TECHNOMEDIA : Informatics and Computer Science, Vol. 2 No. 2, Juli 2025, 72 - 79
e-ISSN: 3047-2180 | DOI: 10.58641

TINJAUAN PUSTAKA SISTEMATIS TENTANG TEKNOLOGI KEAMANAN DATA: TREN DAN TANTANGAN

[1)]Muhamad Fuat Asnawi, [2)] Nur Fitriyanto, [3)] M. Agoeng Pamoengkas
[1)]Universitas Sains Al-Qur'an
[2,3)] Mahasiswa Pascasarjana Universitas Amikom Yogyakarta
fuatasnawi@unsiq.ac.id

INFO ARTIKEL

Riwayat Artikel :
Diterima : 19 Juli 2025
Disetujui : 31 Juli 2025

Kata Kunci :
Keamanan data, enkripsi, kecerdasan buatan, cloud computing, GDPR.

ABSTRAK

Penelitian ini merupakan tinjauan pustaka sistematis (Systematic Literature Review/SLR) yang bertujuan mengidentifikasi tren dan tantangan utama dalam teknologi keamanan data selama periode 2020–2025. Sebanyak 91 artikel dari basis data IEEE Xplore dan ScienceDirect telah dikaji secara mendalam dengan fokus pada inovasi teknologi enkripsi, penerapan kecerdasan buatan (AI) dan machine learning dalam keamanan data, serta tantangan dalam perlindungan data pribadi di lingkungan cloud computing dan Internet of Things (IoT). Hasil kajian menunjukkan bahwa tren utama teknologi keamanan data meliputi adopsi Advanced Encryption Standard (AES), homomorphic encryption, searchable encryption, hingga enkripsi berbasis blockchain, serta integrasi AI untuk deteksi dan mitigasi ancaman secara proaktif. Meskipun demikian, penelitian ini juga menyoroti tantangan besar berupa keamanan data pribadi, kompleksitas pengelolaan data di cloud, serta implementasi regulasi seperti GDPR yang masih menghadapi berbagai kendala teknis dan hukum. Studi ini memberikan kontribusi penting dengan memetakan perkembangan terbaru sekaligus mengidentifikasi gap riset yang relevan untuk penguatan keamanan data di masa mendatang.

ARTICLE INFO

Article History :
Received : Jul 19, 2025
Accepted : Jul 31, 2025

Keywords:
Data security, encryption, artificial intelligence, cloud computing, GDPR

ABSTRACT

This study is a systematic literature review (SLR) aimed at identifying key trends and challenges in data security technologies during the period 2020–2025. A total of 91 articles from the IEEE Xplore and ScienceDirect databases were thoroughly reviewed, focusing on innovations in encryption technologies, the application of artificial intelligence (AI) and machine learning in data security, as well as challenges in protecting personal data in cloud computing and the Internet of Things (IoT) environments. The findings reveal that key trends in data security technologies include the adoption of Advanced Encryption Standard (AES), homomorphic encryption, searchable encryption, blockchain-based encryption, and the integration of AI for proactive threat detection and mitigation. However, the study also highlights significant challenges, such as personal data security, the complexity of data management in the cloud, and the implementation of regulations like GDPR, which still face various technical and legal barriers. This study provides an important contribution by mapping the latest developments and identifying research gaps relevant for strengthening data security in the future.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah menghadirkan tantangan baru dalam melindungi data dari ancaman keamanan siber. Data menjadi aset berharga yang rentan terhadap berbagai serangan seperti pencurian, manipulasi, dan penyalahgunaan data pribadi (Li and Saxunová 2020). Seiring dengan peningkatan penggunaan teknologi digital seperti komputasi awan, Internet of Things (IoT), dan kecerdasan buatan (AI), kebutuhan akan perlindungan data yang kuat dan efektif semakin mendesak (Isaac Abiodun et al. 2022; Miller, Lukic, and Skiera 2025; Rawat, Doku, and Garuba 2021).

Teknologi keamanan data berkembang secara signifikan dengan munculnya pendekatan baru seperti enkripsi canggih, autentikasi multifaktor, blockchain, dan metode keamanan berbasis AI (Isaac Abiodun et al. 2022; Li et al. 2024; Miller et al. 2025; Niu et al. 2020; Wang et al. 2023). Blockchain, misalnya, memberikan jaminan integritas data melalui pencatatan transaksi yang transparan dan aman, menjadikannya pilihan populer dalam berbagai aplikasi keamanan data . Demikian pula, penggunaan AI dan machine learning mampu mendeteksi ancaman secara real-time serta meningkatkan ketahanan terhadap serangan siber (Awaysheh et al. 2022; Feng et al. 2024; Miller et al. 2025).

Namun, meskipun teknologi tersebut berkembang pesat, tantangan utama seperti kompleksitas penerapan regulasi privasi seperti General Data Protection Regulation (GDPR), ancaman keamanan cloud computing dan IoT masih menjadi hambatan yang serius (Azam et al. 2023; Guaman, Del Alamo, and Caiza 2021; Miller et al. 2025; Wang et al. 2023). Studi menunjukkan bahwa GDPR mampu menekan jumlah pelacak online secara signifikan, tetapi memiliki dampak yang terbatas pada jenis pelacak tertentu seperti pelacak iklan dan analitik (Azam et al. 2023; Cejas et al. 2023; Miller et al. 2025).

Selain itu, penggunaan teknologi cloud computing menghadapi tantangan serius dalam aspek forensik digital dan provenance data (Dai et al. 2020; Dou et al. 2024; Isaac Abiodun et al. 2022). Menurut Abiodun et al. (2022), data provenance menjadi krusial dalam investigasi forensik karena memungkinkan pelacakan asal-usul data, meskipun implementasinya di lingkungan cloud masih menemui kendala seperti kompleksitas bukti digital dan tantangan pengelolaan data volatile (Isaac Abiodun et al. 2022).

Penelitian ini bertujuan untuk melakukan tinjauan pustaka sistematis terhadap tren dan tantangan dalam teknologi keamanan data. Secara spesifik, penelitian ini ingin mengidentifikasi tren terbaru dalam teknologi enkripsi dan kontribusi kecerdasan buatan dalam keamanan data, serta memahami tantangan utama dalam perlindungan data di cloud computing, IoT, serta penerapan regulasi perlindungan data seperti GDPR. Hasil dari penelitian ini diharapkan dapat memberikan wawasan komprehensif kepada praktisi dan akademisi mengenai perkembangan serta tantangan terkini dalam teknologi keamanan data.

Penelitian ini memberikan pemahaman mendalam terkait kemajuan teknologi keamanan data, serta menjadi acuan bagi pengambil kebijakan dalam merancang strategi keamanan siber yang efektif. Di samping itu, hasil penelitian ini juga diharapkan bisa membantu organisasi dalam mengidentifikasi area yang membutuhkan perhatian lebih dalam hal kepatuhan regulasi dan pengamanan data sensitif.

Tinjauan pustaka dari penelitian sebelumnya menunjukkan bahwa perkembangan teknologi keamanan data sangat dipengaruhi oleh kemajuan teknologi enkripsi, AI, blockchain, dan regulasi seperti GDPR. Menurut Miller et al. (2025), GDPR telah berhasil mengurangi penggunaan pelacak online invasif hingga 14,79%, namun masih menunjukkan keterbatasan dalam mengatasi pelacak kategori tertentu. Studi lain oleh Li (2025) menyoroti pentingnya teknologi enkripsi dalam mengatasi ancaman keamanan data, khususnya dalam lingkungan jaringan komputer.

Abiodun et al. (2022) menjelaskan pentingnya provenance data dalam forensik digital di lingkungan cloud computing. Tantangan utama yang diidentifikasi adalah kompleksitas pengumpulan bukti digital serta volatilitas data yang memerlukan pendekatan khusus agar data tidak hilang sebelum sempat dianalisis. Sementara itu, Li dan Saxunová

(2020) menyatakan bahwa regulasi GDPR secara signifikan meningkatkan kesadaran global terhadap perlindungan data pribadi, tetapi implementasinya masih menghadapi kendala teknis dan hukum yang serius.

Penelitian ini memberikan pembaruan dalam beberapa aspek. Pertama, kajian ini secara khusus mengeksplorasi perkembangan teknologi terbaru seperti enkripsi modern, blockchain, dan metode berbasis AI dalam konteks keamanan data. Kedua, penelitian ini menyoroti secara mendalam tantangan teknis dan regulasi yang dihadapi organisasi, khususnya terkait dengan implementasi GDPR di lingkungan teknologi baru seperti cloud computing dan IoT. Ketiga, studi ini menawarkan perspektif integratif yang mencakup pendekatan teknologi dan regulasi dalam satu kerangka analisis yang komprehensif.

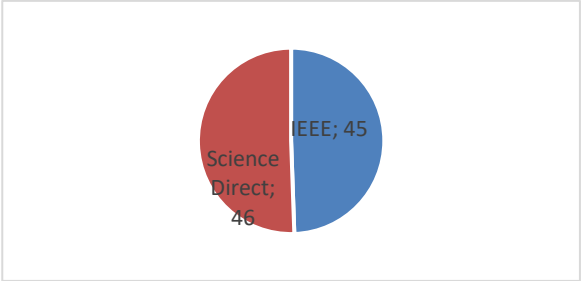
2. METODE

Penelitian ini menggunakan metode Tinjauan Pustaka Sistematis (Systematic Literature Review/SLR) yang bertujuan untuk mengidentifikasi dan menganalisis tren serta tantangan dalam teknologi keamanan data (Alouffi et al. 2021; Bliznak, Munk, and Pilkova 2024; Ghebreselassie, Hammen, and Hustad 2025). SLR ini dilakukan dengan mengkaji 91 artikel yang diperoleh dari sumber-sumber bereputasi, yaitu IEEE Xplore dan ScienceDirect.

a. Strategi Pencarian

Strategi penelusuran literatur pada penelitian ini melibatkan beberapa langkah sistematis seperti ditunjukkan pada Gambar 1. Basis data yang digunakan meliputi IEEE Xplore, dan ScienceDirect. Kata kunci yang digunakan dalam penelusuran adalah: 'Data Security Technologies', 'Recent trends in data encryption', 'Modern encryption techniques', 'Data encryption trends in cybersecurity', 'Artificial intelligence in data security', 'AI for encryption and data security', 'Challenges in cloud data security', 'Data protection challenges in IoT', 'Data protection regulations', dan 'Global data privacy laws'. Proses dimulai dengan identifikasi kata kunci utama, kemudian digunakan berbagai kombinasi kata kunci tersebut untuk menelusuri artikel yang relevan. Hasil pencarian kemudian disaring berdasarkan relevansi dan periode publikasi tahun 2020–2025. Artikel yang memenuhi kriteria inklusi dikumpulkan dan diunduh teks lengkapnya untuk dianalisis lebih lanjut. Gambar 1 menunjukkan tahapan strategi penelusuran, sedangkan Gambar 2 menampilkan distribusi artikel akhir berdasarkan database asal.

Gambar 1. Tahapan Strategi Penelusuran



Gambar 2. Distribusi artikel terpilih berdasarkan basis data

b. Pertanyaan Penelitian

Untuk memandu dan memfokuskan tinjauan ini, pertanyaan penelitian berikut akan digunakan:

1) Tren dalam Teknologi Keamanan Data
   RQ1: Apa tren terbaru dalam penerapan teknologi enkripsi untuk melindungi data di era digital?
   RQ2: Bagaimana kecerdasan buatan (AI) dan Machine Learning berkontribusi dalam pengembangan teknologi keamanan data?
2) Tantangan dalam Keamanan Data
   RQ3: Apa tantangan utama dalam mengamankan data pribadi dan sensitif di lingkungan cloud computing dan IoT?
   RQ4: Apa saja tantangan regulasi yang dihadapi dalam penerapan standar perlindungan data global?

3. HASIL DAN PEMBAHASAN

a. Tren dalam Teknologi Keamanan Data

1) Teknologi Enkripsi data

Perkembangan teknologi enkripsi terus menjadi salah satu tren utama dalam keamanan data modern. Enkripsi tingkat lanjut seperti Advanced Encryption Standard (AES) tetap banyak diadopsi karena kekuatan algoritmanya yang terbukti mampu melindungi data sensitif (Bilal et al. 2025). Penelitian terkini juga menunjukkan tren penggunaan metode homomorphic encryption dan searchable encryption untuk mendukung komputasi awan dan IoT agar data tetap terenkripsi meskipun sedang diproses (Alsadie 2024; Harbi et al. 2021). Selain itu, pendekatan enkripsi berbasis blockchain juga dikembangkan untuk menjaga integritas data dalam transaksi digital (Ullah et al. 2024). Taherdoost (2025) menekankan bahwa kombinasi teknik enkripsi dengan kebijakan akses granular memberikan perlindungan yang lebih adaptif terhadap ancaman siber (Popoola et al. 2024; Taherdoost, Le, and Slimani 2025).

Tabel 1. Tren Teknologi Enkripsi

Jenis Teknologi Enkripsi	Sumber Artikel	Tren Penggunaan Terbanyak
Advanced Encryption Standard (AES)	(Bilal et al. 2025; Gupta et al. 2022; Harbi et al. 2021; Zafir et al. 2024)	Enkripsi file, komunikasi jaringan, keamanan database dan transaksi daring.
Homomorphic Encryption	(Harbi et al. 2021; Khan et al. 2021; Tsouvalas et al. 2025; Zafir et al. 2024)	Komputasi aman pada data terenkripsi dalam layanan cloud computing dan IoT.
Searchable Encryption	(Alsadie 2024; Omote et al. 2024)	Cloud storage yang memungkinkan pencarian data terenkripsi tanpa dekripsi terlebih dahulu.
Blockchain-based Encryption	(Niu et al. 2020; Ullah et al. 2024)	Perlindungan data sensitif, transaksi digital, dan kontrak pintar yang terdistribusi untuk memastikan integritas data.
Identity-based Encryption	(Popoola et al. 2024; Wu et al. 2023)	Kontrol akses berbasis identitas pengguna, banyak digunakan untuk autentikasi dalam skenario komputasi awan dan IoT.

Tabel 1. menampilkan tren penggunaan teknologi enkripsi data berdasarkan hasil tinjauan pustaka dari berbagai literatur. Advanced Encryption Standard (AES) menjadi teknologi enkripsi paling populer, digunakan untuk mengamankan file, komunikasi jaringan, database, serta transaksi daring (Zafir et al. 2024). Homomorphic Encryption juga meningkat penggunaannya dalam layanan cloud dan IoT karena memungkinkan pemrosesan data terenkripsi tanpa dekripsi langsung (Harbi et al. 2021; Zafir et al. 2024). Searchable Encryption umum diterapkan dalam penyimpanan cloud untuk pencarian data terenkripsi yang efisien (Alsadie 2024). Teknologi Blockchain-based Encryption digunakan luas dalam transaksi digital dan perlindungan data sensitif untuk memastikan integritas data (Ullah et al. 2024). Identity-based Encryption populer dalam kontrol akses berbasis identitas pengguna, terutama di komputasi awan dan IoT (Popoola et al. 2024).

2) Peran AI dan Machine Learning

Penerapan kecerdasan buatan (AI) dan pembelajaran mesin (ML) juga menjadi tren penting dalam teknologi keamanan data. AI digunakan untuk mendeteksi pola anomali secara real-time sehingga mampu memprediksi dan mencegah serangan siber (Miller et al. 2025) (Miller, Lukic, & Skiera, 2025). Menurut Abdi et al. (2024), sistem deteksi intrusi berbasis AI dapat belajar dari data serangan sebelumnya sehingga keakuratannya meningkat seiring waktu (Abdi et al. 2024). Penelitian oleh Abiodun et al. (2022) juga menunjukkan potensi AI dalam mendukung forensik digital dengan menganalisis provenance data secara otomatis di lingkungan cloud computing (Isaac Abiodun et al. 2022).

b. Tantangan dalam Keamanan Data

1) Tantangan Pengamanan data pribadi

Salah satu tantangan signifikan adalah pengamanan data pribadi pengguna, terutama di era big data dan IoT. Studi menunjukkan bahwa data pribadi semakin mudah dieksploitasi melalui kebocoran data yang sulit terdeteksi (Li and Saxunová 2020). Di lingkungan cloud, tantangan utamanya adalah bagaimana mengelola data volatile agar tetap dapat dilacak sumbernya untuk kepentingan forensic (Lingga et al. 2024; Marwan et al. 2024; Salih and Jasim Mohammad 2024; Zhang et al. 2022). Selain itu, pengguna IoT seringkali tidak memiliki kontrol penuh atas bagaimana data mereka dikumpulkan dan diproses, sehingga meningkatkan risiko kebocoran informasi sensitif (Adam et al. 2024; Karim et al. 2024; Qureshi et al. 2025; Rai et al. 2024).

2) Tantangan Regulasi penerapan standar perlindungan data

Dari sisi regulasi, implementasi standar perlindungan data seperti GDPR masih menghadapi berbagai kendala teknis dan hukum. Miller, Lukic, & Skiera (2025) mengungkapkan bahwa meskipun GDPR berhasil menurunkan jumlah pelacak online invasif (Miller et al. 2025), tetapi efektivitasnya masih terbatas untuk kategori pelacak tertentu. Hal ini menunjukkan perlunya adaptasi regulasi dengan dinamika teknologi baru (Alves et al. 2023; Guaman et al. 2021; Han and Park 2022; Yang et al. 2024; Zhang et al. 2024). Menurut Li dan Saxunová (2020), sinkronisasi kebijakan privasi lintas negara juga menjadi tantangan karena perbedaan kebijakan perlindungan data dapat menimbulkan celah keamanan dalam pertukaran data global (Li and Saxunová 2020).

4. PENUTUP

4.1. Kesimpulan

Berdasarkan hasil tinjauan pustaka sistematis terhadap 91 artikel dari tahun 2020–2025, dapat disimpulkan bahwa perkembangan teknologi keamanan data semakin kompleks seiring pesatnya adopsi teknologi digital seperti cloud computing, IoT, dan kecerdasan buatan. Tren utama yang ditemukan adalah penggunaan enkripsi tingkat lanjut, penerapan AI dan machine learning dalam deteksi ancaman, serta pemanfaatan blockchain untuk menjaga integritas data digital. Namun, tantangan besar masih dihadapi, terutama dalam pengamanan data pribadi, manajemen data di lingkungan cloud dan IoT, serta penerapan regulasi perlindungan data seperti GDPR yang memerlukan adaptasi terus-menerus seiring perkembangan teknologi. Selain itu, kesenjangan antara inovasi teknologi dan kesiapan regulasi di tingkat global masih menjadi isu penting yang perlu ditangani melalui kolaborasi multidisiplin. Penelitian ini memberikan gambaran menyeluruh bagi praktisi, peneliti, dan pembuat kebijakan mengenai arah perkembangan, kendala utama, dan peluang riset lanjutan di bidang keamanan data siber.

4.2. Saran

Berdasarkan hasil tinjauan pustaka sistematis terhadap tren dan tantangan dalam teknologi keamanan data, disarankan agar penelitian lebih fokus pada pengembangan solusi untuk mengatasi kendala yang ada, khususnya dalam hal pengamanan data pribadi di lingkungan cloud computing dan IoT. Peneliti dapat melakukan penelitian lebih lanjut mengenai penerapan enkripsi yang lebih adaptif dengan kebijakan akses granular yang dapat menangani ancaman di era digital yang semakin berkembang. Selain itu, penelitian yang lebih mendalam mengenai dampak implementasi regulasi global seperti GDPR juga sangat dibutuhkan, mengingat adanya tantangan teknis dan hukum yang masih menghambat efektivitasnya. Kolaborasi antara teknologi dan regulasi di tingkat global perlu diperkuat untuk menciptakan lingkungan keamanan data yang lebih robust dan terintegrasi.

5. DAFTAR PUSTAKA

Abdi, Abdinasir Hirsi, Lukman Audah, Adeb Salh, Mohammed A. Alhartomi, Haroon Rasheed, Salman Ahmed, and Ahmed Tahir. 2024. ‘Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions’. IEEE Access 12:69941–80. doi:10.1109/ACCESS.2024.3393548.

Adam, Mumin, Mohammad Hammoudeh, Rana Alrawashdeh, and Basil Alsulaimy. 2024. ‘A Survey on Security, Privacy,

Trust, and Architectural Challenges in IoT Systems'. IEEE Access 12:57128–49. doi:10.1109/ACCESS.2024.3382709.

Alouffi, Bader, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. 2021. 'A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies'. IEEE Access 9:57792–807. doi:10.1109/ACCESS.2021.3073203.

Alsadie, Deafallah. 2024. 'Artificial Intelligence Techniques for Securing Fog Computing Environments: Trends, Challenges, and Future Directions'. IEEE Access 12:151598–648. doi:10.1109/ACCESS.2024.3463791.

Alves, Paulo Henrique, Fernando Correia, Isabella Frajhof, Clarisse Sieckenius De Souza, and Helio Lopes. 2023. 'Designing Intelligent Agents in Normative Systems Toward Data Regulation Representation'. IEEE Access 11:51590–605. doi:10.1109/ACCESS.2023.3276294.

Awaysheh, Feras M., Mohammad N. Aladwan, Mamoun Alazab, Sadi Alawadi, Jose C. Cabaleiro, and Tomas F. Pena. 2022. 'Security by Design for Big Data Frameworks Over Cloud Computing'. IEEE Transactions on Engineering Management 69(6):3676–93. doi:10.1109/TEM.2020.3045661.

Azam, Naila, Lito Michala, Shuja Ansari, and Nguyen Binh Truong. 2023. 'Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective'. IEEE Transactions on Big Data 9(2):388–414. doi:10.1109/TBDATA.2022.3227336.

Bilal, Muhammad, Ghulam Murtaza, Bilal Demir, Miguel D. Bustamante, and Umar Hayat. 2025. 'An Efficient Algorithm to Generate Dynamic Substitution-Boxes and Its Applications in Image Encryption'. Alexandria Engineering Journal 116:214–31. doi:10.1016/j.aej.2024.11.014.

Bliznak, Karol, Michal Munk, and Anna Pilkova. 2024. 'A Systematic Review of Recent Literature on Data Governance (2017-2023)'. IEEE Access.

Cejas, Orlando Amaral, Muhammad Ilyas Azeem, Sallam Abualhaija, and Lionel C. Briand. 2023. 'NLP-Based Automated Compliance Checking of Data Processing Agreements Against GDPR'. IEEE Transactions on Software Engineering 49(9):4282–4303. doi:10.1109/TSE.2023.3288901.

Dai, Weiqi, Chunkai Dai, Kim Kwang Raymond Choo, Changze Cui, Deiqing Zou, and Hai Jin. 2020. 'SDTE: A Secure Blockchain-Based Data Trading Ecosystem'. IEEE Transactions on Information Forensics and Security 15:725–37. doi:10.1109/TIFS.2019.2928256.

Dou, Haochen, Zhenwu Dan, Peng Xu, Wei Wang, Shuning Xu, Tianyang Chen, and Hai Jin. 2024. 'Dynamic Searchable Symmetric Encryption With Strong Security and Robustness'. IEEE Transactions on Information Forensics and Security 19:2370–84. doi:10.1109/TIFS.2024.3350330.

Feng, Dengguo, Hui Li, Rongxing Lu, Zheli Liu, Jianbing Ni, and Hui Zhu. 2024. 'Data Security and Privacy Computing in Artificial Intelligence'. Journal of Information and Intelligence 2(2):99–101. doi:10.1016/j.jiixd.2024.02.007.

Ghebreselassie, Meron Yonas, Henrik Hammen, and Eli Hustad. 2025. 'Challenges and Considerations in Migration to Cloud Solutions: A Systematic Literature Review'. Pp. 214–21 in Procedia Computer Science. Vol. 256. Elsevier B.V.

Guaman, Danny S., Jose M. Del Alamo, and Julio C. Caiza. 2021. 'GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps'. IEEE Access 9:15961–82. doi:10.1109/ACCESS.2021.3053130.

Gupta, Ishu, Ashutosh Kumar Singh, Chung Nan Lee, and Rajkumar Buyya. 2022. 'Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and

Future Directions'. IEEE Access 10:71247–77.

Han, Sejin, and Sooyong Park. 2022. 'A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review'. IEEE Access 10:103888–905.

Harbi, Yasmine, Zibouda Aliouat, Allaoua Refoufi, and Saad Harous. 2021. 'Recent Security Trends in Internet of Things: A Comprehensive Survey'. IEEE Access 9:113292–314.

Isaac Abiodun, Oludare, Moatsum Alawida, Abiodun Esther Omolara, and Abdulatif Alabdulatif. 2022. 'Data Provenance for Cloud Forensic Investigations, Security, Challenges, Solutions and Future Perspectives: A Survey'. Journal of King Saud University - Computer and Information Sciences 34(10):10217–45.

Karim, Abderrazek, Mustapha Zeroual, Youssef Baddi, Hicham Toumi, and Faysal Bensalah. 2024. 'Using Artificial Intelligence and SDN for Dynamic Scalable Control of Security Rules: An IoT Security Solution'. Pp. 814–17 in Procedia Computer Science. Vol. 251. Elsevier B.V.

Khan, Abudul Wahid, Maseeh Ullah Khan, Javed Ali Khan, Arshad Ahmad, Khalil Khan, Muhammad Zamir, Wonjoon Kim, and Muhammad Fazal Ijaz. 2021. 'Analyzing and Evaluating Critical Challenges and Practices for Software Vendor Organizations to Secure Big Data on Cloud Computing: An AHP-Based Systematic Approach'. IEEE Access 9:107309–32. doi:10.1109/ACCESS.2021.3100287.

Li, Song, Wen Fen Liu, Yan Wu, and Jie Zhao. 2024. 'Generative Architecture for Data Imputation in Secure Blockchain-Enabled Spatiotemporal Data Management'. Journal of Web Engineering 23(1):111–64. doi:10.13052/jwe1540-9589.2315.

Li, Yuanxin, and Darina Saxunová. 2020. 'A Perspective on Categorizing Personal and Sensitive Data and the Analysis of Practical Protection Regulations'. Pp. 1110–15 in Procedia Computer Science. Vol. 170. Elsevier B.V.

Lingga, Patrick, Jaehoon Jeong, Jinhyuk Yang, and Jeonghyeon Kim. 2024. 'SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services'. IEEE Transactions on Dependable and Secure Computing 21(6):5156–69. doi:10.1109/TDSC.2024.3371788.

Marwan, Mbarek, Abdelkarim Ait Temghart, Said Ouhmi, and Mohamed Lazaar. 2024. 'Security, QoS and Energy Aware Optimization of Cloud-Edge Data Centers Using Game Theory and Homomorphic Encryption: Modeling and Formal Verification'. Results in Engineering 24. doi:10.1016/j.rineng.2024.102902.

Miller, Klaus M., Karlo Lukic, and Bernd Skiera. 2025. 'The Impact of the General Data Protection Regulation (GDPR) on Online Tracking'. International Journal of Research in Marketing. doi:10.1016/j.ijresmar.2025.03.002.

Niu, Jie, Xuelian Li, Juntao Gao, and Yue Han. 2020. 'Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for IoT'. IEEE Internet of Things Journal 7(2):1502–18. doi:10.1109/JIOT.2019.2956322.

Omote, Kazumasa, Yoko Inoue, Yoshihide Terada, Naohiro Shichijo, and Toshiyuki Shirai. 2024. 'A Scientometrics Analysis of Cybersecurity Using E-CSTI'. IEEE Access 12:40350–67. doi:10.1109/ACCESS.2024.3375910.

Popoola, Olusogo, Marcos A. Rodrigues, Jims Marchang, Alex Shenfield, Augustine Ikpehai, and Jumoke Popoola. 2024. 'An Optimized Hybrid Encryption Framework for Smart Home Healthcare: Ensuring Data Confidentiality and Security'. Internet of Things (Netherlands) 27. doi:10.1016/j.iot.2024.101314.

Qureshi, Saima Siraj, Jingsha He, Nafei Zhu, Ahsan Nazir, Juan Fang, Xiangjun Ma, Ahsan Wajahat, Faheem Ullah, Sirajuddin Qureshi, Sahroui Dhelim, and Muhammad Salman Pathan. 2025. 'Enhancing IoT Security and Healthcare Data Protection in the Metaverse: A

Dynamic Adaptive Security Mechanism'. Egyptian Informatics Journal 30. doi:10.1016/j.eij.2025.100670.

Rai, Hari Mohan, Kaustubh Kumar Shukla, Lilia Tightiz, and Sanjeevikumar Padmanaban. 2024. 'Enhancing Data Security and Privacy in Energy Applications: Integrating IoT and Blockchain Technologies'. Heliyon 10(19).

Rawat, Danda B., Ronald Doku, and Moses Garuba. 2021. 'Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security'. IEEE Transactions on Services Computing 14(6):2055–72. doi:10.1109/TSC.2019.2907247.

Salih, Bassim M., and Omer K. Jasim Mohammad. 2024. 'Cloud Data Leakage, Security, Privacy Issues and Challenges: Review'. Pp. 592–601 in Procedia Computer Science. Vol. 242. Elsevier B.V.

Taherdoost, Hamed, Tuan Vinh Le, and Khadija Slimani. 2025. 'Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review'. Cryptography 9(1).

Tsouvalas, Vasileios, Samaneh Mohammadi, Ali Balador, Tanir Ozcelebi, Francesco Flammini, and Nirvana Meratnia. 2025. 'EncCluster: Scalable Functional Encryption in Federated Learning through Weight Clustering and Probabilistic Filters'. Pervasive and Mobile Computing 108. doi:10.1016/j.pmcj.2025.102021.

Ullah, Zia, Abdul Waheed, Muhammad Ismail Mohmand, Sadia Basar, Mahdi Zareei, and Fausto Granda. 2024. 'AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity'. IEEE Access 12:142194–214. doi:10.1109/ACCESS.2024.3463976.

Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. 2023. 'Enabling Integrity and Compliance Auditing in Blockchain-Based GDPR-Compliant Data Management'. IEEE Internet of Things Journal 10(23):20955–68. doi:10.1109/JIOT.2023.3285211.

Wu, Axin, Weiqi Luo, Jian Weng, Anjia Yang, and Jinghang Wen. 2023. 'Fuzzy Identity-Based Matchmaking Encryption and Its Application'. IEEE Transactions on Information Forensics and Security 18:5592–5607. doi:10.1109/TIFS.2023.3310663.

Yang, Fan, Mohammad Zoynul Abedin, Yanan Qiao, and Lvyang Ye. 2024. 'Toward Trustworthy Governance of AI-Generated Content (AIGC): A Blockchain-Driven Regulatory Framework for Secure Digital Ecosystems'. IEEE Transactions on Engineering Management 71:14945–62. doi:10.1109/TEM.2024.3472292.

Zafir, Ehsanul Islam, Afifa Akter, M. N. Islam, Shahid A. Hasib, Touhid Islam, Subrata K. Sarker, and S. M. Muyeen. 2024. 'Enhancing Security of Internet of Robotic Things: A Review of Recent Trends, Practices, and Recommendations with Encryption and Blockchain Techniques'. Internet of Things (Netherlands) 28.

Zhang, Lei, Hu Xiong, Qiong Huang, Jiguo Li, Kim Kwang Raymond Choo, and Jiangtao Li. 2022. 'Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities'. IEEE Transactions on Services Computing 15(1):567–87. doi:10.1109/TSC.2019.2937764.

Zhang, Yongxin, Jiacheng Yang, Hong Lei, Zijian Bao, Ning Lu, Wenbo Shi, and Bangdao Chen. 2024. 'PACTA: An IoT Data Privacy Regulation Compliance Scheme Using TEE and Blockchain'. IEEE Internet of Things Journal 11(5):8882–93. doi:10.1109/JIOT.2023.3321308.