Tijauan Artikel: Kecerdasan Buatan didalam Keamanan Siber

a) Definisi Kecerdasan Buatan

Kecerdasan Buatan atau *Artificial Intelegence* yang dibahas di dalam aritikel ini dapat identifakasi sebagai teknologi yang peruntukan untuk meningkatkan kemampuan dalam mendeteksi, merespon, dan mengurangi ancaman siber. Kecerdasan Buatan memanfaatkan algoritma yang dapat digunakan untuk menganalisis data dengan skala besar, mengenali pola, serta mendeteksi keberadaan anomali yang mungkin pertanda serangan siber. AI juga digunakan untuk analisis perilaku, pemrosesan bahasa alami *(Natural Language Processing/NLP*), dan pembelajaran mesin *(machine learning*), untuk memberikan konteks dan wawasan tentang ancaman yang akan muncul.Dengan kemampuannya AI dapat membantu dalam mengelola kerentanan, meningkatkan keamanan autentikasi,dan melindungi jaringan dalam ancaman yang tidak diinginkan dan tidak diketahui.

b) Studi Kasus Pemanfaatan Kecerdasan dalam Keamanan Siber

Artikel ini membahas beberapa studi kasus dan aplikasi AI dalam keamanan siber, antara lain:

1. **Mendeteksi ancaman yang tidak dikenal**: Kecerdasan Buatan dapat digunakan untuk memprediksi ancaman yang tidak diketahui. Dengan kemampuan analisis data yang besar, AI atau Kecerdasan Buatan dapat mengenali pola serangan baru yang mungkin tidak terdeteksi oleh sistem keamanan tradisional yang mana ini merupakan hal yang menjadi keunggulan pada AI atau Kecerdasan Buatan. Contohnya adalah serangan rekayasa sosial (*social engineering*) dan malware canggih yang terus berkembang dan berbahaya bagi sistem operasi.

2. **Manajemen Kerentanan**: AI atau Kecerdasan Buatan dapat membantu organisasi dalam mengidentifikasi dan mengelola kerentanan di dalam sistem mereka dengan lebih cepat dan efisien. Dengan AI atau Kecerdasan Buatan, hal yang dapat membahayakan bagi perusahaan dapat ditangani dengan cepat dan efisien

3. **Analisis Perilaku**: AI atau Kecerdasan Buatan dapat digunakan untuk mempelajari perilaku normal pengguna dan lalu lintas di dalam jaringan. Jika terjadi sesuatu seperti pergerakan yang mencurigakan, AI atau Kecerdasan Buatan dapat mendeteksi potensi ancaman.

4. **Pemrosesan Bahasa Alami (NLP)**: AI menggunakan NLP (*Natural Language Processing*) untuk menganalisis data yang tidak terstruktur, seperti laporan insiden, forum, atau media sosial. Hal ini dapat membantu dalam memberikan konteks dan wawasan tambahan mengenai ancaman atau kerentanan yang sering kali muncul.

5. **Keamanan dalam Autentikasi**: AI atau Kecerdasan Buatan dapat digunakan untuk meningkatkan dan mengembangkan keamanan autentikasi pada sebuah situs web atau aplikasi dengan lebih ketat. Dengan adanya AI atau Kecerdasan Buatan, sistem dapat memverifikasi identitas pengguna dengan lebih akurat dan teliti, terutama disaat pengguna mencoba mengakses akun mereka yang mana akan mempersulit penyusup yang akan masuk ke dalam akun karena harus sesuai dengan Autentikasi Pengguna.
6. **Ancaman yang Tidak di Ketahui**: AI atau Kecerdasan Buatan telah terbukti dapat menemukan dan menangani ancaman yang tidak terduga yang akan membawa malapetaka bagi perusahaan. Terutama bagi peretas yang melakukan ratusan juta serangan dengan berbagai alasan. Disini AI atau kecerdasan buatan sangat berperan penting terutama dalam mengamankan jaringan dengan mendeteksi dan menangani berbagai macam ancaman yang dapat merugikan perusahaan yang bahkan tidak bisa dilakukan oleh manusia.

c) Perkembangan AI dalam Keamanan Siber dari Masa ke Masa

Perkembangan AI atau Kecerdasan Buatan didalam bidang keamanan siber telah mengalami kemajuan yang sangat signifikan dari masa ke masa. Pada awalnya, keamanan siber masih menggunakan sistem tradisional seperti menggunakan *firewall* sebagai sistem keamanan dan deteksi berbasis signature yang tergolong sudah lawas dengan adanya teknologi saat ini. Namun, dengan pengingkatan secara kompleks dan kecanggihan serangan siber, sistem tradisional menjadi tidak efektif dibandingkan dengan teknologi saat ini.

1. **Era Awal (2010-an)**: Pada awal tahun 2010-an, penelitian dimulai untuk fokus pada penggunaan AI atau Kecerdasan Buatan untuk pendektesian spam dan pishing. Misalnya, Ganesan (2010) memperkenalkan konsep bernama "*scareware"* untuk mendeteksi adanya email palsu yang dikirim oleh *hacker*. Pada saat itu, AI masih dalam tahap pengembangan dan lebih banyak digunakan untuk tugas-tugas sederhana seperti deteksi spam.
2. **Perkembangan Menengah (2010-2015)**: Pada periode ini, AI mulai digunakan untuk menganalisis pola serta perilaku dan mendeteksi adanya anomali yang mencurigakan. Penelitian oleh Govardhan (2010) menunjukkan bahwa serangan siber sudah semakin canggih, dan AI dibutuhkan dalam amenghadapi tantangan dinamis ini. Selain itu, AI juga mulai digunakan dalam manajemen kerentanan dan deteksi serangan finansial contohnya perbankan, seperti yang dibahas oleh Shukla dan Upadyaya (2011).
3. **Era Modern (2015-sekarang)**: Dalam beberapa tahun terakhir, AI telah menjadi komponen penting didalam bidang keamanan siber. Dengan adanya kemajuan dalam

machine learning dan NLP, AI kini dapat menganalisis data dalam skala besar atau biasa disebut dengan (*Big Data)* dan mendeteksi adanya kompleksitas ancaman. AI juga dapat digunakan untuk meningkatkan keamanan autentikasi dan melindungi jaringan dari serangan yang tidak terduga. Selain itu, AI telah membantu dalam mengidentifikasi ancaman baru yang muncul, seperti serangan rekayasa sosial dan malware canggih.

4. **Masa Depan**: Artikel ini menekankan bahwa masa depan AI atau Kecerdasan Buatan dalam keamanan siber akan terus berkembang. Interdisipliner kolaborasi, penelitian berkelanjutan, dan pengembangan model AI atau Kecerdasan Buatan yang lebih adaptif akan menjadi kunci dalam menghadapi ancaman siber yang semakin canggih. Selain itu, kerangka etika serta regulasi global sangat perlu dikembangkan untuk memastikan penggunaan AI yang bertanggung jawab dan menghindari hal yang tidak diperlukan.

d) Pengembangan Kecerdasan Buatan Sederhana di Lingkungan Sekitar

Pemantauan lingkungan dengan bantuan CCTV merupakan bentuk penerapan kecerdasan buatan sederhana, sekaligus berfungsi sebagai sistem pendukung keamanan. AI tidak hanya berperan dalam keamanan siber, tetapi juga dapat berfungsi sebagai pengawas 24 jam untuk memantau dan mendeteksi aktivitas mencurigakan.

Kesimpulan

AI atau Kecerdasan Buatan telah menjadi alat yang sangat penting dalam keamanan siber, membantu organisasi dalam mendeteksi, mencegah, dan merespons berbagai ancaman siber dengan lebih efektif dan efisien. Dari deteksi ancaman yang tidak dikenal hingga manajemen kerentanan yang sering disebabkan oleh cara tradisional, AI telah menunjukkan kemampuannya dalam menghadapi tantangan keamanan siber yang selalu berkembang. Perkembangan AI dari masa ke masa menunjukkan bahwa teknologi ini akan terus menjadi bagian yang tidak terpisahkan dari strategi keamanan siber di masa mendatang. Namun, penting untuk memastikan bahwa penggunaan AI dilakukan dengan etika dan regulasi yang tepat untuk melindungi privasi dan keamanan pengguna terutama didalam era banyaknya kejahatan yang semakin marak terjadi seperti yang dilakukan oleh para hacker.