sering digunakan dalam berbagai sistem salah satunya pada sistem *monitoring* atau pemantauan [5], MQTT menggunakan prosedur pembentukan koneksi berdasarkan protokol TCP. Sebuah perangkat memulai

request message yaitu *connect* untuk membuat koneksi dengan broker. Banyak aplikasi yang menggunakan protokol MQTT, termasuk pemantauan perawatan kesehatan, karena sifatnya yang ringan dan kemampuannya untuk mengelola ribuan klien jarak jauh dengan satu server. Namun, protokol MQTT menunjukkan sebuah kerentanan yakni sifatnya yang terbuka. Kerentanan ini dapat dieksploitasi untuk meluncurkan berbagai jenis serangan, termasuk serangan DoS dan DDoS [6] akan tetapi sebagai salah satu protokol yang ringan MQTT diakui sebagai standar komunikasi pada IoT secara nyata dan mampu merealisasikan transmisi beberapa literatur mengatakan bahwa protokol MQTT menyediakan performa yang baik dan serbaguna [7]. Namun, MQTT tidak memiliki fitur enkripsi yang kuat secara *default*, pihak yang tidak berwenang dapat dengan mudah menyadap data yang dikirimkan. Selain itu, mekanisme autentikasi yang sederhana membuatnya rentan terhadap serangan.

Oleh karena itu untuk menghadapi serangan-serangan yang terjadi dibutuhkan sebuah penerapan *Intrusion Detection System* (IDS) adalah perangkat yang mendeteksi adanya intrusi dalam jaringan komputer, apabila terjadi masalah pada jaringan komputer IDS akan memberitahu *administrator* bahwasanya terdapat masalah dengan jaringan computer tersebut [8]. Dalam konteks ini, IDS turut memberikan informasi jenis-jenis serangan yang terjadi pada jaringan komputer [9]. Sebelumnya terdapat peneliti yang membahasan tentang IDS pada jaringan IoT untuk melindungi dari serangan, di protokol MQTT, karena dapat menjamin reproduktifitas peneliti untuk melatih model DL yang tertanam dalam IDS, yang menggunakan kumpulan data publik MQTT-IoT-IDS2020 di mana perangkat IoT

menggunakan protokol MQTT evaluasi kinerja IDS dengan akurasi 97,09% dan *F1-score* yang setara dengan 98,33% saat mendeteksi serangan MQTT [10]. Maka dari itu IDS merupakan salah satu teknik yang paling produktif untuk mendeteksi serangan dalam suatu jaringan [11].

Namun juga terdapat beberapa peneliti sebelumnya yang telah melakukan upaya penelitian terhadap deteksi serangan protokol MQTT antara lain seperti Ali Al-Zahrani dan Theyazn HH Aldhyani yang telah meneliti di lingkungan IoT. Dalam penelitian ini, dataset MQTT standar digunakan untuk mengembangkan akurasi sebesar 80,82%. pada penelitian ini KNN menunjukkan kinerja yang baik dalam mendeteksi sistem serangan siber. KNN mencapai Model ML dan DL terbukti sangat efisien, Rata-rata persentase dihitung metrik model KNN adalah 86%, 81%. dapat menjalankan sistem yang diusulkan ditampilkan dalam 82% [12]. selain itu juga ada Galuh Muhammad iman akbar telah melakukan penelitian mengenai deteksi serangan di protokol MQTT IoT dengan metode *Random Forest* peneliti melakukan uji coba pada data primer dan hasil yang diperoleh yaitu akurasi 99,55%, presisi 100%, *recall* 99,54% dan *f-measure* 99,77% Sedangkan untuk data sekunder peneliti memperoleh akurasi 99.77, *recall* 99.43%, *f-measure* 98.71% [13]. Dan yang terakhir penelitian yang dilakukan oleh Mabda Amnesti Hananto, Ari Kusyanti, Rakhmadhany Primananda yang melakukan implementasi terhadap Pengamanan Data pada Protokol MQTT menggunakan Perangkat WemosESP8266 dengan pengujian *test vector*, kinerja enkripsi dan dekripsi menghasilkan rata-rata 12,6 *millisecond* dan dekripsi adalah 61,2 *millisecond* [14]. Dari beberapa

penelitian yang ada telah mendapatkan hasil yang baik tetapi juga membutuh suatu peningkatan dengan memilih algoritma yang tepat.

Meskipun penelitian sebelumnya telah melakukan upaya dalam mendeteksi serangan pada protokol MQTT dan menunjukkan hasil yang signifikan, masih terdapat masalah dalam hal optimalisasi dan efisiensi. Pada penelitian sebelumnya mereka menggunakan beberapa algoritma seperti KNN dan *Random Forest* yang menghasilkan akurasi yang baik, namun belum mampu sepenuhnya menangani pola serangan yang kompleks. Selain itu, penelitian yang dilakukan oleh Mabda Amnesti Hananto dan tim berfokus pada pengamanan data melalui enkripsi protokol MQTT, akan tetapi belum mencakup implementasi *deep learning* dalam deteksi serangan. Oleh karena itu, diperlukan pendekatan baru dengan menggunakan algoritma *deep learning* dan dapat menjadi pilihan yang *real-time*, algoritma RNN menjadi salah satu pilihan pada penelitian ini untuk melakukan pendekatan dalam mengatasi tantangan dalam mendeteksi serangan terhadap protokol MQTT

Berdasarkan hal tersebut, algoritma *Recurrent Neural Network* (RNN) dapat menjadi algoritma yang efektif untuk mendeteksi pola serangan, terutama berlaku untuk serangan yang menggunakan data berurutan dalam waktu. Metode- metode yang digunakan RNN untuk dapat menghasilkan informasi dari masa lalu adalah looping dalam arsitekturnya, yang secara otomatis membuat informasi dari masa lalu tetap tersimpan. Salah satu bagian dari RNN adalah LSTM. LSTM merupakan sistem pengumpulan data yang dapat menganalisis, mengkategorikan, dan menafsirkan data yang dikumpulkan sebelumnya**,** [15] algoritma RNN bisa menjadi

salah satu Solusi model algoritma yang menjanjikan. Pada akhirnya, mekanisme kerja RNN mengalami penyempurnaan melalui berbagai bentuk modifikasi, salah satunya adalah LSTM Namun, sejak era 1980-an, RNN telah diakui sebagai algoritma yang sangat efektif, terutama karena kemampuannya yang didukung oleh memori internalnya. [16]. Dengan menggunakan RNN yang merupakan salah satu algoritma *deep learning,* maka akan dilakukan implementasi untuk memprediksi deteksi di lingkungan IoMT karena RNN termasuk algoritma yang menggunakan perhitungan probabilitas [17].

Untuk mendukung performa algoritma RNN, dataset yang digunakan pada penelitian ini di ambil dari *Canadian Institute for Cybersecurity* (CIC) pada universitas *new Brunswick* (UNB), Kanada CIC IoMT *Dataset* 2024 yaitu kumpulan data yang dikembangkan untuk mendukung sistem deteksi di lingkungan (IoMT), yang berfokus pada deteksi serangan jaringan seperti *Distributed Denial of Service* (DDoS) yang sering mengancam keamanan sistem IoMT. *Dataset* ini berjumlah sebanyak 234.648 baris dan terdapat 46 atribut yang relevan dalam mendeteksi pola anomali. *Dataset* berisi ribuan entri direkam dalam bentuk lalu lintas paket komunikasi jaringan yang menunjukan aktivitas normal dan aktivitas berbahaya yang disimulasikan. Dataset ini dapat membantu dalam pengujian algoritma RNN untuk deteksi ancaman di lingkungan IoMT, sehingga dapat meningkatkan keamanan pada jaringan perangkat medis yang terhubung.

Dari uraian yang ada di atas, penulis melakukan penelitian yang berfokus untuk mengimplementasikan model *Recurrent Neural Network* (RNN) untuk mendeteksi pola serangan, Dengan judul penelitian **“IMPLEMENTASI**

ALGORITMA (RNN) UNTUK DETEKSI SERANGAN PADA PROTOKOL MQTT DI LINGKUNGAN *INTERNET OF MEDICAL THINGS* (IOMT)"

1.2 RUMUSAN MASALAH

Penelitian sebelumnya telah menggunakan Metode *Support Vector Machine* (SVM) dalam mendeteksi serangan pada protokol MQTT di IoT/IoMT menunjukkan keakuratan yang baik dalam mendeteksi serangan tertentu. Akan tetapi seperti diungkapkan oleh Raza dan Huang (2022), SVM menjadi kurang efisien ketika diimplementasikan pada perangkat IoT dengan sumber daya komputasi yang terbatas dan membuatnya kurang sesuai untuk digunakan secara *real-time* [18] . Selain itu, metode berbasis klasifikasi ini masih dinilai kurang efektif dalam mengelola data yang besar, sehingga dibutuhkan model yang lebih canggih untuk mendeteksi ancaman secara *real-time* dan lebih optimal.

Berdasarkan uraian yang telah di dipaparkan di atas, maka terdapat beberapa pertanyaan penelitian dalam penelitian ini yaitu :

1. Bagaimana mengimplementasi algoritma *recurrent neural network (RNN),* dapat membantu mendeteksi pola serangan pada protokol MQTT pada lingkungan IoMT yang memiliki data besar?
2. Bagaimana performa algoritma RNN dalam mendeteksi pola serangan secara *real-time* pada protokol MQTT?

1.3 BATASAN MASALAH

Agar penelitian ini lebih terarah, penelitian ini menetapkan batasan-batasan masalah yang mencakup :

1. Penelitian berfokus pada mengidentifikasi serangan pada protokol MQTT di lingkungan IoMT.
2. Penelitian ini menggunakan dataset yang di ambil dari Canadian *Institute for Cybersecurity* (CIC) IoMT dataset 2024, Dataset tersebut berisikan data serangan siber pada protokol MQTT di lingkungan IoMT dengan jumlah data sebanyak 234.648 baris data dan 46 atribut.
3. Pengukuran kinerja performa RNN untuk menentukan nilai akurasi, presisi, TPR, *F1-score*, *Recall*, dan ROC
4. Penelitian ini menggunakan *google colab* sebagai alat bantu untuk mengukur performa dalam mendeteksi pola serangan MQTT.

1.4 TUJUAN PENELITIAN

Berdasarkan latar belakang di atas penelitian ini memiliki tujuan antara lain yaitu :

1. Mendeteksi pola serangan pada protokol MQTT di lingkungan *internet of meducal things* (IOMT) dengan mengimplementasikan algoritma RNN.
2. Mengevaluasi kinerja RNN dalam mendeteksi pola serangan protokol MQTT berdasarkan nilai akurasi, TPR, *F1-score*, *Recall*, dan ROC.
3. Mengetahui hasil akhir performa algoritma RNN dalam deteksi pola serangan MQTT di lingkungan IoMT.

1.5 MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah :

1. Dapat meningkatkan keamanan data pada lingkungan IoMT terutama terkait dengan komunikasi data protokol MQTT.
2. Memberikan gambaran keseluruhan mengenai efektivitas nya model RNN dalam deteksi serangan pada protokol MQTT di IoMT
3. Hasil dari penelitian ini dapat menjadi Referensi untuk Penelitian Selanjutnya dalam penerapan algoritma RNN pada protokol MQTT di lingkungan IoMT.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan ini menggambarkan tentang pembahasan untuk mempermudah dalam memahami penulisan laporan penelitian ini,maka penulis menyajikan sistematika penulisan-penulisan sebagai berikut:

BAB I : PENDAHULUAN

Dalam bab I pendahuluan ini berisis tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penulisan dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini penulis membahas beberapa definisi dari beberapa teori-teori yang berhubungan dengan masalah yang diteliti bersumber dari buku dan jurnal-jurnal, untuk mendukung pemahaman terhadap penulis. Dan digunakan

sebagai landasan untuk menjawab masalah penelitian serta membantu penulis supaya memiliki landasan teori yang baik mengenai penelitian yang dilakukan.

BAB III : METODOLOGI PENELITIAN

Bab ini menjelaskan metodologi penelitian, yang mencakup beberapa hal penting. Penulis memberikan rincian tentang teknik yang digunakan untuk mengumpulkan informasi yang relevan. Penulis juga membahas metode analisis data, yang menjelaskan bagaimana data yang dikumpulkan diolah dan dianalisis. Untuk memberikan pemahaman yang lengkap tentang metodologi yang digunakan dalam penelitian ini, setiap kerangka kerja ini saling berhubungan.

BAB IV : ANALISIS DAN HASIL

Dalam bab ini penulis memaparkan analisis performa RNN dalam mdeteksi serangan dan data yang diperoleh selama penelitian dan hasil dari analisis tersebut. Bab ini juga mencakup interpretasi hasil serta diskusi mengenai temuan penelitian.

BAB V : PENUTUP

Dalam bab ini penulis memberikan kesimpulan dari hasil penelitian dan menyampaikan saran-saran yang relevan untuk penelitian lebih lanjut tentang penerapan deteksi serangan pada protocol MQTT di lingkungan IoMT atau penerapan praktis dari temuan penilitian.

Dengan sistematika penulisan ini, diharapkan pembaca dapat dengan mudah mengikuti alur penelitian dan memahami setiap bagian dari laporan penelitian yang disusun.