STUDI LITERATUR: ANCAMAN SERANGAN SIBER *ARTIFICIAL INTELLIGENCE* (AI) TERHADAP KEAMANAN DATA DI INDONESIA

LITERATURE STUDY: THE THREAT OF ARTIFICIAL INTELLIGENCE (AI) CYBERATTACKS ON DATA SECURITY IN INDONESIA

Anastasya Zalsabilla Hermawan[1*], M. Novianto Anggoro[1], Ditha Lozera Devi[1], Asif Faroqi[1]
[*]E-mail: Anastasyazher@gmail.com
[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Proses perkembangan pada teknologi Artificial Intelligence (AI) cukup tren saat ini dalam berbagai aspek kehidupan telah memberikan dampak yang signifikan, termasuk keamanan data. Namun, dengan kemajuan tersebut juga muncul ancaman serangan siber AI yang dapat mengancam keamanan data terutama di Indonesia. Penelitian ini bertujuan untuk memberikan sebuah pemahaman yang lebih baik tentang ancaman serangan siber AI terhadap keamanan data di Indonesia dengan menggunakan metode pendekatan *Systematic Literature Review* (SLR). Dari hasil analisis diperoleh bahwa terdapat beberapa jenis serangan siber yang melibatkan penggunaan Artificial Intelligence (AI) yang dapat mengancam keamanan data di Indonesia. Salah satunya adalah serangan Botnet AI, di mana komputer yang terinfeksi malware dapat dioperasikan dan dipantau oleh botmaster untuk melancarkan serangan, seperti pemerasan. Dampak serangan siber AI terhadap keamanan data di Indonesia sangat signifikan. Salah satu dampaknya adalah pencurian data sensitif, seperti data banking dan informasi pribadi, yang dapat dieksploitasi untuk kepentingan komersial atau kejahatan lainnya. Untuk melindungi data dari serangan siber AI, beberapa langkah dan upaya telah diambil di Indonesia. Salah satunya adalah menerapkan access control dan teknik enkripsi untuk big data guna membatasi hak akses dan memberikan kerahasiaan data yang kuat. Pada penelitian ini juga memberikan sebuah pemahaman yang lebih baik tentang ancaman serangan siber AI terhadap keamanan data di Indonesia. Diharapkan hasil dari penelitian ini dapat menjadi dasar untuk proses pengembangan strategi keamanan yang lebih efektif dan upaya perlindungan data yang lebih baik di era AI yang terus berkembang.

Kata kunci*: Siber, Artificial Intelligence, Serangan, Keamanan Data.*

Abstract

The development process on Artificial Intelligence (AI) technology is quite the current trend in various aspects of life has had a significant impact, including data security. However, with this progress, there is also a threat of AI cyber attacks that can threaten data security especially in Indonesia. The study aims to provide a better understanding of the threat of AI cyber attacks on data security in Indonesia using the method of Systematic Literature Review. (SLR). Analysis shows that there are several types of cyber attacks involving the use of Artificial Intelligence (AI) that can threaten data security in Indonesia. One of them is an AI botnet attack, in which a computer infected with malware can be operated and monitored by a botmaster to launch attacks, such as blackmail. The impact of AI cyber attacks on data security in Indonesia is very significant. One impact is the theft of sensitive data, such as banking data and personal information, which can be exploited for commercial or other criminal purposes. To protect data from AI cyber attacks, several steps and efforts have been taken in Indonesia. One is to implement access control and

encryption techniques for big data to limit access rights and provide strong data confidentiality. The study also provides a better understanding of the threat of AI cyber attacks on data security in Indonesia. It is hoped that the results of this research could be the basis for the process of developing more effective security strategies and better data protection efforts in the ever-expanding era of AI.
***Keywords**: Cyber, Artificial Intelligence, Attacks, Data Security.*

1. PENDAHULUAN

Pesatnya perkembangan teknologi digital yang semakin maju dan dengan berbagai kecerdasan buatan atau *Artificial Intelligence* (AI) di berbagai bidang kehidupan manusia telah banyak digunakan. AI telah memberikan kemajuan yang signifikan di beberapa bidang seperti, industri, kesehatan, dan layanan publik. Akan tetapi seiring dengan kemajuannya, ancaman serangan siber dapat muncul dan melibatkan penggunanya. Serangan siber AI dinilai merugikan karena menyerang keamanan data dan privasi pengguna. Adanya teknologi komputer telah membentuk ruang baru yang merupakan sebuah dunia komunikasi berbasis komputer disebut dengan *cyberspace*. Ruang baru tersebut tidak hanya menimbulkan dampak baik tapi juga menimbulkan dampak buruk, sering kali beberapa oknum memanfaatkanya untuk melakukan kejahatan di *cyberspace* biasa disebut dengan kejahatan siber (*cybercrime*). *Cybercrime* ialah suatu perbuatan menggunakan jaringan komputer yang melawan hukum dilakukan dengan menjadikan komputer sebagai objek, dengan cara memperoleh keuntungan dari kerugian orang lain [1].
Di Indonesia masih kurangnya kesadaran dan pemahaman masyarakat mengenai ancaman serangan siber AI terhadap keamanan data mereka. Diperlukan penelitian yang komprehensif untuk memahami ancaman-ancaman serta dampaknya terhadap keamanan data di Indonesia. Tujuan dari penelitian ini untuk memberikan pemahaman yang lebih baik tentang ancaman serangan siber AI terhadap keamanan data di Indonesia. Dengan pemahaman ini, diharapkan dapat dikembangkan strategi perlindungan yang efektif untuk melawan serangan siber AI dan memastikan privasi pengguna terjaga dengan baik. Diharapkan bahwa hasil dari penelitian ini akan memberikan kontribusi yang signifikan dalam meningkatkan kesadaran masyarakat, pemerintah, dan sektor swasta di Indonesia tentang ancaman serangan siber AI terhadap keamanan data dan privasi. Selain itu, dari penelitian ini diharapkan dapat memberikan panduan dan rekomendasi untuk pengembangan kebijakan dan strategi perlindungan data yang lebih baik dalam menghadapi serangan siber AI di Indonesia.

2. METODOLOGI

Pada penelitian ini menggunakan metodologi dengan pendekatan *Systematic Literature Review (SLR).* Metode *Systematic Literature Review (SLR)* merupakan sebuah proses mengidentifikasi masalah, menilai, dan menafsirkan data penelitian yang ada bertujuan untuk menjawab pertanyaan dari penelitian secara tepat [2]. Berikut tahapan dalam metode *Systematic Literature Review*.

2.1 Rumusan Masalah

Pada tahap ini peneliti menentukan rumusan masalah yang akan diulas secara rinci. Berdasarkan kebutuhan topik penelitian, berikut hasil pertanyaan penelitian dalam penelitian ini adalah:
RQ1. Apa saja jenis-jenis serangan siber yang melibatkan penggunaan *Artificial Intelligence* (AI) yang dapat mengancam keamanan data di Indonesia?
RQ2. Apa saja dampak yang timbul dari serangan siber *Artificial Intelligence* (AI) terhadap keamanan data di Indonesia?
RQ3. Apakah upaya dan langkah-langkah yang bisa diambil Indonesia untuk melindungi data dari serangan siber *Artificial Intelligence* (AI)?

2.2 Mencari Literature (*Identification*)

Proses pencarian literature dilakukan melalui pencarian manual dari artikel jurnal atau prosiding yang relevan untuk menjawab pertanyaan dari rumusan masalah atau *research question* (RQ).

2.3 Memilih Hasil Pencarian *Literatur* yang sesuai *Quality Assessment (Penyaringan dan Kelayakan)*

Tahap ini dilakukan untuk memilah data yang ditemukan layak atau tidak untuk digunakan dalam penelitian dan pada tahap ini dipilihnya kriteria inklusi dan eksklusi (*Population, Intervention, Comparison, Outcomes, Study*) seperti pada Tabel 1.

Table 1. Tabel Inklusi dan Eksklusi

Kriteria	Inklusi	Eksklusi
Population	Terkait studi tentang ancaman serangan siber *Artificial Intelligence* (AI) terhadap keamanan data di Indonesia.	Studi yang tidak terkait dengan ancaman serangan siber *Artificial Intelligence* (AI) terhadap keamanan data di Indonesia.
Outcomes	Jenis serangan, dampak, dan langkah perlindungan dari serangan siber *Artificial Intelligence* (AI).	-
Kriteria	Inklusi	Eksklusi
Tahun Publikasi	Tahun 2018	Sebelum tahun 2018
Bahasa	Indonesia dan Inggris	Selain Indonesia dan Inggris

Selanjutnya dilakukan penilaian kualitas atau *Quality Assessment* (QA) yang terdapat pada setiap artikel dapat dilihat pada Tabel 2. Artikel yang akan dinilai adalah artikel yang telah memenuhi kriteria dari inklusi dan eksklusi.

Table 2. *Quality Assessment*

QA	Keterangan
QA1	Apakah artikel tersebut sesuai dengan topik yang ditentukan yaitu serangan siber dan Artificial Intelligence di Indonesia?
QA2	Apakah artikel tersebut menjelaskan jenis serangan siber Artificial Intelligence?
QA3	Apakah artikel tersebut menjelaskan bagaimana dampak dari serangan siber dan *Artificial Intelligence?*
QA4	Apakah artikel tersebut memuat tentang informasi ancaman serangan siber dan *Artificial Intelligence*?
QA5	Apakah artikel tersebut terbit pada tahun 2018 atau setelahnya?
QA6	Apakah artikel tersebut berbahasa Indonesia dan bahasa inggris?

Dari setiap artikel, akan diberi nilai untuk setiap pertanyaan diatas.
Y (Ya) : Untuk artikel yang lolos dari semua kriteria diatas
T (Tidak) : Untuk artikel yang tidak lolos dari kriteria diatas.
Tabel 3 merupakan hasil dari penilaian kelayakan artikel.

Table 3. *Quality Assessment*

No	Judul	Penulis	QA						Ket	
			Q1	Q2	Q3	Q4	Q5	Q6	Y	T
1.	Ancaman dan Solusi Serangan Siber di Indonesia	Sahat Parulian, Devi Anassalifa, Meiliya Cahya Yustina	✓	✓	✓	✓	✓	✓	✓	

2.	Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphisher, Shellphish Dan Whphisher: Phising.	Ni Komang Arista Tri Wahyuni	✓	✓	✓	✓	✓	✓	✓	
3.	Deepfake, Tantangan Baru Untuk Netizen	Itsna Hidayatul Khusna, Sri Pangestuti	✓	✓	✓	✓	✓	✓	✓	
4.	Botnet Detection Using Independent Component Analysis	Wan Nurhidayah Ibrahim	✓	✓	✓	x	✓	✓		✓
5.	Cybersecurity in big data era: From securing big data to data-driven security	Danda B. Rawat	✓	✓	✓	✓	✓	✓	✓	
6.	Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia	Nurbaiti Ma'rufah, Hayatul Khairul Rahmat, I Dewa Ketut Kerta Widana	✓	x	✓	✓	✓	✓		✓
7.	Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia	Muhammad Faqih Faathurrahman, Enni Soerjati Priowirjanto.	✓	✓	✓	✓	✓	✓	✓	
8.	Analisis Kebutuhan Senjata Siber Dalam Meningkatkan Pertahanan Indonesia Di Era Peperangan Siber	Sri Hidayati, Rudi A.G. Gultom	✓	✓	✓	✓	✓	✓	✓	
9.	Kejahatan Siber Sebagai Penghambat E-Commerce Dalam Perkembangan Industri 4.0 Berdasarkan Nilai Budaya Indonesia	Sheryn Lawrencya, Margamu Desy Putri Dewi	✓	✓	✓	✓	✓	✓	✓	
10.	Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)	Abdul Hadi, Bima Guntara	✓	x	✓	✓	✓	✓		✓
11.	Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber	Ishak Farid, Agus HS Reksoprodjo, Suhirwan	✓	✓	✓	✓	✓	✓	✓	
12.	Artificial Intelligence and Indonesia Government Cyber Security Strategies	Rundri Andewi, Muhammad Rizki, Risky Yustiani Posumah	✓	✓	✓	✓	✓	✓	✓	

13.	Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence	Azizah Nur Rahmatika	✓	✓	✓	✓	✓	✓	✓	
14.	Cyber Security Meets Artificial Intelligence: A Survey	Jian-hua	✓	✓	x	✓	✓	✓		✓
15.	Artificial Intelligence in Cyber Security: Research advances, challenges, and opportunities	Zhimmin Zhang, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, Kim Kwang Raymond Choo	x	✓	✓	✓	✓	✓		✓
16.	Artificial Intelligence and Cyber Defense System forBanking Industry: A Qualitative Study of AIApplications and Challenges	Khalifa AL-Dosari, Noora Fetais, and Murat Kucukvar	✓	✓	✓	✓	✓	✓	✓	
17.	Application Of Artificial Intelligence Techniques To Combating Cyber Crimes : A Review	Selma Dilek, Hüseyin Çakır and Mustafa Aydın	✓	✓	✓	✓	x	✓		✓
18.	Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management	Dr. Geethamanikanta Jakka, Nikhitha Yathiraju, Dr. Meraj Farheen Ansari	✓	✓	✓	✓	✓	✓	✓	
19.	Artificial Intelligence and Cyber Security - Face to Face With Cyber Attack - A Maltese Case Of Risk Management Approach	Narcisa Roxana Mosteanu, Kevin Galea	✓	✓	✓	✓	✓	✓	✓	
20.	The Emerging Threat of Ai-driven Cyber Attacks: A Review	Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz, and Vera Pospelova	✓	✓	✓	✓	✓	✓	✓	

2.4 Analisis Hasil *Literatur* dari Artikel yang Lolos *Quality Assessment*

Tahap ini digunakan peneliti untuk menganalisis, menguraikan, dan membedakan data yang digunakan, untuk digolongkan dan dikelompokkan sesuai dengan kriteria *Quality Assessment*. Dari penilaian pada artikel diatas terdapat artikel yang lolos pada *Quality Assessment* (QA) sebanyak 14 Artikel dan Artikel yang tidak lolos *Quality Assessment* (QA) sebanyak 6 Artikel.

2.5 Membuat Kesimpulan Penelitian

Ini merupakan tahap membuat kesimpulan berupa pernyataan singkat dari analisis deskripsi yang berasal dari fakta-fakta yang memiliki hubungan logis dan berisikan jawaban atas pertanyaan yang sudah diajukan pada bagian rumusan masalah (Tabel 4).

Table 4. Pengumpulan Data

Pengumpulan Data	Keterangan
Q1	Jenis-jenis ancaman yang serangan siber Artificial Intelligence (AI).
Q2	Dampak yang timbul dari serangan siber Artificial Intelligence (AI) terhadap keamanan data di Indonesia
Q3	Upaya dan langkah-langkah yang bisa diambil Indonesia untuk melindungi data dari serangan siber Artificial Intelligence

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pencarian

Tabel 5 menunjukkan hasil dari proses pencarian. Pada proses pencarian artikel dilakukan dengan menggunakan kata kunci: *ancaman siber, serangan siber, Artificial Intelligence.* Berikut beberapa artikel yang telah diseleksi sesuai dengan kriteria inklusi, eksklusi, dan kriteria kualitas.

Table 5. Artikel Jurnal dan Prosiding Terpilih

Tahun	Nama Jurnal atau Prosiding	Judul Artikel
2023	Jurnal Teknik Mesin, Elektro dan Ilmu Komputer	Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphisher, Shellphish Dan Whphisher: Phising.
2019	PROMEDIA (Public Relation Dan Media Komunikasi)	Deepfake, Tantangan Baru Untuk Netizen
2020	International Conference on Public Organizing	Artificial Intelligence and Indonesia Government Cyber Security Strategies
2021	TELNECT (Telecommunications, Networks, Electronics, and Computer Technologies)	Ancaman dan Solusi Serangan Siber di Indonesia
2021	IEEE Transactions on Services Computing	Cybersecurity in big data era: From securing big data to data-driven security
2022	Jurnal Peperangan Asimetris	Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence
2023	NUSANTARA : Jurnal Ilmu Pengetahuan Sosial	Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber
2022	Cybernetics and Systems An International Journal	Artificial Intelligence and Cyber Defense System forBanking Industry: A Qualitative Study of AIApplications and Challenges
2022	Applied Artificial Intelligence	The Emerging Threat of Ai-driven Cyber Attacks: A Review
2022	Journal of Positive School Psychology	Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management
2020	Ecoforum Journal	Artificial Intelligence and Cyber Security - Face to Face With Cyber Attack - A Maltese Case Of Risk Management Approach
2022	Jurnal Indonesia Sosial Teknologi	Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten

		Pornografi Berdasarkan Hukum Positif Indonesia
2021	Prosiding Serina	Kejahatan Siber Sebagai Penghambat E-Commerce Dalam Perkembangan Industri 4.0 Berdasarkan Nilai Budaya Indonesia
2020	Teknologi Persenjataan	Analisis Kebutuhan Senjata Siber Dalam Meningkatkan Pertahanan Indonesia Di Era Peperangan Siber

3.2 Hasil Studi Literature

Berdasarkan temuan hasil studi literatur dan data yang dikumpulkan menghasilkan informasi sebagai berikut.

3.2.1 Jenis-jenis Serangan Siber AI

Serangan Botnet *Artificial Intelligence* (AI), Botnet ialah sekumpulan komputer yang sudah terinfeksi oleh perangkat lunak berbahaya (malware) yang dijalankan oleh botmaster (Ibrahim dkk., 2022). Semua perangkat Internet of Things (IoT) seperti komputer, kamera web, cctv, dan perangkat seluler dapat terinfeksi oleh malware. Perangkat yang sudah terinfeksi dapat dioperasikan dan dipantau dari jarak jauh oleh botmaster. Tujuan utama dari botnet ini ialah untuk melancarkan serangan pada korban, dapat berupa pemerasan.

Badan Siber dan Sandi Negara (BSSN) telah mencatat bahwa MyloBot Botnet menominasi anomali trafik di indonesia dengan jumlah 44,62 persen/lebih dari 730 juta anomali pada tahun 2021. MyloBot Botnet ini menargetkan sistem operasi windows dengan menyebar melalui spam pada pesan e-mail dan file unduhan yang sudah terinfeksi. Setelah botnet terinstall, botnet dapat mematikan windows defender dan menghapus file .exe yang dapat menyebabkan hilangnya data.

Serangan Phishing Cerdas, Phising adalah serangan siber dengan informasi atau data sensitif korban sebagai targetnya, dengan mengirim serangan melalui pesan email, unggahan di media sosial, dan pesan teks (Wahyuni dkk., 2023). Serangan ini dilakukan untuk menipu atau memancing korban agar menekan tautan serta menginput informasi username dan password korban. Data yang menjadi incaran phising adalah data akun pribadi dan data finansial seperti kartu kredit dan rekening bank.

Baru-baru ini di Indonesia sedang marak phising menggunakan file aplikasi yang dikirimkan melalui pesan WhatsApp. Pelaku menjalankan aksinya dengan memperdaya korban agar mengunduh file aplikasi dengan berbohong bahwa itu adalah file undangan pernikahan. Setelah file diunduh maka rekening tabungan korban dapat dikuras habis oleh pelaku.

Serangan *Deepfake* dengan Generative Adversarial Networks (GAN), *Deepfake* merupakan teknologi yang mampu membuat cerminan dari manusia berdasarkan kecerdasan buatan/AI. Teknologi ini menyatukan serta meletakkan video dan gambar yang ada ke sumber video atau gambar memakai teknik Generative Adversarial Network (GAN). GAN ditemukan pada tahun 2014 oleh Ian Goodfellow dari data yang telah ada secara algoritma sebagai jalan untuk menciptakan data baru. Selain itu, GAN dapat membuat audio baru dari audio yang telah ada dan teks baru dari teks yang pernah ada. (Khusna dan Pangestuti., 2019)

Pada 2018 aplikasi bernama FakeApp untuk membuat deepfake menyebar luas dan dapat diunduh oleh siapa saja. Dengan fitur dari FakeApp dapat disalahgunakan dengan tujuan penyebaran hoax dan ujaran kebencian di Indonesia. Seperti halnya pada tahun 2022, artis Nagita Slavina menjadi korban dari deepfake. Terdapat video berdurasi 61 detik yang menampilkan adegan tidak senonoh dengan wajah yang mirip dengan Nagita.

3.2.2 Dampak dari Serangan Siber AI

Dampak serangan siber *Artificial Intelligence* (AI) terhadap keamanan data di Indonesia dapat sangat signifikan. Beberapa dampak yang ditimbulkan dari serangan siber *Artificial Intelligence* (AI) sebagai berikut:

Pencurian data sensitif, serangan siber AI tersebut mengarah pada pencurian data sensitif seperti informasi pribadi, informasi keuangan, atau informasi industri. Data yang dicuri kemudian dapat dieksploitasi untuk kepentingan komersial atau kejahatan lainnya. Tepatnya di tahun 2019, terjadi serangan serangan siber yang melibatkan *Artificial Intelligence* (AI) di Bank Negara Indonesia (BNI). Serangan tersebut menyebabkan data nasabah yang mencapai jutaan terpapar dan digunakan untuk melakukan pencurian identitas dan penipuan keuangan.

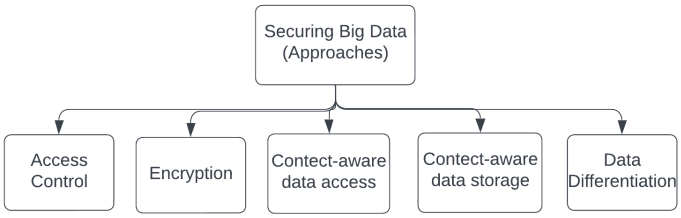
Serangan Ransomware, *Artificial Intelligence* (AI) dapat digunakan sebagai salah satu untuk mengembangkan serangan ransomware yang lebih kompleks dan canggih. Serangan tersebut digunakan untuk mengenkripsi data korban dan meminta tebusan dalam bentuk mata uang kripto untuk mengembalikan akses ke data tersebut. Pada tahun 2017, serangan ransomware yang melibatkan *Artificial Intelligence* (AI) terjadi di sebuah rumah sakit di Jakarta menjadi salah satu korban. Data pasien yang tersimpan dalam sistem rumah sakit dienkripsi, dan para pelaku minta tebusan yang cukup besar untuk mengembalikan akses ke data tersebut.

Manipulasi Informasi, serangan yang dilakukan *Artificial Intelligence* (AI) lainnya juga dapat digunakan untuk menyebarkan informasi palsu atau merusak reputasi melalui media sosial atau platform online lainnya. serangan tersebut dapat berdampak negatif terhadap stabilitas politik, ekonomi, dan sosial di Indonesia. Tepatnya pada tahun 2019, terjadi serangan siber berbasis *Artificial Intelligence* (AI) yang digunakan untuk mencuri data pribadi pengguna. Serangan ini menyebabkan jutaan data para pengguna terpapar dan dipergunakan sedangkan tujuan merugikan pihak lain.

3.2.3 Upaya dan Langkah Perlindungan

Berikut langkah dan upaya yang dilakukan Indonesia untuk melindungi data dari serangan siber *Artificial Intelligence* (AI):

Access Control dan Teknik Encryption untuk Big Data, Banyak perusahaan besar di Indonesia telah mengadopsi dua metode ini sebagai upaya menjaga privasi dan mencegah akses yang tidak sah terhadap Big Data. Access Control digunakan untuk mengatur dan membatasi hak akses terhadap data, sedangkan Teknik Encryption memberikan tingkat keamanan tinggi terhadap kerahasiaan data. Melalui enkripsi, data hanya dapat dilihat oleh entitas yang memiliki otorisasi khusus. Sementara itu, Access Control berfokus pada upaya membatasi akses terhadap data tersebut . Gambar 1 merupakan teknik yang biasa dipakai untuk melindungi big data.



Gambar 1. Teknik pengamanan big data

Salah satu contoh penerapan alternatif untuk mengamankan Big Data adalah melalui penggunaan model berdasarkan *blockchain* yang melibatkan *smart contract* dan teknologi *blockchain* sebagai mekanisme pengamanan.

Applying Artificial Intelligence, Saat ini sedang tren sebuah Virus Polymorphic berbasis AI, dan ada aplikasi yang bisa mengubah malware menjadi trik perangkat lunak pembelajaran mesin antivirus. Dalam percobaan dilakukan oleh Endgame (sebuah perusahaan keamanan), mereka mengetahuinya bahwa AI memiliki titik buta yang dapat diketahui oleh AI lainnya aplikasi. Ini terbukti seperti yang terlihat dalam Generative Adversarial Jaringan ditemukan oleh peneliti google. Di indonesia sendiri ada beberapa perusahaan yang telah menerapkan AI untuk sistem keamanan mereka seperti GOjek, Tokopedia, Traveloka, Telkom, dan OVO.

Decentralized and Context-aware Data Storage, Perusahaan-perusahaan besar seperti GAFA (Google, Apple, Facebook, Amazon) telah mengumpulkan sejumlah besar data. Mereka memilih untuk menerapkan penyimpanan data yang terdesentralisasi dan memiliki pemahaman terhadap konteks, karena metode ini dianggap lebih aman dalam menangkal serangan dan tidak rentan terhadap masalah kegagalan satu titik. Meskipun di Indonesia masih sedikit perusahaan yang secara khusus dikenal menerapkan konsep Penyimpanan Data yang Terdesentralisasi dan Context-Aware, beberapa perusahaan seperti HARA sudah mengadopsi pendekatan ini.

4. KESIMPULAN DAN SARAN

Hasil dari penelitian ini, dapat diambil kesimpulan bahwa terdapat tren serangan siber yang dilakukan oleh AI, seperti Botner, Phishing Cerdas yang merujuk pada serangan siber di mana AI digunakan untuk meningkatkan keefektifan dan tingkat akurasi serangan phishing. Serangan-serangan ini dapat menyebabkan kerugian finansial, pencurian data sensitif, dan merusak reputasi individu maupun perusahaan.

Serangan siber AI terhadap keamanan data di Indonesia menimbulkan dampak yang sangat signifikan. Salah satu dampaknya adalah pencurian data sensitif, seperti informasi pribadi dan data keuangan, yang dapat dieksploitasi untuk kepentingan komersial atau kejahatan lainnya. Terdapat beberapa cara atau metode yang efektif untuk mencegah terjadinya serangan siber AI, seperti Access Control dan Teknik Encryption, Applying Artificial Intelligence, dan Decentralized and Context-aware Data Storage.

5. DAFTAR RUJUKAN

[1] Marufah, N., Rahmat, H.K. and Widana, I.D.K.K., 2020. Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7*(1), pp.191-201.

[2] Latifah, L. and Ritonga, I., 2020. Systematic Literature Review (SLR): Kompetensi Sumber Daya Insani Bagi Perkembangan Perbankan Syariah Di Indonesia. *Al Maal: Journal of Islamic Economics and Banking, 2*(1), pp.63-80.

[3] Ibrahim, W.N., Anuar, M.S., Selamat, A. and Krejcar, O., 2022. BOTNET DETECTION USING INDEPENDENT COMPONENT ANALYSIS. *IIUM Engineering Journal, 23*(1), pp.95-115.

[4] Wahyuni, N.K.A.T., Cahayani, P.P., Wicaksana, I.G.N.Y. and Wijayanti, I.A.K.B., 2023. ANALISIS KERENTANAN KEJAHATAN ONLINE PHISING MENGGUNAKAN TOOLS ZPHISHER, SHELLPHISH DAN WHPHISHER: Phising. *Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 3*(1), pp.23-31.

[5] Tekno Kompas, 2022. *Indonesia Hadapi 1,6 Miliar Serangan Siber dalam Setahun, Ini Malware Terbanyak.* [Online] (Update 08 Maret 2022) Available at : https://tekno.kompas.com/read/2022/04/08/06020007/indonesia-hadapi-1-6-miliar-serangan-siber-dalam-setahun-ini-malware-terbanyak?page=all [Accessed 27 Mei 2023]

[6] CNN Indonesia, 2023. *Mahasiswa Pembuat Aplikasi Undangan Nikah Sedot Rekening Ditangkap*. [Online] (Update 01 Februari 2023) Available at: https://www.cnnindonesia.com/nasional/20230201195555-12-907804/mahasiswa-pembuat-aplikasi-undangan-nikah-sedot-rekening-ditangkap [Accessed 28 Mei 2023]
[7] Kepner, J., Gadepally, V., Michaleas, P., Schear, N., Varia, M., Yerukhimovich, A. and Cunningham, R.K., 2014, September. Computing on masked data: a high performance method for improving big data veracity. In *2014 IEEE High Performance Extreme Computing Conference (HPEC)* (pp. 1-6). IEEE.
[8] Patil, T.B., Patnaik, G.K. and Bhole, A.T., 2017, January. Big data privacy using fully homomorphic non-deterministic encryption. In *2017 IEEE 7th International Advance Computing Conference (IACC)* (pp. 138-143). IEEE.
[9] Hidayati, S., & Gultom, R. A., 2020. ANALISIS KEBUTUHAN SENJATA SIBER DALAM MENINGKATAN PERTAHANAN INDONESIA DI ERA PEPERANGAN SIBER. *Teknologi Persenjataan*, 1(1).
[10] Faqih, M., & Priowirjanto, E. S., 2022. Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia. *Jurnal Indonesia Sosial Teknologi*, 3(11), 1156-1168.
[11] Lawrencya, S., & Dewi, M. D. P., 2021. KEJAHATAN SIBER SEBAGAI PENGHAMBAT E-COMMERCE DALAM PERKEMBANGAN INDUSTRI 4.0 BERDASARKAN NILAI BUDAYA INDONESIA. *Prosiding Serina*, 1(1), 277-286.
[12] Hadi, A., & Guntara, B., 2022. Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence). *Jurnal Hukum Mimbar Justitia*, 8(1), 233-253.
[13] Selma Dilek, Hüseyin Çakır and Mustafa Aydın., 2015. Application Of Artificial Intelligence Techniques To Combating Cyber Crimes : A Review. *International Journal of Artificial Intelligence & Applications (IJAIA)*, Vol. 6, No. 1
[14] AL-Dosari, K., Fetais, N. and Kucukvar, M., 2022. Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernetics and Systems*, pp.1-29.
[15] Mosteanu, N.R., 2020. Artificial intelligence and cyber security–face to face with cyber attack–a maltese case of risk management approach. *Ecoforum Journal*, 9(2).
[16] Jakka, G., Yathiraju, N. and Ansari, M.F., 2022. Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, 6(3), pp.6156-6165.
[17] Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L. and Pospelova, V., 2022. The emerging threat of ai-driven cyber attacks: A Review. *Applied Artificial Intelligence,* 36(1), p.2037254.
[18] Rahmatika, A.N., 2022. STRATEGI PERTAHANAN NEGARA INDONESIA DALAM MENGHADAPI ANCAMAN ARTIFICIAL INTELLIGENCE. *Peperangan Asimetris (PA)*, 8(1), pp.84-99.
[19] Li, J.H., 2018. Network security meets artificial intelligence: a review. *Frontiers of Information Technology & Electronic Engineering, 19*(12), pp.1462-1475.
[20] R. A. Gati, M. Rizki, and R. Y. Posumah, "Artificial Intelligence and Indonesia Government Cyber Security Strategies," *Academia.Edu*.
[21] I. Farid, A. H. Reksoprodjo, and Suhirwan, "Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber," *Nusant. J. Ilmu Pengetah. Sos.*, vol. 10, no. 2, pp. 779–788, 2020, doi: 10.31604/jips.v10i2.2023.779-788.

[22] Nadriana, L. and Sukmana, P., 2022. Exploring the Applicability of Common Law Principles in Combating Cybercrime in Indonesia: An Analysis of Current Legal Framework and Challenges. *International Journal of Cyber Criminology, 16*(2), pp.192-204.
[23] Parulian, S., Pratiwi, D.A. and Yustina, M.C., 2021. Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. T*elecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1*(2), pp.85-92.