**Analisis Forensik Serangan Cyber dan Anomali pada Web Server UNUSIDA Menggunakan Deep Learning**

**Edi Dwi Prasetyo**

**23066020017**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Dalam beberapa tahun terakhir, pesatnya pertumbuhan internet telah menyebabkan peningkatan serangan syber yang menargetkan server web. Serangan - serangan ini dapat berdampak negatif pada fungsionalitas dan keamanan server web, yang menyebabkan pelanggaran data yang signifikan, gangguan layanan, dan kerugian finansial. Ketika ancaman dunia maya menjadi semakin canggih, teknik analisis forensik tradisional seringkali tidak cukup untuk mendeteksi dan memitigasi serangan ini secara tepat waktu.

Penelitian ini bertujuan untuk menyelidiki penerapan teknik pembelajaran mendalam dalam analisis forensik untuk meningkatkan deteksi dan mitigasi serangan cyber dan anomali server web Pembelajaran mendalam, bagian dari pembelajaran mesin, menggunakan jaringan saraf tiruan untuk menganalisis pola dan hubungan kompleks dalam kumpulan data besar. Dengan memanfaatkan kemampuan ini, algoritme pembelajaran mendalam dapat belajar dari data dalam jumlah besar dan mengidentifikasi potensi serangan siber dengan akurasi lebih tinggi. Tujuan utama penelitian ini adalah untuk mengeksplorasi dan menerapkan algoritma pembelajaran mendalam dalam konteks analisis forensik server web.

Dengan menganalisis log sistem, lalu lintas jaringan, dan sumber data terkait lainnya, kami bertujuan untuk mengembangkan kerangka kerja yang kuat yang mampu membedakan aktivitas pengguna yang sah dari tindakan jahat, sehingga memungkinkan deteksi dini serangan cyber. Selain itu, penelitian ini bertujuan untuk mengidentifikasi fitur dan indikator spesifik yang dapat membantu membedakan aktivitas anomali dari aktivitas standar, sehingga semakin meningkatkan akurasi deteksi.

Selain itu, penelitian ini bertujuan untuk mengatasi tantangan dan keterbatasan yang umumnya terkait dengan algoritma pembelajaran mendalam dalam analisis forensik. Salah satu tantangan utama adalah persyaratan kumpulan data pelatihan substansial yang terdiri dari kejadian normal dan serangan. Dalam penelitian ini, kami akan mengeksplorasi berbagai teknik pengumpulan, agregasi, dan pelabelan data untuk memastikan ketersediaan kumpulan data yang beragam dan representatif untuk pelatihan model.

Hasil penelitian ini akan berkontribusi pada pengembangan teknik analisis forensik yang canggih dan proaktif untuk server web, sehingga memungkinkan para profesional keamanan siber untuk merespons serangan siber dengan cepat. Dengan memanfaatkan kekuatan algoritma pembelajaran mendalam, organisasi dapat meningkatkan kemampuan pertahanan mereka dan meminimalkan potensi kerusakan yang disebabkan oleh ancaman dunia maya.

Secara keseluruhan, penelitian ini bertujuan untuk menjembatani kesenjangan antara teknik analisis forensik tradisional dan kebutuhan akan metode yang lebih maju untuk memerangi serangan cyber dan anomali di server web. Dengan memanfaatkan potensi pembelajaran mendalam, penelitian ini dapat meningkatkan keamanan server web secara signifikan dan melindungi data sensitif dari akses tidak sah dan penyalahgunaan.

1. **Rumusan Masalah**

Rumusan masalah dari penelitian "Analisis Forensik Serangan Cyber dan Anomali pada Web Server Menggunakan Deep Learning" dapat dirumuskan sebagai berikut:

1. Bagaimana melakukan analisis forensik terhadap serangan cyber pada web server?
2. Bagaimana mendeteksi dan mengidentifikasi serangan cyber yang terjadi pada web server menggunakan deep learning?
3. Apa saja jenis serangan cyber yang umum terjadi pada web server dan bagaimana cara mengenali anomali yang mungkin terjadi?
4. Bagaimana membangun model deep learning yang efektif untuk mendeteksi serangan cyber dan menganalisis anomali pada web server?
5. Bagaimana menerapkan model deep learning dalam praktik analisis forensik serangan cyber dan anomali pada web server?
6. Dapatkah analisis forensik menggunakan pembelajaran mendalam meningkatkan keamanan dan keandalan server web terhadap serangan dunia maya?
7. Bagaimana cara menafsirkan hasil analisis forensik menggunakan pembelajaran mendalam untuk mengidentifikasi sumber serangan siber dan menerapkan langkah mitigasi yang tepat?

Dengan merumuskan permasalahan di atas, penelitian ini dapat fokus pada pengembangan metode dan algoritma deep learning yang sesuai untuk melakukan analisis forensik terhadap serangan cyber dan anomali mesin web host. Hasil penelitian ini dapat memberikan kontribusi terhadap upaya meningkatkan keamanan web server dan mengatasi serangan cyber yang terjadi.

1. **Batasan Masalah**

Batasan masalah dalam penelitian Analisis Forensik Mengenai Serangan Syber Dan Anomali Pada Server Web Menggunakan Deep Learning dapat mencakup:

1. Keterbatasan data yang tersedia: Penelitian ini mungkin terbatas pada kumpulan data yang tersedia untuk dianalisis. Kuantitas data yang tidak mencukupi atau kualitas data yang rendah dapat mempengaruhi keakuratan hasil penelitian.
2. Keterbatasan metode analisis: Pemilihan metode analisis yang tepat sangatlah penting dalam penelitian ini. Beberapa teknik pembelajaran mendalam mungkin lebih cocok dibandingkan yang lain untuk menganalisis serangan dunia maya dan mendeteksi anomali di server web. Oleh karena itu, penting untuk mempertimbangkan keterbatasan dan kompleksitas metode yang digunakan.
3. Akurasi dan deteksi kesalahan: Meskipun metode deep learning dapat memberikan hasil yang akurat dalam menganalisis serangan cyber dan mendeteksi anomali pada server web, deteksi kesalahan tidak dapat sepenuhnya dihindari. Positif palsu dan negatif palsu dapat terjadi sehingga dapat mengurangi efektivitas metode deep learning yang digunakan.
4. Ketergantungan pada teknologi Internet: Penelitian ini mengandalkan teknologi Internet. Jika terjadi gangguan jaringan, kemampuan untuk mendeteksi serangan dan anomali mungkin terganggu atau tidak mungkin dilakukan. Oleh karena itu, dalam melakukan penelitian ini harus memperhatikan faktor-faktor seperti ketersediaan jaringan yang stabil.
5. Keamanan dan privasi data: Dalam penelitian ini, analisis dilakukan terhadap data web server. Oleh karena itu, penting untuk mempertimbangkan masalah privasi dan keamanan data saat melakukan penelitian ini, termasuk perlindungan data dan kepatuhan terhadap peraturan privasi yang berlaku.
6. Skalabilitas: Jika metode deep learning yang digunakan memerlukan sumber daya komputasi yang besar, maka skalabilitas penelitian ini juga perlu diperhatikan. Ketersediaan sumber daya yang memadai seperti CPU dan GPU harus diperhatikan agar pencarian dapat dilakukan secara efisien dan real time.
7. **Tujuan**

Tujuan dari penelitian analisis forensik mengenai serangan siber dan anomali server web adalah:

1. Untuk menganalisis serangan cyber yang terjadi pada web server dengan menggunakan metode analisis forensik. Penelitian ini bertujuan untuk mengidentifikasi berbagai jenis serangan yang dapat terjadi pada server web, seperti serangan DDoS, serangan injeksi SQL, serangan cross-site scripting (XSS), dll.
2. Identifikasi perilaku yang tidak biasa atau mencurigakan di server web. Pencarian ini dimaksudkan untuk mendeteksi aktivitas yang tidak biasa atau aneh, yang mungkin mengindikasikan adanya serangan atau aktivitas jahat di server web.
3. Menerapkan teknik pembelajaran mendalam dalam analisis forensik serangan cyber dan anomali server web. Penelitian ini bertujuan untuk mengoptimalkan proses analisis menggunakan kecerdasan buatan dan teknik deep learning untuk mencapai hasil yang lebih akurat dan cepat dalam mendeteksi dan menganalisis serangan, biasanya pada server web.
4. Tingkatkan keamanan server web dengan mendeteksi serangan cyber dan mengidentifikasi anomali secara real time. Penelitian ini bertujuan untuk memberikan solusi efektif untuk meminimalkan risiko serangan cyber dan anomali pada server web, untuk memberikan keamanan yang lebih baik bagi pengguna dan data yang tersimpan di dalamnya.
5. Berkontribusi pada bidang keamanan siber dan analisis forensik. Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan teknik dan metode dalam menangani serangan cyber dan mengidentifikasi anomali pada web server, guna meningkatkan keamanan sistem informasi di tingkat organisasi dan individu.
6. **Kontribusi Penelitian**

Penelitian Analisis Forensik Serangan Cyber Dan Anomaly Pada Web Server Menggunakan Deep Learning memiliki kontribusi yang signifikan dalam keamanan dan deteksi serangan cyber. Berikut adalah beberapa kontribusi yang dapat diberikan oleh penelitian ini:

1. Meningkatkan keamanan server web: Menggunakan teknik deep learning dalam analisis forensik, penelitian ini dapat membantu meningkatkan Meningkatkan keamanan server web. Pembelajaran mendalam dapat mendeteksi dan mengklasifikasikan serangan cyber dengan akurasi tinggi, membantu administrator sistem mengambil tindakan cepat dan tepat terhadap serangan.
2. Deteksi Anomali Cepat: Deep Learning juga memungkinkan deteksi anomali cepat di server web. Dengan mempelajari pola lalu lintas reguler, model pembelajaran mendalam dapat mengidentifikasi dan melacak anomali mencurigakan dengan akurasi tinggi. Hal ini memungkinkan administrator sistem untuk mengambil langkah proaktif untuk mencegah dan merespons serangan siber.
3. Mengurangi operasi manual: Dengan menggunakan deep learning, penelitian ini dapat mengurangi ketergantungan pada operasi manual dalam analisis forensik serangan cyber. Model deep learning dapat secara otomatis menganalisis data lalu lintas server dan mengidentifikasi serangan atau anomali, menghemat waktu dan upaya bagi administrator sistem.
4. Meningkatkan Respons Terhadap Serangan: Dengan deteksi yang cepat dan akurat, penelitian ini dapat membantu meningkatkan respons terhadap serangan. Melalui identifikasi dan analisis yang mendalam terhadap serangan cyber, penelitian ini dapat menyediakan informasi penting kepada administrator sistem untuk merespons serangan dengan tepat dan efektif.
5. Dukungan terhadap pengembangan sistem keamanan: Hasil penelitian ini dapat memberikan informasi berharga mengenai pengembangan sistem keamanan yang lebih maju. Dengan mempelajari pola dan anomali serangan baru, penelitian ini dapat membantu meningkatkan kemampuan sistem keamanan dalam menghadapi serangan yang semakin kompleks dan canggih.

Secara keseluruhan, penelitian tentang Analisis Serangan Cyber Dan Anomali Pada Web Server Menggunakan Deep Learning telah memberikan kontribusi penting dalam meningkatkan keamanan dan mendeteksi serangan cyber. Dengan menggunakan deep learning, penelitian ini dapat meningkatkan ketahanan web server dan memberikan solusi yang lebih efektif dalam merespons serangan cyber.