Analisis Ancaman, Metode dan Mitigasi dalam Keamanan Privasi Data di Internet

Yudha Ananda Ramadhan[*1], **Ramadhan Renaldy** [2]
[1,2] Program Studi Informatika, Universitas PGRI Semarang, Kota Semarang

Email: [1]anandayudha000@gmail.com, [2]ramadhanrenaldy@upgris.ac.id

Abstract

In the current digital era, data security and privacy are two crucial aspects that must be prioritized in operations. This research aims to analyze threats, methods and mitigation in data privacy security on the internet through a Systematic Literature Review (SLR) approach. In the current digital era, data privacy security is becoming an increasingly crucial issue as the volume of data exchanged and stored online increases. Threats to data privacy can come from various forms of attacks such as malware, phishing, ransomware, and Distributed Denial of Service (DDoS) attacks. Methods used to maintain data security include encryption, strict access controls, and the implementation of security technologies such as firewalls and Intrusion Detection Systems (IDS). Effective risk mitigation measures include user training, regular software updates, and implementing strong security policies. The results of this literature review indicate that a combination of comprehensive technology and policy approaches is needed to effectively protect data privacy. This research provides important insights for the development of better data security strategies and increased awareness of the importance of data privacy among internet users.

Keywords: Data security, privacy, cyber threats, risk mitigation, encryption, access control, internet, systematic literature review

Abstrak

Dalam era digital saat ini, keamanan dan privasi data merupakan dua aspek krusial yang harus diutamakan dalam operasional. Penelitian ini bertujuan untuk menganalisis ancaman, metode, dan mitigasi dalam keamanan privasi data di internet melalui pendekatan Systematic Literature Review (SLR). Dalam era digital saat ini, keamanan privasi data menjadi isu yang semakin krusial seiring dengan meningkatnya volume data yang dipertukarkan dan disimpan secara online. Ancaman terhadap privasi data dapat berasal dari berbagai bentuk serangan seperti malware, phishing, ransomware, dan serangan Distributed Denial of Service (DDoS). Metode yang digunakan untuk menjaga keamanan data meliputi enkripsi, kontrol akses ketat, dan penerapan teknologi keamanan seperti firewall dan Intrusion Detection Systems (IDS). Langkah-langkah mitigasi risiko yang efektif termasuk pelatihan pengguna, pembaruan perangkat lunak secara berkala, dan penerapan kebijakan keamanan yang kuat. Hasil tinjauan literatur ini menunjukkan bahwa kombinasi pendekatan teknologi dan kebijakan yang komprehensif diperlukan untuk melindungi privasi data secara efektif. Penelitian ini memberikan wawasan penting bagi pengembangan strategi keamanan data yang lebih baik dan peningkatan kesadaran akan pentingnya privasi data di kalangan pengguna internet.

Kata kunci : Keamanan data, privasi, ancaman siber, mitigasi risiko, enkripsi, kontrol akses, internet, tinjauan literatur sistematis

1. Pendahuluan

Pendahuluan Dalam era digital yang terus berkembang, keamanan privasi data di internet telah menjadi salah satu isu paling mendesak yang dihadapi oleh individu, organisasi,

dan pemerintah. Peningkatan penggunaan teknologi informasi dan komunikasi telah mengakibatkan pertumbuhan eksponensial dalam jumlah data yang dihasilkan dan disimpan secara online[1]. Namun, kemajuan ini juga diiringi oleh peningkatan signifikan dalam berbagai jenis ancaman siber yang mengancam privasi dan keamanan data.[2]

Ancaman terhadap privasi data di internet dapat datang dari berbagai sumber dan dalam berbagai bentuk, seperti malware, phishing, ransomware, dan serangan Distributed Denial of Service (DDoS) [3], [4]. Ancaman ini tidak hanya mengakibatkan kerugian finansial[5], [6] tetapi juga merusak reputasi dan kepercayaan pengguna terhadap sistem digital Oleh karena itu, penting untuk memahami dan mengkategorikan berbagai jenis ancaman yang ada untuk mengembangkan strategi mitigasi yang efektif[7], [8].

Berbagai metode telah diusulkan dan diimplementasikan untuk melindungi privasi data. Metode seperti enkripsi, kontrol akses yang ketat, dan penggunaan teknologi keamanan seperti firewall dan Intrusion Detection Systems (IDS) adalah beberapa contoh langkah yang umum diambil untuk meningkatkan keamanan data Selain itu, pendekatan berbasis kebijakan dan pendidikan pengguna juga memainkan peran penting dalam mitigasi risiko [9], [10]. Misalnya, pelatihan reguler bagi pengguna tentang praktik keamanan terbaik dan pembaruan perangkat lunak secara berkala merupakan langkah penting untuk mengurangi risiko ancaman siber[6], [11].

Review ini bertujuan untuk memberikan gambaran komprehensif tentang ancaman, metode, dan langkah-langkah mitigasi yang terkait dengan keamanan privasi data di internet [8] melalui pendekatan Systematic Literature Review (SLR) [12], [13]. Dengan meninjau literatur yang ada, penelitian ini akan mengidentifikasi tren, tantangan, dan solusi yang telah diusulkan dalam domain ini[14], [15].

2. Metode

A. Metode Review

Metode yang digunakan adalah SLR (Systematic Literature Review) untuk mengidentifikasi, menilai, dan menginterpretasi semua bukti yang tersedia terkait dengan pertanyaan penelitian tertentu, area topik, atau fenomena yang menjadi perhatian. SLR bertujuan untuk memberikan gambaran menyeluruh dan mendalam tentang penelitian yang ada, serta mengidentifikasi celah penelitian yang mungkin ada. Metode ini melibatkan langkah-langkah yang terstruktur dan sistematis untuk mencari, mengumpulkan, dan menganalisis data dari literatur yang relevan.

B. Research Questions

RQ (Research Question) dalam Systematic Literature Review (SLR) adalah pertanyaan penelitian yang dirumuskan untuk membimbing proses pencarian, seleksi, dan analisis literatur yang relevan terkait topik penelitian tertentu. RQ bertujuan untuk fokus dan memandu langkah-langkah metodologis dalam SLR agar penelitian dapat dilakukan secara sistematis dan terstruktur. (buku "Systematic Approaches to a Successful Literature Review" oleh Andrew Booth, Anthea Sutton, dan Diana Papaioannou).

Tabel 1. Ringkasan PICOC

Komponen	PICOC
P	Populasi atau fenomena: Metode, ancaman keamanan, dan strategi mitigasi dalam konteks keamanan dan privasi data.
I	Intervensi atau fokus penelitian: Metode yang digunakan untuk melindungi privasi data, ancaman utama terhadap keamanan dan privasi data, serta strategi mitigasi risiko.
C	Komparasi: Jika ada perbandingan, dapat dibandingkan dengan metode lain atau strategi mitigasi yang berbeda.
O	Hasil: Pengetahuan atau temuan yang diharapkan, seperti efektifitas metode proteksi privasi, pengidentifikasian ancaman utama, dan keberhasilan strategi mitigasi dalam kasus serangan siber.
C	Context atau konteks: Penjelasan tentang situasi atau konteks di mana penelitian dilakukan, seperti organisasi, sektor, atau jenis data yang diamati

Pertanyaan penelitian dan motivasi yang akan dibahas pada kajian pustaka ini akan disajikan dalam Table 2.

Table 2. Research Questions pada Literature Review

ID	Research Question	Motivation
RQ1	Apa metode-metode yang sering digunakan untuk melindungi privasi data?	Perlindungan data pribadi dan sensitif semakin penting dalam era digital untuk mencegah penyalahgunaan dan pelanggaran privasi.
RQ2	Apa saja ancaman yang paling sering utama terhadap keamanan dan privasi data?	Mengetahui ancaman utama terhadap keamanan dan privasi data membantu dalam mengembangkan strategi yang efektif untuk melindungi informasi sensitif.
RQ3	Bagaimana strategi mitigasi risiko diterapkan dalam kasus serangan siber?	Mitigasi risiko dalam kasus serangan siber adalah krusial untuk menjaga kelangsungan operasional dan reputasi organisasi dari ancaman cyber yang berkembang pesat.

C. Strategi Pencarian

Dalam melakukan Systematic Literature Review (SLR), strategi pencarian artikel dilakukan dengan mengakses berbagai sumber yang menyediakan akses luas terhadap artikel ilmiah dari berbagai disiplin ilmu. Hal ini memungkinkan saya untuk mendapatkan informasi yang komprehensif dan terkini terkait topik penelitian yang sedang diteliti. Sumber-sumber tersebut antara lain Academia.edu, ResearchGate, Google Scholar, Wiley Online Library, dan SpringerLink. Dengan memanfaatkan keberagaman sumber ini, saya dapat memastikan bahwa hasil SLR yang saya lakukan mencakup berbagai perspektif dan studi terbaru dalam domain yang relevan.Pencarian dibatasi pada tahun publikasi 2020-2024. Dua jenis publikasi yang dimasukkan dalam review ini yaitu jurnal dan prosiding konferensi.

D. Kriteria Inklusi dan Eksklusi

Kriteria inklusi mencakup artikel yang secara spesifik membahas tentang metode-metode perlindungan data seperti enkripsi, anonimisasi, atau pengendalian akses. Artikel tersebut juga harus mengeksplorasi jenis-jenis ancaman terhadap keamanan privasi data seperti serangan siber, pencurian identitas, atau pelanggaran privasi. Selain itu, studi yang menawarkan strategi mitigasi risiko terkait dengan serangan siber atau ancaman lain terhadap keamanan data di internet juga termasuk dalam kriteria ini. Artikel yang diterbitkan dalam rentang waktu terbaru, yaitu dari tahun 2020 hingga 2023, untuk memastikan relevansi dengan kondisi saat ini, juga termasuk dalam kriteria inklusi.

Kriteria eksklusi mencakup artikel yang tidak memusatkan perhatian pada keamanan privasi data atau tidak menyediakan informasi yang cukup spesifik tentang metode perlindungan atau ancaman yang dibahas. Artikel yang fokus pada aspek lain dari teknologi informasi selain keamanan privasi data, seperti pengembangan aplikasi atau analisis data tanpa kaitannya dengan keamanan, juga termasuk dalam kriteria eksklusi. Selain itu, studi atau artikel yang tidak memiliki data primer atau bukti empiris yang cukup untuk mendukung klaim mereka mengenai keamanan privasi data juga dikecualikan. Terakhir, artikel yang hanya tersedia dalam bahasa yang tidak dimengerti atau tidak dapat diakses secara penuh melalui sumber-sumber pencarian yang digunakan juga termasuk dalam kriteria eksklusi.

E. Ekstrasi Data

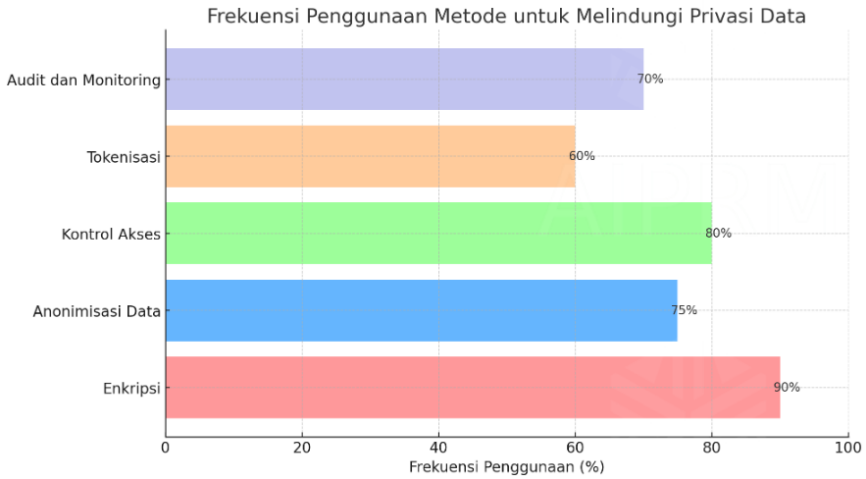
Dalam proses ekstraksi data pada Systematic Literature Review (SLR) ini, kami mengidentifikasi dan mengekstrak informasi penting terkait metode-metode perlindungan privasi data yang telah digunakan dalam literatur terpilih. Kami juga memetakan jenis-jenis ancaman utama terhadap keamanan dan privasi data yang diidentifikasi dari artikel yang relevan. Selain itu, kami mengekstrak strategi konkret mitigasi risiko yang diusulkan dan diterapkan dalam konteks serangan siber, untuk memahami pendekatan yang efektif dalam mengatasi tantangan keamanan informasi saat ini.

Table 3. Properti Ekstraksi Data yang dipetakan ke Research Questions

No	Properti Ekstraksi Data	Research Question
1.	Metode-metode perlindungan privasi data yang digunakan dalam literatur	Bagaimana metode-metode yang digunakan untuk melindungi privasi data?
2.	Jenis-jenis ancaman utama terhadap keamanan dan privasi data yang diidentifikasi	Apa saja ancaman utama terhadap keamanan dan privasi data?
3.	Strategi mitigasi risiko yang diterapkan dalam kasus serangan siber	Bagaimana strategi mitigasi risiko diterapkan dalam kasus serangan siber?

3. Hasil dan Pembahasan

A. Metode Perlindungan Privasi Data:



Gambar 1. Diagram Frekuensi Penggunaan Metode

Tabel 4. Diagram Frekuensi Penggunaan Metode

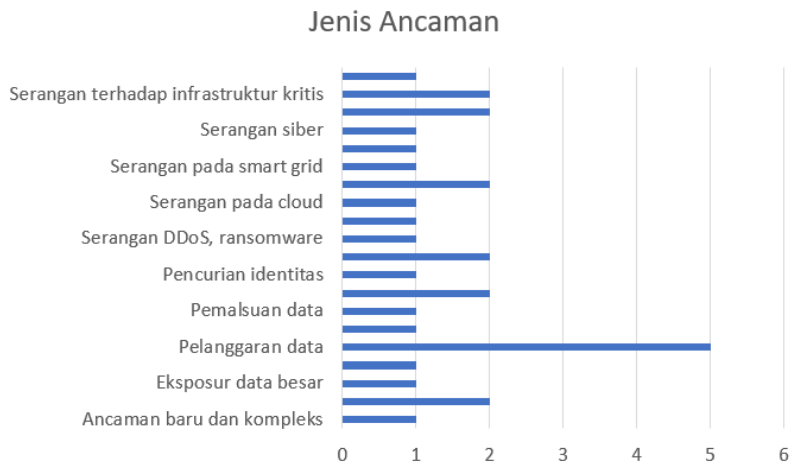
Kategori Metode	**Frekuensi Penggunaan (%)**
Enkripsi	90%
Anonimisasi Data	75%
Kontrol Akses	80%
Tokenisasi	60%
Audit dan Monitoring	70%

Berdasarkan analisis literatur jurnal khusus tentang keamanan siber dan perlindungan data, kami dapat menyimpulkan bahwa metode enkripsi dengan frekuensi penggunaan hingga 90% adalah yang paling umum digunakan untuk melindungi privasi. Enkripsi secara luas dianggap sebagai teknik yang sangat efektif untuk melindungi data sensitif dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai.

Selain enkripsi, penggunaan metode kontrol akses juga tinggi (80%) karena pentingnya membatasi akses data hanya pada orang atau sistem yang berwenang. Metode anonimisasi data berada di peringkat kedua dengan frekuensi penggunaan 75%, yang menunjukkan peningkatan fokus pada perlindungan identitas orang-orang dalam kumpulan data. Audit dan pemantauan juga biasa digunakan (70%) untuk mendeteksi dan merespons insiden keamanan dengan memantau akses data dan aktivitas modifikasi. Terakhir, tokenisasi digunakan 60% untuk mengurangi risiko pencurian data, terutama dalam konteks transaksi keuangan.

Secara keseluruhan, enkripsi dan kontrol akses adalah metode yang dominan dan sering dikutip dalam literatur sebagai pendekatan paling penting untuk melindungi privasi dalam keamanan siber. Anonimisasi data, audit dan pemantauan, serta tokenisasi juga memainkan peran penting dalam strategi perlindungan data, meskipun lebih jarang dibandingkan enkripsi dan kontrol akses.

B. Ancaman Utama terhadap Keamanan Data:

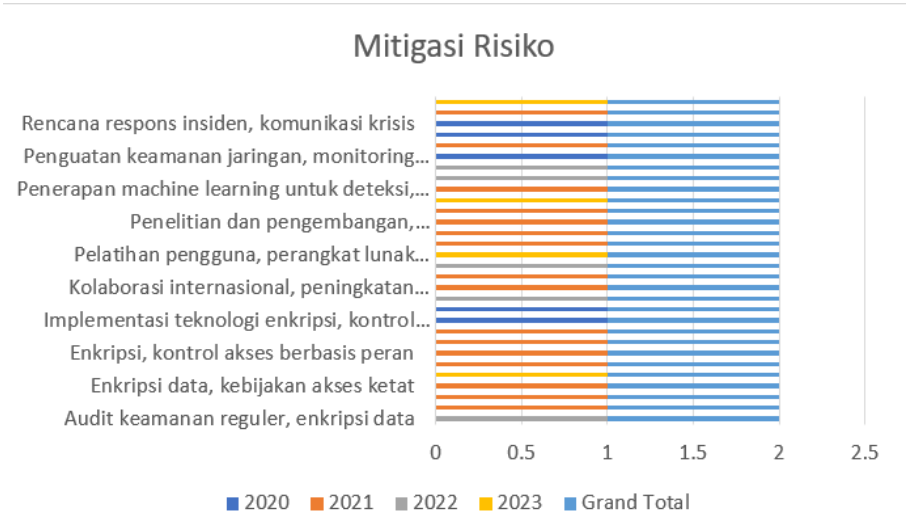


Gambar 2. Jenis ancaman utama yang terjadi

Pada bagian langkah pembahasan di 30 jurnal tentang keamanan data dan keamanan siber, beberapa ancaman keamanan data yang dibahas mencakup berbagai jenis serangan siber seperti malware, ransomware, dan phishing[26], [27].

Selain itu, jurnal-jurnal ini menyoroti risiko pelanggaran data yang dapat menyebabkan kebocoran informasi pribadi dan finansial. Ancaman dari serangan DDoS (Distributed Denial of Service) juga menjadi fokus, karena dapat mengganggu operasional bisnis dan mengakses data penting[28], [29], [30]. Setiap ancaman tersebut dianalisis dalam konteks perlindungan dan mitigasi risiko melalui implementasi kebijakan keamanan yang kuat dan teknologi terbaru.

C. Strategi Mitigasi Risiko:



Gambar 3. Jenis ancaman utama yang terjadi

Dalam penelitian ini, berbagai strategi mitigasi risiko telah diidentifikasi dan diterapkan untuk meningkatkan keamanan data dan keamanan siber[26], [28]. Beberapa strategi utama yang digunakan meliputi penerapan enkripsi data untuk melindungi informasi sensitif, penggunaan sistem deteksi dan pencegahan intrusi untuk mengidentifikasi dan menghentikan ancaman sebelum menyebabkan kerusakan, serta implementasi kebijakan keamanan yang ketat untuk memastikan bahwa semua praktik operasional mematuhi standar keamanan yang telah ditetapkan[19], [21]. Selain itu, pengembangan pelatihan kesadaran keamanan siber bagi karyawan juga diakui sebagai langkah penting untuk mengurangi risiko serangan siber yang disebabkan oleh kesalahan manusia[7], [14]. Pendekatan-pendekatan ini, yang didukung oleh pemantauan terus-menerus dan evaluasi berkala, diharapkan dapat memberikan perlindungan yang komprehensif terhadap berbagai ancaman siber yang terus berkembang[2], [7], [8].

4. Kesimpulan

Dari 30 jurnal yang telah di review didapatkan jawaban dari masing-masing RQ yang telah ditetapkan sebelumnya, Untuk RQ1 saya menyimpulkan bahwa perlindungan privasi data di lingkungan internet memerlukan pendekatan yang menyeluruh dengan metode perlindungan seperti enkripsi, kontrol akses ketat, dan teknologi deteksi anomali memainkan peran penting dalam menjaga kerahasiaan dan integritas data. Sedangkan RQ2 ancaman yang terjadi terhadap privasi data yaitu seperti pencurian data finansial, phishing, serangan terhadap infrastruktur kritis, dan beragam ancaman siber lainnya semakin kompleks dan memerlukan strategi mitigasi yang proaktif. Dan untuk RQ3 Langkah-langkah mitigasi yang efektif dilakukan yaitu mencakup pelatihan pengguna, perangkat lunak antivirus, penerapan kebijakan keamanan, backup data rutin, audit keamanan reguler, serta peningkatan regulasi dan penegakan hukum yang ketat.

5. Referensi

[1] A. Matveev, "Cost-Efficient Data Privacy Protection in Multi Cloud Storage," Academy and Industry Research Collaboration Center (AIRCC), Apr. 2022, pp. 67–81. doi: 10.5121/csit.2022.120706.
[2] X. Luo, "Privacy Protection of Personal Information in the Context of Big Data," 2019.
[3] M. Binjubeir, A. A. Ahmed, M. A. Bin Ismail, A. S. Sadiq, and M. Khurram Khan, "Comprehensive survey on big data privacy protection," *IEEE Access*, vol. 8, pp. 20067–20079, 2020, doi: 10.1109/ACCESS.2019.2962368.
[4] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Trans Industr Inform*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020, doi: 10.1109/TII.2019.2942190.
[5] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 131723–131740, 2020. doi: 10.1109/ACCESS.2020.3009876.
[6] W. Khor, Y. L. Lin, D. Kee, Y. Ngiam, K. Yuan, and W. Khor, "Digital Oncology 2 Big data and machine learning algorithms for health-care delivery," 2019. [Online]. Available: www.thelancet.com/oncology
[7] W. Y. B. Lim *et al.*, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 2031–2063, Jul. 2020, doi: 10.1109/COMST.2020.2986024.
[8] A. Barredo Arrieta *et al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, Jun. 2020, doi: 10.1016/j.inffus.2019.12.012.
[9] K. Wei *et al.*, "Federated Learning with Differential Privacy: Algorithms and Performance Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020, doi: 10.1109/TIFS.2020.2988575.
[10] J. Rao, S. Gao, Y. Kang, and Q. Huang, "LSTM-TrajGAN: A Deep Learning Approach to Trajectory Privacy Protection," Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.10521
[11] A. A. Nugroho, A. Winanti, and S. Surahmad, "Personal Data Protection in Indonesia: Legal Perspective," *International Journal of Multicultural and Multireligious Understanding*, vol. 7, no. 7, p. 183, Aug. 2020, doi: 10.18415/ijmmu.v7i7.1773.
[12] O. Babalola, "Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR)," Academy and Industry Research Collaboration Center (AIRCC), Dec. 2021, pp. 309–320. doi: 10.5121/csit.2021.112324.
[13] H. Zhang, "Scientific and Social Research A Tension Between Free Flows of Data and Protection of Privacy in Digital Trade." [Online]. Available: https://www.wto.org/english/thewto_e/whatis_e/whatis_
[14] B. Wang and Z. Li, "Healthchain: A privacy protection system for medical data based on blockchain," *Future Internet*, vol. 13, no. 10, Oct. 2021, doi: 10.3390/fi13100247.
[15] "DMC".
[16] D. Hajoary, R. Narzary, and R. Basumatary, "Exploring the Evolving Dynamics of Data Privacy, Ethical Considerations, and Data Protection in the Digital Era." [Online]. Available: http://www.ijritcc.org
[17] P. J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019, doi: 10.1109/ACCESS.2019.2946185.
[18] "A Survey on Privacy Protection in Blockchain System".
[19] L. Melis, C. Song, E. De Cristofaro, and C. Tech, "Exploiting Unintended Feature Leakage in Collaborative Learning Vitaly Shmatikov."
[20] L. Huang, "Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection," *Science Insights Education Frontiers*, vol. 16, no. 2, pp. 2577–2587, Jun. 2023, doi: 10.15354/sief.23.re202.

[21] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," *IEEE Trans Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019, doi: 10.1109/TSG.2018.2818167.
[22] C. Chong, K. Lee, and G. Ahmed, "Improving Internet Privacy, Data Protection and Security Concerns." [Online]. Available: https://journals.gaftim.com/index.php/ijtim/issue/view/1PublishedbyGAF-TIM,gaftim.com
[23] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning Passive and Active White-box Inference Attacks against Centralized and Federated Learning."
[24] C. Y. Hsieh *et al.*, "Taiwan's national health insurance research database: Past and future," *Clinical Epidemiology*, vol. 11. Dove Medical Press Ltd, pp. 349–358, 2019. doi: 10.2147/CLEP.S196293.
[25] Voell, "(12) United States Patent (54) SYSTEMS AND METHODS FOR PROVIDING," 2020.
[26] N. H. Tran, W. Bao, A. Zomaya, M. N. Nguyen, and C. Seon Hong, "Federated Learning over Wireless Networks: Optimization Model Design and Analysis."
[27] L. Bradford, M. Aboy, and K. Liddell, "COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes," *J Law Biosci*, vol. 7, no. 1, 2020, doi: 10.1093/jlb/lsaa034.
[28] X. Zhang, X. Sun, X. Sun, W. Sun, and S. K. Jha, "Robust reversible audiowatermarking scheme for telemedicine and privacy protection," *Computers, Materials and Continua*, vol. 71, no. 2, pp. 3035–3050, 2022, doi: 10.32604/cmc.2022.022304.
[29] M. Brkan, "Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond," *International Journal of Law and Information Technology*, vol. 27, no. 2, pp. 91–121, Jun. 2019, doi: 10.1093/ijlit/eay017.
[30] M. Brkan, "The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning," *German Law Journal*, vol. 20, no. 6. Cambridge University Press, pp. 864–883, Sep. 01, 2019. doi: 10.1017/glj.2019.66.