BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Internet of Medical Things (IoMT) adalah jaringan perangkat medis yang terhsubung ke internet yang terdiri dari infrastruktur, perangkat keras, dan aplikasi perangkat lunak yang digunakan dalam teknologi informasi kesehatan. *IoMT* memungkinkan perangkat medis, pasien, dan penyedia layanan kesehatan berkomunikasi nirkabel dan jarak jauh. Ini memudahkan pengumpulan dan analisis data medis secara real-time[1]. Keamanan siber di bidang *Internet of Medical Things (IoMT)* kini menjadi perhatian utama di tingkat global, seiring dengan makin meluasnya penggunaan perangkat medis terhubung internet di berbagai negara, hal ini disebabkan oleh peningkatan penggunaan perangkat medis yang terhubung ke internet di berbagai negara. Untuk mengatasi masalah ini, standar keamanan yang ketat telah dibuat, sistem enkripsi data yang kuat, dan kerangka regulasi telah diperkuat[2]. Namun demikian, solusi-solusi tersebut masih menghadapi sejumlah tantangan yang menghalangi implementasinya. Yang paling menonjol adalah masalah pembiayaan dan kompleksitas teknis pada tingkat sistemik[3].

Terlepas dari berbagai upaya peningkatan keamanan *IoMT*, perangkat-perangkat ini tetap menjadi sasaran empuk bagi para peretas[4]. Studi terkini mengungkapkan bahwa insiden seperti serangan *DDoS*, infeksi malware, dan manipulasi data semakin marak terjadi pada perangkat *IoMT*.[5] Hal ini berpotensi membahayakan keselamatan pasien dan mengganggu operasional fasilitas kesehatan. Lemahnya sistem keamanan pada perangkat-perangkat tersebut

mengakibatkan kurangnya kemampuan deteksi dini terhadap serangan, sehingga mengancam keberlanjutan layanan yang sangat bergantung pada *IoMT*[6]. Oleh karena itu, pengembangan sistem deteksi serangan yang handal dan efektif menjadi kebutuhan mendesak untuk menjamin keamanan operasional perangkat *IoMT*.

A. Reji, B. Pranggono, J. Marchang, and A. Shenfield telah menerapkan teknik *Machine Learning (ML) seperti Decision Tree, Support Vector Machine (SVM),* dan *Random Forest* dalam upaya mendeteksi serangan pada *IoMT* dengan rata-rata akurasi setinggi 99,99% [7]. Selain itu, penelitian yang dilakukan H. Tauqeer, M. M. Iqbal, A. Ali, S. Zaman, and M. U. Chaudhry menggunakan teknik *Machine Learning (ML)* dengan algoritma *Random Forest, Support Vector Machine (SVM),* dan *Gradient Boosting* dengan akurasi tertinggi menggunakan metode *Random Forest* yakni sebesar 96,9% [8] Kemudian pada penelitian yang di lakukan oleh E. A. Winanto, K. Kurniabudi, S. Sharipuddin, I. S. Wijaya, and D. Sandra dengan menerapkan teknik *Deep Learning(DL)* untuk penelitiannya pada deteksi serangan jaringan kompleks *IoT* dengan akurasi mencapai 87,55%[9] Seiring kemajuan teknologi, *Convolutional Neural Network (CNN)* mulai dimanfaatkan untuk mengidentifikasi anomali jaringan, namun aplikasinya dalam lingkup *IoMT* belum dieksplorasi secara komprehensif. Dengan demikian, pendekatan yang lebih canggih, seperti integrasi *CNN* dengan metode geometri, diyakini berpotensi meningkatkan presisi dalam mendeteksi serangan.

Mayoritas studi terdahulu cenderung mengandalkan metode tunggal seperti *CNN* atau pendekatan geometri dasar, tanpa mengintegrasikan keduanya[10].

Relevansi penelitian ini semakin krusial mengingat eskalasi frekuensi serangan dan konsekuensinya terhadap layanan kesehatan berbasis digital.

Tujuan utama dari penelitian ini adalah untuk menerapkan metode inovatif dalam mendeteksi serangan pada sistem IoMT dengan menggabungkan teknologi Convolutional Neural Network (CNN) dan pemilihan fitur SelectKBest yang berbasis ANOVA F-score. SelectKBest digunakan untuk memilih fitur jaringan yang paling signifikan, sementara CNN berfungsi dalam mendeteksi serangan secara langsung.

Peneliti memilih dua tipe serangan yang akan di deteksi yakni *Reconnaissance* dan *Distributed Denial of Service(DDoS)* dikarenakan Kombinasi antara *DDoS* dan Recon menunjukkan bahwa penyerang sering menggunakan teknik *Reconnaissance* untuk mempersiapkan serangan *DDoS*, sehingga pemahaman mendalam tentang kedua jenis serangan ini sangat penting untuk deteksi yang efektif. Selain itu, ketersediaan data dan sumber daya penelitian yang melimpah mengenai serangan *DDoS* dan *Reconnaissance* memudahkan peneliti dalam melakukan analisis dan pengembangan metode deteksi yang inovatif.

Penelitian ini memanfaatkan dataset *IoMT* 2024 yang disediakan oleh *Canadian Institute for Cybersecurity (CIC).* Dataset ini berisi data terkait berbagai jenis serangan yang terjadi dalam lingkungan *IoMT*. dataset yang digunakan mencakup total 353,532 baris dengan 45 atribut. Berikut link dari dataset nya http://205.174.165.80/IOTDataset/CIC*IoMT*2024/Dataset/WiFI_and_MQTT/attacks/CSV/

Dari latar belakang tersebut, peneliti menyusun tugas akhir dengan judul **"Deteksi Serangan Pada *Internet Of Medical Things (IoMT)* Menggunakan Metode *Convolutional Neural Network (CNN)* Dan Seleksi Fitur *SelectKBest*"**

1.2 RUMUSAN MASALAH

Dengan melihat latar belakang yang telah diuraikan sebelumnya, keamanan perangkat *IoMT (Internet of Medical Things)* masih mengalami berbagai hambatan dalam mengidentifikasi serangan siber, seperti *DDoS* dan *Reconnaissance*, yang dapat membahayakan pasien dan mengganggu layanan kesehatan. Studi ini bertujuan untuk memperbaiki deteksi serangan pada sistem *IoMT* melalui penerapan *Convolutional Neural Network (CNN)*. Agar kinerja model dapat ditingkatkan, diterapkan seleksi fitur *SelectKBest* yang berdasar pada *ANOVA F-score* pada tahap pemilihan fitur untuk mengidentifikasi atribut yang paling relevan dalam dataset. Metode ini diharapkan mampu meningkatkan keamanan sistem *IoMT* dalam mendeteksi dan menanggulangi ancaman siber dengan lebih efisien.

Dengan latar belakang yang telah dijelaskan di atas, maka diketahui bahwa masalah dari penelitian ini yaitu:

1. Bagaimana penerapan *SelectKBest* berbasis *ANOVA F-score* dan *Convolutional Neural Network* dalam mendeteksi serangan pada *IoMT*?
2. Bagaimana kemampuan metode *CNN* dalam membedakan jenis serangan siber pada perangkat *IoMT* dengan bantuan *SelectKBest* berbasis *ANOVA F-score* dalam proses pemilihan fitur dari lalu lintas jaringan?

1.3 BATASAN MASALAH

Supaya pembahasan lebih terencana dan konsisten dengan tujuan, maka diperlukan pembatasan masalah pada suatu bahasan. Oleh karena itu batasan-batasan yang ditetapkan oleh peneliti dalam penelitian ini adalah:

1. Penelitian ini akan membatasi metode deteksi serangan dengan *Convolutional Neural Network (CNN).*
2. Dalam penelitian ini, pemanfaatan *SelectKBest* yang berlandaskan *ANOVA F-score* diterapkan untuk memilih fitur jaringan yang paling signifikan, sehingga dapat meningkatkan efektivitas pemrosesan data dan ketepatan dalam mendeteksi serangan pada *IoMT*.
3. Dataset ini berfokus pada protokol yang umum digunakan dalam perangkat *IoMT*, yakni *Wi-Fi*, dan *MQTT*
4. Dalam penelitian ini mencakup pengukuran kinerja model dengan menggunakan metrik-metrik seperti akurasi, *True Positive Rate/ TPR, F1-Score, recall*, serta analisis kurva *ROC*
5. Serangan yang dianalisis dibatasi oleh dua jenis serangan saja yakni *DDoS (Distributed Denial of Service)* dan *Reconnaissance*
6. Penelitian ini memanfaatkan dataset *IoMT* 2024 yang disediakan oleh *Canadian Institute for Cybersecurity (CIC)*. Dataset ini berisi data terkait berbagai jenis serangan yang terjadi dalam lingkungan *IoMT*. dataset ini mencakup total 44,455 baris dengan 45 atribut. Berikut link dari data setnya http://205.174.165.80/IOTDataset/CIC*IoMT*2024/Dataset/WiFI_and_MQTT/attacks/CSV/

1.4 TUJUAN PENELITIAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Berdasarkan pada masalah yang sudah dikemukakan, maka penelitian ini memiliki tujuan:

1. Mengembangkan dan mengimplementasikan metode deteksi serangan siber pada jaringan *Internet of Medical Things (IoMT)* dengan memanfaatkan *Convolutional Neural Network (CNN)* serta seleksi fitur menggunakan *SelectKBest* berbasis *ANOVA F-score*.
2. Memvalidasi model deteksi serangan yang dikembangkan menggunakan dataset *CICIoMT2024* serta menganalisis performanya dalam mendeteksi serangan berdasarkan parameter akurasi, presisi, *recall*, dan *F1-score*.

1.4.2 Manfaat Penelitian

Manfaat yang akan didapatkan dari penelitian ini, yaitu:

1. Memberikan kontribusi dalam meningkatkan sistem keamanan pada perangkat IoMT dengan menerapkan pendekatan berbasis Convolutional Neural Network (CNN) dan SelectKBest berbasis ANOVA F-score untuk memilih fitur jaringan yang paling relevan.
2. Penelitian ini dapat membantu melindungi data pasien serta sistem operasional fasilitas kesehatan dari potensi ancaman siber, seperti serangan DDoS dan Reconnaissance.

1.5 SISTEMATIKA PENULISAN

Sistematika ini menggambarkan tentang pembahasan yang penulis buat pada proyek penelitian untuk memudahkan dalam memahami penulisan laporan ini. Adapun sistematika penulisan dalam penelitian ini disusun sebagai berikut:

BAB I : PENDAHULUAN

Dalam bab pendahuluan peneliti membahas tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian serta sistematika penulisan.

BAB II : LANDASAN TEORI

Dalam bab ini peneliti menguraikan teori-teori yang menjadi dasar dalam penelitian ini. Adapun teori-teori ini bersumber dari buku dan jurnal-jurnal untuk mendukung pemahaman.

BAB III : METODOLOGI PENELITIAN

Dalam bab ini peneliti menjelaskan metodologi yang digunakan dalam penelitian, termasuk desain penelitian, teknik pengumpulan data, dan metode analisis data.

BAB IV : ANALISIS DAN HASIL

Dalam bab ini peneliti memaparkan analisis 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 peneliti memberikan kesimpulan dari hasil penelitian dan menyampaikan saran-saran yang relevan untuk penelitian lebih lanjut atau penerapan praktis dari temuan penelitian.

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