BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan teknologi informasi dan komunikasi (TIK) telah membawa dampak signifikan dalam peradaban manusia. Salah satu tonggak penting dalam evolusi ini adalah perkembangan jaringan komunikasi seluler generasi kelima, atau lebih dikenal dengan sebutan 5G. Jaringan 5G menghadirkan kecepatan dan keterhubungan yang belum pernah terjadi sebelumnya, membuka peluang tak terbatas dalam berbagai bidang, seperti *Internet of Things (IoT), augmented reality, virtual reality*, dan mobilitas tingkat tinggi [1]. Meskipun jaringan 5G menjanjikan banyak manfaat, pertumbuhan teknologi ini juga membawa tantangan baru dalam aspek keamanan, khususnya dalam melawan serangan *malware*.

Serangan *malware* telah menjadi ancaman utama dalam dunia siber, dan dengan perkembangan jaringan 5G, keparahan serangan malware semakin meningkat. *Malware* adalah perangkat lunak berbahaya yang dirancang untuk merusak, mencuri informasi, atau merusak integritas sistem komputer atau jaringan [2]. Serangan malware terbaru semakin kompleks dan canggih, mengeksploitasi kerentanan dalam sistem yang terhubung ke jaringan 5G. Serangan semacam itu bisa mengakibatkan kerugian besar, baik dalam hal kehilangan data sensitif, kerusakan perangkat, maupun ancaman terhadap privasi individu dan bisnis.

Oleh karena itu, penting untuk mengembangkan solusi yang efektif untuk mendeteksi dan mengatasi serangan malware terbaru pada jaringan 5G. Salah satu pendekatan yang menjanjikan dalam hal ini adalah pemanfaatan kecerdasan buatan (*Artificial Intelligence - AI*) untuk deteksi dan mitigasi serangan *malware*. Kecerdasan buatan adalah bidang yang berkembang pesat dalam ilmu komputer yang berkaitan dengan pengembangan sistem komputer yang mampu berpikir dan belajar seperti manusia. Dalam konteks keamanan siber, kecerdasan buatan telah terbukti sangat efektif dalam mendeteksi dan mengatasi serangan malware dengan tingkat akurasi yang tinggi.

Meskipun sudah banyak penelitian yang menggunakan kecerdasan buatan untuk melawan serangan malware, jaringan 5G membawa tantangan khusus. Kecepatan dan kompleksitas jaringan ini membuat deteksi dan mitigasi serangan malware semakin rumit. Jaringan 5G juga menghadirkan tantangan dalam hal skalabilitas, karena jumlah perangkat yang terhubung ke jaringan ini sangat besar. Oleh karena itu, penelitian yang fokus pada analisis kecerdasan buatan untuk deteksi dan mitigasi serangan malware terbaru pada jaringan 5G sangat relevan dan penting.

Penelitian ini akan mengeksplorasi berbagai aspek yang berkaitan dengan penggunaan kecerdasan buatan dalam menghadapi ancaman malware pada jaringan 5G. Dalam konteks ini, kecerdasan buatan dapat digunakan untuk mendeteksi serangan malware dengan cepat dan akurat, mengklasifikasikan jenis malware, serta memberikan respons yang efektif untuk menghentikan serangan sebelum menyebabkan kerusakan yang signifikan. Selain itu, kecerdasan buatan juga dapat digunakan untuk mengidentifikasi kerentanan dalam jaringan 5G yang dapat dieksploitasi oleh malware [3].

Salah satu keunggulan besar dari penggunaan kecerdasan buatan adalah kemampuannya untuk belajar dari data historis dan mengidentifikasi pola serangan yang belum pernah terdeteksi sebelumnya. Dengan demikian, kecerdasan buatan dapat membantu organisasi dan penyedia layanan jaringan 5G untuk tetap selangkah di depan para penyerang yang terus berinovasi. Ini menjadi sangat penting mengingat serangan malware terbaru seringkali berubah dan berkembang dengan cepat.

Selain itu, penelitian ini juga akan membahas strategi mitigasi yang efektif untuk serangan malware pada jaringan 5G. Mitigasi serangan tidak hanya melibatkan deteksi, tetapi juga melibatkan upaya untuk mengisolasi dan memulihkan sistem yang terkena serangan. Penggunaan kecerdasan buatan dalam konteks ini dapat membantu dalam mengidentifikasi solusi yang paling efektif untuk mengurangi dampak serangan malware, mengembalikan integritas jaringan, dan menghindari kerugian yang lebih besar.

Penelitian ini juga akan membahas berbagai teknik kecerdasan buatan yang dapat digunakan, seperti pembelajaran mesin (*machine learning*), jaringan saraf tiruan (*artificial neural networks*), dan pemrosesan bahasa alami (natural language processing). Kombinasi berbagai teknik ini dapat memberikan solusi yang holistik dalam menghadapi serangan malware pada jaringan 5G.

Dalam konteks pengembangan teknologi keamanan siber, penelitian ini diharapkan dapat memberikan panduan dan kontribusi yang signifikan dalam upaya melindungi jaringan 5G dari serangan malware yang terus berkembang. Penelitian ini juga diharapkan dapat memberikan wawasan yang lebih dalam tentang tantangan dan peluang yang muncul dengan pertumbuhan jaringan 5G, serta bagaimana kecerdasan buatan dapat menjadi alat yang kuat dalam memitigasi risiko keamanan yang terkait.

Melalui penelitian ini, diharapkan dapat ditemukan solusi yang inovatif dan efektif untuk menghadapi serangan malware pada jaringan 5G. Keamanan jaringan 5G merupakan elemen kunci dalam mendukung perkembangan teknologi masa depan, dan penelitian ini akan berkontribusi pada pencapaian tujuan tersebut. Selanjutnya, dengan pemahaman yang lebih baik tentang cara mengatasi serangan malware pada jaringan 5G, organisasi dan penyedia layanan dapat memitigasi risiko keamanan dengan lebih baik, sehingga menghasilkan jaringan yang lebih aman dan andal dalam menghadapi ancaman masa depan.

1.2 Rumusan Masalah

Dari latar belakang seperti pada 1.1, berikut adalah beberapa rumusan masalah yang dapat dijadikan dasar untuk penelitian ini :

1. Bagaimana perkembangan jaringan komunikasi seluler generasi kelima (5G) mempengaruhi meningkatnya ancaman serangan malware pada infrastruktur jaringan 5G?
2. Bagaimana kontribusi kecerdasan buatan (AI) dalam mendeteksi, mengklasifikasikan, dan merespons serangan malware pada jaringan 5G dengan tingkat akurasi yang tinggi?

3. Apa tantangan utama yang dihadapi dalam mengimplementasikan kecerdasan buatan untuk deteksi dan mitigasi serangan malware pada jaringan 5G, termasuk dalam konteks kecepatan, kompleksitas, dan skalabilitas jaringan tersebut?
4. Bagaimana kombinasi teknik kecerdasan buatan seperti machine learning, artificial neural networks, dan natural language processing dapat digunakan secara efektif dalam melawan serangan malware pada jaringan 5G?
5. Bagaimana strategi mitigasi efektif dapat dikembangkan untuk mengurangi dampak serangan malware pada jaringan 5G, termasuk upaya dalam mengisolasi dan memulihkan sistem yang terkena serangan?
6. Bagaimana penelitian ini dapat memberikan panduan dan kontribusi yang signifikan dalam upaya melindungi jaringan 5G dari serangan malware yang terus berkembang, serta menyediakan wawasan tentang tantangan dan peluang yang muncul seiring pertumbuhan jaringan 5G?
7. Bagaimana inovasi solusi yang ditemukan dalam penelitian ini dapat membantu meningkatkan keamanan jaringan 5G, sehingga mendukung perkembangan teknologi masa depan dan mengurangi risiko keamanan yang terkait dengan ancaman serangan malware pada jaringan tersebut?

1.3 Batasan Masalah

Berikut batasan masalah yang dapat digunakan untuk penelitian penulis :

1. Penelitian ini akan membatasi fokus pada pengembangan dan evaluasi teknik kecerdasan buatan (AI) yang digunakan untuk deteksi dan mitigasi serangan malware pada jaringan 5G.
2. Analisis akan terbatas pada serangan malware terbaru yang relevan dengan konteks jaringan 5G, seperti serangan yang dapat merusak integritas sistem, mencuri informasi sensitif, atau merusak perangkat.

3. Penelitian ini akan mempertimbangkan variasi teknik kecerdasan buatan, termasuk machine learning, artificial neural networks, dan natural language processing, untuk menentukan pendekatan yang paling efektif.
4. Skripsi ini akan mengeksplorasi dampak kecepatan, kompleksitas, dan skalabilitas jaringan 5G terhadap efektivitas solusi kecerdasan buatan dalam mengatasi serangan malware.
5. Evaluasi kinerja solusi yang diajukan akan dilakukan menggunakan data simulasi dan data riil yang tersedia, untuk mengukur akurasi, kecepatan deteksi, dan efektivitas mitigasi.
6. Penelitian ini tidak akan mencakup implementasi teknis jaringan 5G, tetapi akan berfokus pada aspek perangkat lunak dan teknik kecerdasan buatan yang relevan dengan deteksi dan mitigasi malware.
7. Dalam konteks mitigasi, penelitian akan menilai efektivitas tindakan respons untuk mengisolasi dan memulihkan sistem yang terkena serangan, serta mempertimbangkan upaya dalam mencegah kerugian lebih lanjut.
8. Aspek keamanan data individu dan privasi juga akan dipertimbangkan dalam kerangka kerja kecerdasan buatan yang digunakan untuk melawan serangan malware.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menganalisis dampak perkembangan jaringan 5G terhadap meningkatnya serangan malware dan kerentanannya dalam konteks teknologi informasi dan komunikasi.
2. Untuk mengidentifikasi teknik dan pendekatan kecerdasan buatan yang dapat efektif digunakan dalam mendeteksi dan mengklasifikasikan serangan malware pada jaringan 5G dengan tingkat akurasi yang tinggi.

3. Untuk mengevaluasi efektivitas solusi kecerdasan buatan dalam merespons serangan malware pada jaringan 5G, termasuk dalam upaya mengisolasi dan memulihkan sistem yang terkena serangan.

4. Untuk mengidentifikasi dan menganalisis tantangan khusus yang terkait dengan penggunaan kecerdasan buatan dalam lingkungan jaringan 5G, termasuk kecepatan, kompleksitas, dan skalabilitas jaringan tersebut.

5. Untuk memberikan panduan dan wawasan yang lebih dalam tentang bagaimana kecerdasan buatan dapat digunakan sebagai alat yang kuat dalam melawan serangan malware pada jaringan 5G, serta cara mengatasi tantangan yang muncul seiring pertumbuhan jaringan tersebut.

6. Untuk menyumbangkan pemahaman yang lebih baik tentang bagaimana teknologi keamanan siber dapat berkembang untuk melindungi jaringan 5G dari serangan malware yang terus berkembang, dan bagaimana solusi inovatif dapat membantu meningkatkan keamanan jaringan tersebut.

Untuk menghasilkan rekomendasi dan temuan yang dapat digunakan oleh organisasi, penyedia layanan jaringan, dan peneliti dalam upaya

1.5 Manfaat Penelitian

Berikut manfaat penelitian yang ditulis oleh penulis:

1. Penelitian ini dapat membantu meningkatkan keamanan jaringan 5G dengan mengembangkan solusi yang efektif untuk mendeteksi dan mengatasi serangan malware terbaru. Ini akan membantu melindungi data sensitif, mencegah kerusakan perangkat, dan menjaga integritas jaringan.

2. Dengan menggunakan kecerdasan buatan untuk deteksi dan mitigasi malware, penelitian ini dapat membantu mengurangi ancaman

keamanan yang semakin berkembang dan canggih dalam lingkungan jaringan 5G.

3. Penelitian ini dapat mendorong pengembangan teknologi kecerdasan buatan dan aplikasinya dalam konteks keamanan siber. Ini akan membantu mengembangkan teknik yang lebih canggih dalam mendeteksi dan merespons serangan malware.
4. Dengan solusi yang efektif, jaringan 5G dapat mempertahankan integritas operasionalnya dan menghindari gangguan yang dapat merugikan penyedia layanan dan pengguna akhir.
5. Dengan deteksi yang lebih baik terhadap serangan malware, data sensitif yang dikirim melalui jaringan 5G dapat lebih terlindungi, membantu menjaga privasi individu dan bisnis.
6. Hasil penelitian ini dapat memberikan panduan dan rekomendasi kepada organisasi, penyedia layanan jaringan, dan peneliti tentang bagaimana mengatasi ancaman malware pada jaringan 5G dengan cara yang efektif.

1.6 Sistematika Penulisan

Penelitian ini meliputi beberapa bagian, yaitu:

BAB 1: Pendahuluan

Bagian bab pertama dari penelitian ini mencakup pendahuluan yang terdiri atas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB 2: Tinjauan Pustaka

Bagian bab kedua dari penelitian ini membahas tentang studi literatur yang terkait dengan penelitian penulis dan dasar teori yang berkaitan dengan penulisan seperti teori teori yang akan dibahas oleh penulis yang mendukung penulisan ini.

BAB 3: Metode Penelitian

Pada bab ini berisikan tentang objek penelitian yang diteliti oleh penulis, alur penelitian yang berisikan penjelasan atau langkah langkah terhadap objek yang diteliti, dan yang terakhir adalah alat dan bahan yang berisikan alat dan bahan apa saja yang akan mendukung pada objek yang diteliti

BAB 4: Hasil dan Pembahasan

Pada bagian ini berisikan hasil dari penelitian yang dilakukan oleh penulis berdasarkan alur penelitian yang ada pada bab 3.

BAB 5: Penutup

Merangkum semua hasil dari penelitian yang menjawab semua dari rumusan masalah yang sesuai dengan tujuan penelitian. Dan berisikan saran yang akan berguna untuk penelitian selanjutnya.