Prosiding Seminar Nasional Ilmu Manajamen, Ekonomi, Keuangan dan Bisnis
Vol. 2, No. 2, 2023: 269 - 284

AI Shield: Protecting Business Data from Cybercrime

Anggi Ariska Putri[1*], Muhammad Asrul Aswar[2]
Universitas Islam Negeri Raden Mas Said Surakarta
Corresponding Author: Anggi anggiariskaputri@gmail.com

ARTICLEINFO

Key word: Cyber Crime, Security Systems, Data, AI, Company

Received : 20 September
Revised : 20 October
Accepted: 25 November

ABSTRAK

This research discusses the application of Artificial Intelligence (AI) in strengthening company data security in collaboration with Firewall systems, Intrusion Detection Systems (IDS), and Cryptography. With the involvement of AI which has algorithmic capabilities and predictive analysis, this qualitative descriptive research provides proactive solutions to security threats, increases detection efficiency and strengthens data security systems. These three systems make it easy to limit illegal network access, detect and encrypt data through coding. These findings have important implications in facing the ever-growing challenges of cyber crime on information security, and provide a strong foundation for a particular company or organization to maintain the integrity and confidentiality of its data.

DOI : https://doi.org/10.55927/snimekb.v2i2.6998
https://journal.formosapublisher.org/index.php/snimekb

AI *Shield*: Melindungi Data Bisnis dari Penjahat Dunia Maya

Anggi Ariska Putri[1*], Muhammad Asrul Aswar[2]
Universitas Islam Negeri Raden Mas Said Surakarta
Corresponding Author: Anggi anggiariskaputri@gmail.com

A R T I C L E I N F O

Kata Kunci: *Cyber Crime*, Sistem Keamanan, Data, AI, Perusahaan

A B S T R A K

Penelitian ini membahas mengenai penerapan *Artificial Intelligence (AI)* dalam memperkuat keamanan data perusahaan yang dikolaborasikan dengan sistem Firewall, *Intrusion Detection System (IDS),* dan Kriptografi. Dengan adanya keterlibatan AI yang memiliki kemampuan algoritma dan analisis prediktif, penelitian yang dilakukan secara deskriptif kualitatif ini memberikan solusi proaktif terhadap ancaman keamanan, meningkatkan efisiensi deteksi, dan memperkuat sistem keamanan data. Ketiga sistem tersebut memberikan kemudahan dalam membatasi akses jaringan ilegal, mendeteksi, dan mengenkripsi data melalui pengodean. Temuan ini memiliki implikasi penting dalam menghadapi tantangan *cyber crime* terhadap keamanan informasi yang terus berkembang, dan memberikan pondasi kuat bagi suatu perusahaan atau organisasi tertentu untuk menjaga integritas dan kerahasiaan data yang dimiliki.

PENDAHULUAN

Transformasi era society 4.0 menuju 5.0 memiliki perjalanan yang menarik dan kompleks karena terjadi perubahan data yang awalnya berbasis fisik menjadi digital. Kemajuan digital ini telah mendominasi di berbagai aspek kehidupan manusia, terutama di bidang ekonomi dan bisnis. Digitalisasi membantu manusia dalam memproses, mengolah, dan menganalisis informasi sehingga mampu menghasilkan data yang relevan secara cepat. Banyak lini bisnis yang telah menerapkan kemajuan digital dalam pelayanan operasionalnya, mulai dari sektor pendidikan, transaksi, hiburan, komunikasi dan informasi. Bahkan, kebutuhan pribadi seperti data dan privasi sekalipun terlayani dengan teknologi. Adanya data berbasis digital membuat individu menjadi lebih leluasa dalam mengakses informasi tanpa terbatas pada ruang dan waktu. Selain itu, perkembangan teknologi ini juga memberikan peningkatan pada kualitas dan efisiensi kapasitas data yang dihasilkan dan dikirimkan (Danuri, 2019)

Sejalan dengan perkembangan dan meluasnya digitalisasi di Indonesia, pasti tidak terlepas dari problematika yang ada, seperti munculnya pola dan varian baru kejahatan berupa *cyber crime* (Danuri & Suharnawi, 2017). Berdasarkan data yang ditunjukkan dalam acara Cyber Crime Summit di Institute Teknologi Bandung (ITB), tingkat kejahatan dunia maya di Indonesia berada dalam kondisi yang mengkhawatirkan, bahkan menempati posisi teratas sebagai negara yang paling sering menjadi sasaran serangan siber (Antoni, 2017). Permasalahan ini memicu munculnya kasus-kasus penipuan dengan berbagai jenis modus, seperti modus undangan atau pengiriman paket berbentuk file APK yang dapat meretas informasi hingga menyebabkan kerugian pada korban. Belakangan ini, diketahui modus tersebut dialami oleh seorang publik figur di tanah air dan menyebabkan kerugian besar akibat membuka file berbentuk APK yang dikirimkan melalui media sosial obrolan.

Tindak kejahatan dunia maya *(cyber crime)* ini tidak hanya menyasar individu, tetapi juga setingkat perusahaan yang sudah terorganisir. Dijelaskan dalam laman CNBC Indonesia terdapat beberapa perusahaan atau lembaga top nasional hingga internasional yang turut mendapat serangan kejahatan dunia maya. Hal ini disebabkan oleh beberapa faktor, salah satunya adalah rentannya sistem keamanan yang ada di perusahaan. Sebagaimana perusahaan yang pernah mengalami insiden serangan cyber antara lain First American Financial Corporation (AS), Capital One (AS), BPJS, Asuransi BRI Life, PT. Bank Syariah Indonesia, PT. BFI Financial Indonesia. Permasalahan terkait kejahatan *cyber crime* yang muncul sangat merugikan baik secara material maupun immaterial. Terlebih lagi apabila data yang tersabotase bersifat rahasia baik data perusahaan ataupun data pribadi konsumen, maka dapat mempengaruhi reputasi perusahaan serta kepercayaan pelanggan. Perusahaan memiliki tanggung jawab terhadap integritas, kerahasiaan, autentikasi data yang pada dasarnya bukan untuk dikonsumsi secara publik tanpa seizin pemilik (Aryani & Susanti, 2022). Maka dari itu keamanan data sangat penting baik bagi perusahaan maupun konsumen.

Perkembangan teknologi digital membuka peluang baru bagi ancaman kejahatan dunia maya, terutama pada era society 4.0 yang dikenal sebagai *informant society* sehingga menciptakan tantangan baru terhadap era selanjutnya. Kemajuan teknologi memberikan gambaran mengenai era society 5.0 bahwa di masa depan manusia akan hidup berdampingan dengan teknologi, seperti kecerdasan buatan. Kecerdasan buatan atau sering disebut AI adalah sistem yang dilengkapi dengan kemampuan *antimalware* yang mampu mencegah kesalahan sistem dan meminimalisir risiko kebocoran data pribadi secara efektif dan efisien. Kemampuan tersebut diperkuat oleh daya komputasi atau kemampuan analisis dan pemrosesan data dalam jumlah besar, sehingga program komputer yang cerdas tersebut memiliki tingkat pembelajaran yang melebihi kemampuan manusia (Disemadi, 2021).

Dengan demikian, problematika mengenai kejahatan dunia maya *(cyber crime)* yang terjadi akhir-akhir ini menjadi isu yang cukup serius untuk diulas. Penulis tertarik untuk menganalisis mengenai pemanfaatan *Artificial Intelligence (AI)* terhadap keamanan data dalam lingkup bisnis khususnya perusahaan. Maka tujuan dari penelitian ini adalah untuk memberikan informasi terhadap khalayak umum termasuk pelaku bisnis supaya memanfaatkan kemajuan teknologi khususnya kecerdasan buatan terutama di era society 5.0 sehingga mampu mengatasi berbagai masalah dan tantangan dalam kehidupan manusia.

TINJAUAN PUSTAKA

Konsep Artificial Intelligence (AI)

Pada era society 5.0, perkembangan teknologi semakin menunjukkan eksistensinya dalam kehidupan manusia. Kecerdasan buatan atau yang lebih populer disebut *Artificial Intelligence (AI)* merupakan bagian dari kemajuan teknologi yang telah berkembang sejak lama dan dirancang untuk memiliki kemampuan yang hampir sama dengan manusia. Pemanfaatan AI membuat sistem dalam bidang teknologi baik telekomunikasi, penyiaran, atau informasi menjadi lebih baik, cepat, dan efisien sehingga mempermudah pekerjaan manusia. *Artificial Intelligence (AI)* dibagi menjadi empat konsep diantaranya *Acting Humanly* (bertindak seperti manusia), *Thinking Humanly* (berpikir seperti manusia), *Thinking Rationaly* (berpikir rasional), dan *Acting Rationally* (bertindak rasional) (Priowirjanto, 2022).

Menurut Russel dan Norvig (2016), *Artificial Intelligence (AI)* adalah program komputer yang mampu membuat keputusan, menyelesaikan masalah, dan membuat prediksi seperti kecerdasan yang dimiliki oleh manusia. Sedangkan, berdasarkan pandangan Rich dan Kevin Knight (Rich & Knight, 1991), *Artificial Intelligence (AI)* merupakan suatu program yang dirancang menjadi cerdas dan pintar sehingga dapat meniru dan melakukan kemampuan lebih baik daripada manusia. John McCarthy (1995) juga menyatakan bahwa *Artificial Intelligence (AI)* adalah suatu proses untuk mengetahui dan merancang mesin supaya berpikir serta berperilaku seperti manusia. Kecerdasan tersebut dapat dirumuskan dengan pengetahuan dan pengalaman yang dimiliki, penalaran dan pemikiran yang logis dalam membuat keputusan dan mengambil tindakan, serta moral yang baik sehingga mesin atau program yang

dirancang harus memiliki pengetahuan *(knowledge base)* dan kemampuan untuk menarik kesimpulan *(inference engine)*.

Pada intinya, *Artificial Intelligence (AI)* merupakan sebuah sistem yang di dalamnya memiliki kemampuan yakni algoritma dan perintah untuk membuat keputusan. Sistem AI tidak terlepas dari campur tangan manusia itu sendiri yang menciptakan program tersebut sehingga dapat diatur dan dikembangkan secara ilmiah dan matematis. Kecerdasan buatan memiliki beberapa kelebihan daripada kecerdasan alami diantaranya bersifat konsisten dan teliti, bersifat permanen selama sistem dan programnya tidak diubah, pengetahuan yang terletak dalam sistem AI mudah diduplikasi dan disebar ke komputer lain dengan mudah, mampu mengerjakan tugas lebih cepat, dan mudah melacak aktivitas pada sistem AI karena terdapat riwayat *(history)* yang tersedia (Kurniawan, 2020). Tidak hanya itu, kecerdasan buatan dilengkapi dengan keunggulan kemampuan dalam menarik kesimpulan atau menalar sedangkan komputasi konvensional tidak dilengkapi kemampuan tersebut (Kusumadewi, 2003).

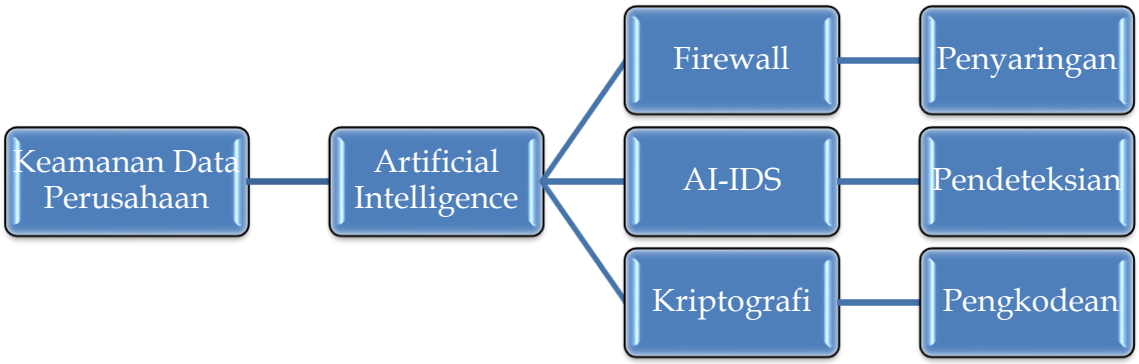
Keamanan Data Berbasis AI Dalam Bisnis

Keamanan data merupakan sebuah sistem yang dalam peranannya ditujukan untuk memberikan penjagaan dan pengamanan paket informasi dalam aktivitas pertukaran data di dunia digital (Sallu & Qammaddin, 2020). Dalam bukunya, Garfinkel dan Lipford (2014) menyebutkan bahwa setidaknya terdapat tiga komponen dalam pengaman data, yaitu kerahasiaan, keutuhan, dan ketersediaan data. Artinya, apabila data sudah berada pada sistem pengamanan maka data akan dijamin kerahasiaannya dan secara eksklusif dilindungi. Perlindungan ini berhubungan dengan tidak adanya perubahan atau modifikasi data pada saat penyimpanan. Tindakan pengaman ini bukan diartikan sebagai tindak pencegahan akses melainkan pemberian kontrol penuh kepada pihak yang berwenang sehingga data tersedia ketika diperlukan. Oleh karena itu, keamanan data menjadi suatu hal penting yang perlu diperhatikan secara khusus terlebih bagi pihak-pihak yang memiliki intensitas tinggi melakukan proses sharing data bersifat rahasia.

Sistem pengaman data umumnya menggunakan kode dalam bentuk password yang terdiri dari kombinasi karakter dengan jumlah yang ditentukan. Namun, proses pengaman ini dianggap masih memiliki cukup resiko karena mudah ditebak dengan jumlah karakter yang minim (Azlin et al., 2018). Dalam perkembangan dunia digital, sistem pengaman data memasuki ranah yang lebih komplek dengan mengkombinasikan kecerdasan buatan. Kemampuan kecerdasan buatan yang semakin meluas membuat pemanfaatannya dapat diaplikasikan di semua hal tidak terkecuali dalam pengaman data bisnis. Data merupakan aset terbesar dalam sebuah organisasi bisnis. Masalah pengamanan data menjadi persoalan yang rumit ketika tidak dikelola dengan tepat. Hal itu karena dapat mempengaruhi kelangsungan operasi dan peluang investasi melalui pengembangan pasar baru (Putri et al., 2020). Dalam proses pengaman data yang lebih kuat dibutuhkan proses penyandian atau enkripsi yang mana dapat dilakukan oleh AI dengan sangat baik. Penggunaan metode penyandian

membuat data asli tidak dapat dibuka tanpa adanya persetujuan dari pihak pemegang akses. Selain itu, standar dalam algoritma yang bersifat kebaruan sangatlah diperlukan untuk memperkuat sistem pengaman data. Sistem algoritma dapat dikombinasikan dengan teknik penyandian sehingga ketika data berpindah tangan maka data tidak akan dapat diakses tanpa persetujuan pihak pemegang akses.

Ruang lingkup pengamanan data berbasis AI tidak hanya untuk memperkuat sistem pertahan keamanan ketika terjadi kebocoran data, lebih dini AI dapat membantu pendeteksian serangan ataupun ancaman dan memberikan perbaikan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Kemampuan belajar yang cepat membuat kecerdasan buatan memiliki kemampuan mempelajari dan mengidentifikasi pola perilaku yang terindikasi sebagai serangan ataupun aktivitas pencarian data rahasia sebagai tindak peretasan. Lebih dalam AI dapat memperkuat keamanan aplikasi melalui proses verifikasi identitas pengguna dan mencegah akses yang tidak sah dengan menganalisis pola perilaku biometrik (Farid et al., 2023).



Gambar 1. Kerangka Konseptual

METODOLOGI

Metode penelitian yang diterapkan dalam penulisan ini adalah pendekatan deskriptif kualitatif, dengan tujuan untuk mengembangkan pengetahuan dan wawasan melalui eksplorasi serta pemahaman yang mendalam. Umumnya, penelitian kualitatif dilakukan ketika permasalahan belum terdefinisikan dengan jelas, tetapi ingin mengungkapkan hal yang tersembunyi, memahami dinamika interaksi sosial, merumuskan teori yang sudah ada, dan meneliti lebih dalam terhadap objek penelitian yang hendak diteliti. Proses analisis data menggunakan metode *content analysis* yang melibatkan pengidentifikasian, pengklasifikasian, penginterpretasian berdasarkan dokumen atau materi tekstual terhadap pola, tema, dan tren dalam data.

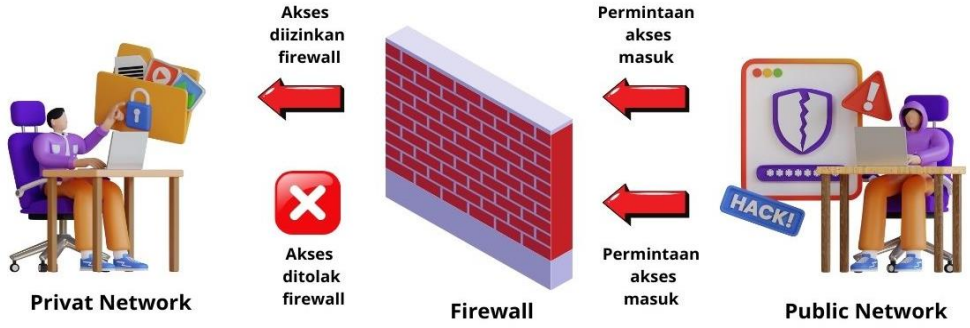
Dalam penelitian ini, peneliti memiliki peran sebagai pengumpul dan penafsiran data. Selaras dengan pandangan yang dikemukakan oleh Nasution dalam (Sugiyono, 2016) bahwa manusia berperan sebagai instrumen utama karena tidak ada pilihan lain. Hal ini disebabkan oleh ketidakpastian dari berbagai aspek, bahkan hasil yang diharapkan masih memerlukan pengembangan sepanjang penelitian sehingga dalam situasi tersebut peneliti sendirilah yang memiliki kendali penuh dalam mencapai tujuan yang diinginkan. Pendekatan pengumpulan data yang digunakan adalah studi literatur, sebagai langkah awal dalam menggali data dari berbagai sumber melalui membaca dan mencatat, serta mengolah bahan penelitian (Zed, 2008). Tujuannya ialah mencari dasar untuk membangun tinjauan pustaka, kerangka berpikir, dan menentukan hipotesis penelitian sehingga peneliti dapat menggunakan variasi pustaka sesuai kebutuhan dan memiliki pendalaman terhadap masalah yang hendak diteliti**.**

HASIL DAN PEMBAHASAN

Di dunia bisnis, data atau privasi merupakan sebuah hal yang sangat penting terlebih jika data tersebut dimiliki oleh perusahaan atau lembaga yang memiliki banyak data yang bersifat confidential dan classified(Yuwinanto, 2011). Data perusahaan yang bersifat krusial ini memerlukan sistem keamanan yang dapat melindungi dari berbagai serangan yang dapat mengancam kerahasiaannya. Ancaman keamanan data dapat berupa usaha untuk memasuki akses tanpa izin, penyalahgunaan data pribadi secara ilegal, hingga secara paksa masuk dan merusak sistem yang sudah ada. Keamanan data berbasis kecerdasan buatan (AI) menjadi penting seiring pesatnya perkembangan teknologi digital. Penerapan kecerdasan buatan pada sektor bisnis tidak hanya memberikan efisiensi pada aspek operasional, tetapi juga memberikan peran ketahanan ganda pada sistem keamanan yang sudah ada. Pemanfaatan AI dapat menjadi inovasi dan strategi pengembangan keamanan data di dunia bisnis terutama dalam perusahaan. Berikut ini uraian tentang penerapan AI pada sistem keamanan data.

Stateful Firewall

Meningkatnya ancaman kejahatan dunia maya *(cyber crime)* semakin menimbulkan kekhawatiran di dunia global. Kejahatan ini dilakukan oleh beberapa orang untuk menembus keamanan suatu sistem, terutama pada perusahaan yang memiliki kumpulan data dalam jumlah besar. Tentunya, perusahaan harus mencari alternatif untuk mengatasi permasalah tersebut salah satunya melalui teknik penyaringan atau disebut firewall. Firewall adalah sebuah *software* yang digunakan untuk memantau dan membatasi akses antar jaringan baik internal maupun eksternal sehingga dapat menjadi solusi untuk mengatasi problematika yang ada (Al-Shaer, 2014).



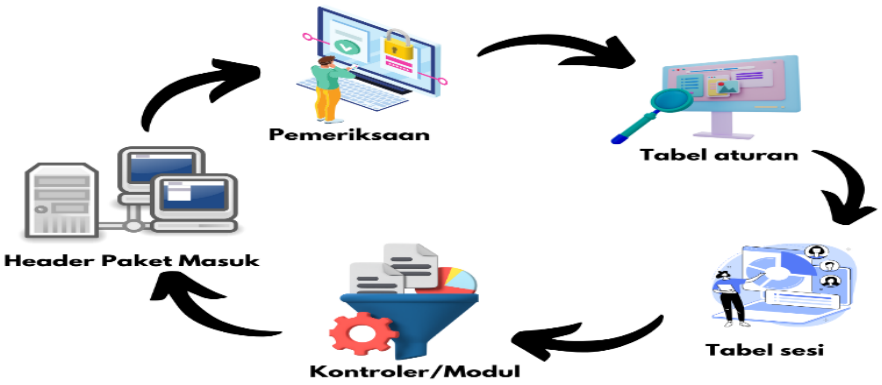
Gambar 2. Ilustrasi Penerapan Firewall

Gambar tersebut menunjukkan bahwa firewall diterapkan dalam sistem untuk melindungi, menyaring, dan menolak sebuah atau semua hubungan pada jaringan pribadi terhadap jaringan luar yang bukan ruang lingkupnya (Purwaningrum et al., 2018).

1. Semua koneksi dari internal ke eksternal harus melewati firewall dengan mengatur pembatasan akses secara menyeluruh.
2. Apabila terdapat akses yang dikenali atau sudah terdaftar, maka dapat menjalin hubungan atau melewati firewall.
3. Firewall harus dilengkapi sistem yang kuat dan aman terhadap serangan.

Dengan konfigurasi yang tepat, firewall mampu mengamankan suatu data atau jaringan pada komputer (Hidayatullah, 2014), yaitu menggunakan menggunakan metode gateway atau metode stateful firewall. Gateway merupakan sebuah perangkat sebuah perangkat yang berfungsi seperti router, yaitu mampu menjadi rute atau patokan untuk menunjukkan tujuan dari suatu lokasi melalui jaringan internet. Gateway juga memiliki fungsi untuk menghubungkan satu jaringan dengan jaringan lainnya meskipun mempunyai rancangan dan bentuk yang berbeda seperti email. Sedangkan, stateful adalah bagian dari firewall yang mampu menggabungkan *packet filtering, proxy*, dan *circuit level* pada suatu sistem. Sehingga, pada lalu lintasnya akan didasarkan sesuai karakteristik paket yang kemudian terdapat sesi pengecekan koneksi untuk memastikan bahwa koneksi tersebut diizinkan (Lahmadi & Festor, 2009).

Dalam penelitian ini, akan berfokus pada satu metode yaitu stateful firewall. Menurut penulis, berdasarkan studi dan penelitian sebelumnya terutama yang dilakukan oleh Vensy Vidya Dkk, metode stateful firewall lebih baik daripada metode gateway karena memiliki beberapa keunggulan seperti peraturan filter firewall sehingga dapat menentukan keaslian otorisasi paket. Aturan tersebut diterapkan pada sumber alamat IP, tujuan alamat IP, dan alamat port. Kemudian, algoritma firewall dalam pemeriksaan dengan metode stateful akan menganalisis untuk mengizinkan atau menolak header paket yang masuk. Kebijakan dalam metode stateful firewall terdiri dari pengelolaan firewall tabel aturan, tabel sesi keamanan informasi arus lalu lintas, dan modul sebagai kontroler yang diprogram dengan aplikasi firewall. Berikut langkah-langkah metode stateful firewall (Vydia et al., 2020)



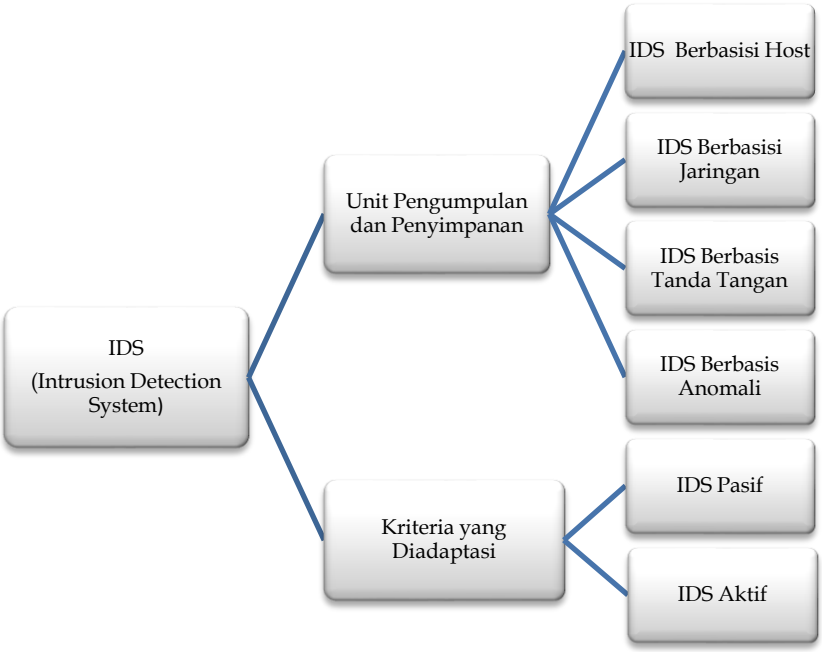
Gambar 3. Ilustrasi Metode Stateful Firewall

1. Pemeriksaan jaringan awal pada paket yang diterima untuk mengurangi beban arus lalu lintas firewall. Kemudian, jika diterima akan dimasukkan dalam proses penyaringan.
2. Menemukan entri aktif dalam tabel sesi dan jika diterima akan dikirimkan sequence nomor check submodule. Apabila tidak ditemukan pada tabel sesi maka akan dikenakan kebijakan firewall.
3. Pemeriksaan header paket sesuai dengan tabel kebijakan firewall. Jika diizinkan akan terbentuk entri sesi baru pada tabel sesi. Apabila tidak maka paket akan dibuang.
4. Pemeriksaan kembali pada tabel sesi untuk menemukan nomor urut kemudian diteruskan ke submodul status sesi pencarian. Jika tidak ditemukan akan dijatuhkan atau dibuang.
5. Status sesi divalidasi dalam tabel sesi dengan menemukan status yang aktif. Jika sesi menyatakan paket tersebut aktif maka akan diteruskan ke pengontrol utama. Apabila yang ditemukan tidak aktif maka akan dibuang atau dijatuhkan.

Sistem Deteksi Intrusi (IDS)

Intrusion Detection System (IDS) merupakan metode pendeteksian ancaman dan pencegahan serangan yang dapat diterapkan dalam perusahaan, lembaga pemerintahan, hingga organisasi keuangan dan perbankan, meliputi Cisco, IBM, Microsoft, Amazon, eBay, dan JPMorgan Chase. IDS juga menjadi bagian dalam membangun infrastruktur keamanan yang mampu melindungi data sensitif dan memberikan respon terhadap serangan yang ditujukan terhadap komputer menggunakan mekanisme yang lebih efisien (Kumar et al., 2010). Penerapan IDS memudahkan administrator dalam mendeteksi tujuan pelanggar yang berusaha memperoleh akses ilegal terhadap jaringan keamanan atau membuat sumber daya sistem tidak tersedia sehingga dapat disalahgunakan. Komponen umum yang digunakan pada sistem IDS adalah identitas pemilik yang akan dipantau dari gangguan (Axelsson, 1999). Hal ini dapat berupa jaringan atau host tunggal;

unit pengumpulan dan penyimpanan data dari berbagai peristiwa serta mengubahnya dalam format yang tepat dan menyimpan ke disk; unit analisis dan pemrosesan data sebagai otak IDS. Selain itu, IDS juga mampu memonitoring sumber aktivitas target dalam bentuk data lalu lintas jaringan pada komputer sehingga dapat mendeteksi serangan yang kemudian akan menghasilkan sebuah sinyal. Berdasarkan jenis IDS, sinyal tersebut diteruskan ke administrator untuk pengambilan keputusan berupa tanggapan otomatis terhadap intrusi atau peringatan aktivitas yang dinilai berbahaya.



Gambar 4. Diagram Jenis Sistem Deteksi Intrusi

Seiring berjalannya waktu, IDS dikolaborasikan dengan kecerdasan buatan yang disebut IDS berbasis AI (AI-IDS). AI-IDS merupakan suatu model yang dirancang menggunakan algoritma pembelajaran mesin untuk memahami dan mengenali pola dari data yang diberikan tanpa ekstraksi awal yang berarti semua string atau data masukan dapat diproses tanpa langkah ekstraksi fitur terpisah (Kim et al., 2020). Pemanfaatan AI dalam IDS membuat pendeteksian serangan menjadi lebih canggih, baik dari pola yang tidak diketahui atau serangan yang dikodekan dari lalu lintas. Berdasarkan pengidentifikasian pola, sistem ini dapat membantu menulis dan meningkatkan aturan snort untuk IDS yang berbasis tanda tangan yang dirancang menggunakan perhitungan probabilitas berbahaya dan pelatihan secara terus menerus sehingga mampu menganalisis serangan web yang tidak dikenal dengan lebih akurat. Penerapan AI-IDS dilatarbelakangi dengan adanya serangan siber yang menggunakan pola tidak beraturan seperti sandi dan penyamaran bypass sistem keamanan. Maka dari itu, untuk mengatasi masalah cyber crime dapat memanfaatkan AI-IDS berbasis tanda tangan karena mampu mendeteksi serangan yang tidak dapat diidentifikasi oleh NIDS (Network Intrusion Detection System). Menurut

Raghunath dan Mahadeo (2008) NIDS berperan sebagai pendeteksi aktivitas mencurigakan yang terdapat dalam lalu lintas jaringan. Hal ini juga didasarkan pada penelitian yang telah berhasil menerapkan AI-IDS dalam lalu lintas berskala big data dengan beberapa langkah sistematis sebagai berikut (Kim et al., 2020).

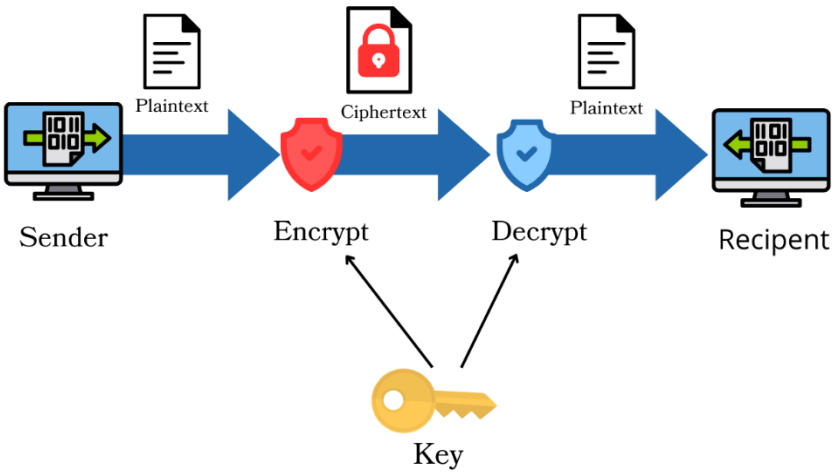
1. Penyimpanan dan Pemisahan Data
   Tahap awal ini dilakukan dengan mengumpulkan informasi analisis baik bersifat positif maupun negatif serta data lalu lintas normal yang diperoleh dari Index Cluster *(Big Data).* Data tersebut kemudian disimpan dan dianalisis. Selanjutnya setelah data berhasil dianalisis, maka akan muncul dua data, yaitu data bermuatan lama dan data yang sudah berlabel oleh AI-IDS. Data yang berhasil dianalisis kemudian diprediksi dengan bantuan AI untuk menguji kelemahan keamanan yang ada. Penerapan AI ini dapat membuat proses data lebih komplek untuk membuat uji keamanan lebih efektif. Proses prediksi memakan waktu cukup lama yang akhirnya menghasilkan data yang telah terbagi sesuai dengan jenis serangan intrusinya. Hasil pembagian data ini yang kemudian menjadi data latih bagi model deep learning.
2. Persiapan dan Pelatihan Data
   Di tahap ini data yang telah terbagi dalam kelompok, kemudian diproses untuk dianalisis struktur data atau sintaks kodenya. Data tersebut kemudian disimpan sekaligus dianalisis menggunakan bantuan kecerdasan buatan untuk mengolah Informasi yang terkandung dalam data. Data atau karakter yang telah diproses diubah menjadi data float untuk dilatih melakukan pembelajaran mendalam dengan Zero padding yang pada umumnya untuk memastikan representasi yang konsisten.
3. Prediksi Untuk Muatan yang Mencurigakan
   Tahap terakhir untuk mendeteksi ancaman dengan melakukan prediksi pada data awal yang mengandung indikasi muatan mencurigakan dan diperiksa menggunakan model yang sudah dilatih pada tahap sebelumnya. Kemudian data disimpan dalam bentuk file JSON dimana data yang terdapat di dalamnya berupa metadata, muatan yang mencurigakan, dan data yang memiliki probabilitas kejahatan.

Sistematika yang sudah dijelaskan di atas membuktikan kemanjuran dari AI-IDS yang mampu mendeteksi serangan yang bervariatif pada NIDS dengan memprediksi melalui model h5 yang telah menunjukkan perkiraan data secara nyata dengan memeriksa serangan sebagai keluaran prediksi. Maksudnya, ketika nilai prediksi mencapai 100%, maka NIDS akan mengetahui bahwa muatannya berbahaya. Namun, hasil dari analisis tidak dapat diandalkan secara penuh karena hasil AI-IDS pertama kemungkinan mengandung kesalahan dalam penganalisisan. Dengan demikian, diperlukan peran dari seorang analisis untuk memastikan langkah terakhir mencapai tingkatan yang stabil. Apabila muatan yang mencurigakan diklasifikasikan sebagai nilai prediksi antara 50-100% dan rata-ratanya 100-500 yang terjadi setiap 3 jam dapat diasumsikan sebagai "normal atau ganas" dan jika kurang lebih dari 50% dari nilai yang sudah

diprediksi berarti diberi label "jinak". Kemudian, AI-IDS akan melakukan pengoptimalan berkelanjutan dengan melatih ulang informasi analisis yang diberi label jinak, berbahaya, dan tidak diketahui. Oleh karena itu, AI-IDS harus digunakan sebagai sistem asisten hingga mencapai tingkat kualitas yang tinggi, tetapi jika kualitas tersebut melampaui kemampuan manusia dengan terus belajar, maka dapat diputuskan sebagai analisis otomatis. Pada akhirnya, AI-IDS menjadi suatu sistem yang memiliki kualitas analisis lebih unggul daripada manusia dan membantu menganalisis keamanan data dari berbagai peristiwa yang tidak diketahui.

Kriptografi

Merebaknya pihak tidak bertanggung jawab yang berusaha memasuki akses yang bukan merupakan otorisasinya membuat banyak pengguna internet merasakan kegelisahan. Dari kondisi ini muncul bidang ilmu pengkodean seperti kriptografi. Kriptografi adalah cabang ilmu yang mengkaji teknik matematis yang berkaitan dengan keamanan informasi, mencakup aspek tingkat kepercayaan, keutuhan data, autentikasi entitas, dan keaslian data. Kemampuan identifikasi dalam Kriptografi dapat digunakan untuk mengetahui keaslian dan pihak pengirim pesan dengan baik. Kriptografi atau bisa disebut Secret Writing (tulisan rahasia) yang bergantung pada pemaksimalan difusi dan kebingungan yang terkait yang mampu mengubah teks biasa menjadi teks tersandi. Idealnya, data terenkripsi dan ciphertext harus sepenuhnya bebas dari pola apa pun. Cipherteks tersebut harus merepresentasikan secara acak dan kompleks dari yang biasanya dikaitkan dengan penerapan fungsi satu arah yang tidak memiliki fungsi invers sehingga memberikan peluang AI dalam pembuatan sandi, klasifikasinya (kekuatan kriptografi), dan analisis atau kriptanalisis data yang terenkripsi. Dalam perkembangannya Kriptografi dapat menjadi opsi dalam melakukan pengamanan data (Mukhtar, 2018).



Gambar 5. Ilustrasi Konsep Kriptografi

Dalam tahap pengaplikasiannya, komponen yang membentuk kriptografi, di antaranya: (Ariyus, 2008)).

1. *Encryption* adalah proses pengubahan pesan atau informasi awal menjadi data baru yang tidak beraturan menggunakan algoritma sehingga memiliki tingkat kesulitan lebih tinggi untuk dikenali.
2. *Decryption* merupakan proses penyusunan ulang pesan-pesan yang teracak sehingga menjadi informasi utuh sesuai data awal yang hendak disampaikan.
3. Kunci merujuk pada elemen yang digunakan untuk melakukan proses enkripsi dan dekripsi. Terdapat dua jenis kunci utama dalam kriptografi, yaitu kunci rahasia *(private key)* dan kunci publik *(public key).*
4. *Ciphertext* adalah pesan yang telah diacak melalui proses Encryption yang membuat pesan tersebut tidak memiliki makna.
5. *Plaintext* atau biasa disebut cleartext adalah Pesan atau informasi asli yang akan diproses di tahap Enkripsi dan dekripsi menggunakan algoritma Kriptografi .
6. Pesan dalam hal ini pesan dapat berupa data yang dikirim melalui saluran informasi ataupun disimpan dalam perangkat.
7. *Cryptanalysis* adalah proses analisis kode dalam upaya untuk merubah ke bentuk semula sesuai data awal yang ingin disampaikan.

Artificial Intelligence (AI) dapat dimanfaatkan untuk menghasilkan sandi karena mampu mengenali pola yang kompleks dalam teks sandi dan mencari tanda tangan yang menentukan kedekatan atau titik serangan dimana terdapat titik kelemahan dalam karakter acak dari data yang sudah terenkripsi. AI juga dilengkapi dengan pelengkap dalam menguji kekuatan metode enkripsi untuk menghasilkan data yang terenkripsi. Dari sini dapat dilihat bahwa AI memiliki peran dalam enkripsi data dan kriptanalisis.

Penggunaan kecerdasaan buatan pada usaha memperkuat keamanan di lingkup perusahaan memberikan banyak keuntungan. Dari segi teknis, Penerapan kecerdasaan buatan membuat sistem keamanan perusahaan dapat mengidentifikasi pola ancaman baru, memberikan respon secara cepat terhadap serangan, dan memperkuat pertahanan jaringan melalui pemantauan terus menerus terhadap aktivitas yang mencurigakan. Sedangkan dari segi ekonomi, Peningkatan keamanan data yang lebih kuat juga berimplikasi pada keuntungan komersial yang diperoleh perusahaan. Perusahaan akan dipandang baik oleh para mitra kerja seperti investor, pelanggan dan pemangku kepentingan lainnya karena dianggap berkomitmen dalam memberikan perlindungan data dan informasi dengan baik. Dari segi biaya perusahaan juga dapat memangkas pengeluaran untuk menangani masalah yang muncul bilamana data tidak dijaga dengan baik sehingga timbul insiden serangan atau kebocoran informasi yang mengharuskan perusahaan melakukan tindakan yang memerlukan biaya yang lebih besar.

KESIMPULAN DAN REKOMENDASI

Keamanan data yang dikolaborasikan dengan kecerdasan buatan (AI) membawa dampak positif dalam melindungi informasi sensitif perusahaan. AI yang dilengkapi dengan kemampuan algoritma dan perintah untuk membuat keputusan dapat mengidentifikasi pola abnormal dan mendeteksi ancaman siber secara *real-time.* Dalam hal ini, perusahaan harus mengintegrasikan keamanan AI dengan strategi sistem keamanan data yang tepat sesuai dengan sektor yang dijalankan, di antaranya Stateful Firewall, AI-IDS, dan Kriptografi. Firewall merupakan batas akses jaringan yang dapat memantau sistem baik secara internal maupun eksternal. AI-IDS adalah metode yang digunakan untuk mendeteksi aktivitas yang mencurigakan. Sedangkan, kriptografi ialah sekumpulan dari kode-kode yang dapat di enkripsi. Ketiga metode tersebut mampu memperkuat sistem jaringan sehingga dapat melindungi data perusahaan secara efektif dan efisien. Perlindungan keamanan data yang kuat dapat meningkatkan kepercayaan dan citra perusahaan di antara mitra kerja sama. Selain itu, perusahaan dapat menghemat biaya terkait serangan keamanan, pemulihan data, dan kebocoran informasi. Dengan demikian, perusahaan dapat memanfaatkan sistem tersebut untuk mewujudkan inovasi dan daya saing yang optimal, sekaligus menjaga keamanan data dan informasi rahasia

PENELITIAN LANJUTAN

Penelitian lanjutan dapat berfokus pada pengembangan sistem keamanan data yang memanfaatkan dan mengintegrasikan teknologi baru sehingga dapat membuka peluang baru untuk meningkatkan keamanan data melalui pendekatan inovatif dan kecanggihan teknologi

DAFTAR PUSTAKA

Al-Shaer, E. (2014). *Automated Firewall Analytics (Design, Configuration, and Optimization)*.

Antoni. (2017). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani*, *17*(2).

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi)* (S. Suyantoro, Ed.; 1st ed.). CV. Andi Offset.

Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen. *Ahmad Dahlan Legal Perspective*, *2*(1).

Axelsson, S. (1999). Research in Intrusion-Detection Systems:ASurvey. *Technical Report (Department of Computer Engineering)*, *120*.

Azlin, Musadat, F., & Nur, J. (2018). Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64. *Jurnal Informatika*, *7*(2).

Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Informasi Komputer Akuntansi Dan Manajemen*, *15*(2).

Danuri, M., & Suharnawi. (2017). Tren Perkembangan Teknologi. *Jurnal Ilmiah Informasi Komputer Akuntansi Dan Manajemen*, *13*(1).

Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2).

Farid, I., Reksoprodjo, A. H., & Suhirwan. (2023). Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber. *Jurnal Ilmu Pengetahuan Sosial*, *10*(2).

Garfinkel, S., & Lipford, H. R. (2014). *Usable Security (History, Themes, and Challenges)*. Morgan & Claypool Publishers.

Hidayatullah, S. (2014). Analisis dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSEC. *Jurnal Informatika*, *1*(2).

Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, *8*, 70245–70261.

Kumar, G., Kumar, K., & Sachdeva, M. (2010). The Use Of Artificial Intelligence Based Techniques for Intrusion Detection: A Review. *Springer Link*, *34*(4).

Kurniawan, R. (2020). *Kecerdasan Buatan (Artificial Intelligence)*. UIN Sumatera Utara Medan.

Kusumadewi, S. (2003). *Artificial Intelligence (Teknik dan Aplikasinya)* (1st ed.). Penerbit Graha Ilmu.

Lahmadi, A., & Festor, O. (2009). SecSip: A stateful Firewall For SIP-based Networks. *IFIP/IEEE International Symposium on Integrated Network Management*.

McCharthy, J. (1995). What has AI in Common with Philosophy?. *IJCAI (International Joint Conference on Artificial Intelligence)*.

Mukhtar, H. (2018). *Kriptografi Untuk Keamanan Data* (1st ed.). Deepublish.

Priowirjanto, E. S. (2022). Urgensi Pengaturan Mengenai Artificial Intelligence Pada Sektor Bisnis Daring Dalam Masa Pandemi Covid-19 di Indonesia. *Jurnal Bina Mulia Hukum*, *6*(2).

Purwaningrum, F. A., Darmadi, E. A., & Purwanto, A. (2018). Optimalisasi Jaringan Menggunakan Firewall. *Jurnal Komputer & Informatika*, *2*(3).

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). Pentingnya Keamanan Data Dalam Intelijen Bisnis. *Jurnal Sistem Informatika*, *1*(2).

Raghunath, B. R., & Mahadeo, S. N. (2008). Network intrusion detection system (NIDS). *Proceedings - 1st International Conference on Emerging Trends in Engineering and Technology, ICETET 2008*, 1272–1277.

Rich, E., & Knight, K. (1991). *Artificial Intelligence* (2nd ed.). McGraw-Hill.

Russell, S., & Norvig, P. (2016). *Artificial Intelligence A Modern Approach* .

Sallu, S., & Qammaddin. (2020). Keamanan Data Pembelajaran Online Jaringan Komputer di Perguruan Tinggi. *Jurnal Instruksional*, *2*(1).

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D* (24th ed.). Alfabeta.

Vydia, V., Surono, & Setiarso, G. (2020). Application Gateway dan Stateful Inspection Method Pada Implementasi Firewall Untuk Optimasi Keamanan Jaringan Komputer. *Jurnal Pengembangan Rekayasa Dan Teknologi*, *16*(2).

Yuwinanto, H. P. (2011). Privasi Online dan Keamanan Data. *Jurnal Palimpsest*, *2*(2).

Zed, M. (2008). *Metode Penelitian Kepustakaan* (2nd ed.). Yayasan Pustaka Obor Indonesia.