Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Nov 2025, VIII (4): 4610 – 4619 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

ANALISIS KEAMANAN DATA PADA SISTEM INFORMASI BERBASIS CLOUD COMPUTING

Novi Rahayu[1], Ade Titin Sumarni[2]
[1]Sekolah Tinggi Ilmu Administrasi Bengkulu, Bengkulu
[2]Universitas Prof. Dr. Hazairin, SH, Bengkulu
e-mail: [1]novierahayu1980@gmail.com, [2]adetitinunihaz@gmail.com

Abstract: *Data security is crucial in the digital era, where cloud computing has become the primary solution for organizations to efficiently store and process data. However, the increasing use of cloud computing also poses significant risks related to data security and privacy. The purpose of this study is to identify challenges and solutions in maintaining data security in cloud computing systems. The method used is a systematic literature review and comparative analysis of various trusted academic sources. The results reveal key threats such as misconfigurations, unauthorized access, and data leaks, which are exacerbated by weak identity management. The study also evaluates mitigation mechanisms such as end-to-end encryption, multi-factor authentication, and a shared responsibility model between cloud service providers and users. These findings can guide the design of effective and adaptive security strategies and policies to support a secure and sustainable digital transformation.*

Keyword: *data security; information systems; cloud computing; encryption; authentication.*

Abstrak: Pentingnya keamanan data dalam era digital di mana cloud computing menjadi solusi utama bagi organisasi untuk menyimpan dan mengolah data secara efisien. Namun, peningkatan penggunaan cloud juga menimbulkan risiko besar terkait keamanan dan privasi data. Tujuan penelitian ini adalah untuk mengidentifikasi tantangan dan solusi dalam menjaga keamanan data pada sistem cloud computing. Metode yang digunakan adalah studi literatur sistematis dan analisis komparatif dari berbagai sumber akademik terpercaya. Hasil penelitian mengungkap ancaman utama seperti kesalahan konfigurasi, akses tidak sah, dan kebocoran data yang diperparah oleh pengelolaan identitas yang lemah. Studi ini juga mengevaluasi mekanisme mitigasi seperti enkripsi end-to-end, otentikasi multi-faktor, dan model tanggung jawab bersama antara penyedia dan pengguna layanan cloud. Temuan ini dapat menjadi panduan dalam merancang strategi dan kebijakan keamanan yang efektif dan adaptif untuk mendukung transformasi digital yang aman dan berkelanjutan.

Kata kunci: keamanan data; sistem informasi; cloud computing; enkripsi; otentikas.

PENDAHULUAN

Perkembangan teknologi informasi telah memberikan dampak yang signifikan terhadap cara organisasi dalam mengelola data dan sistem informasinya. Salah satu perubahan mendasar adalah penerapan cloud computing, yang memungkinkan penyimpanan, pengolahan, serta akses data secara fleksibel melalui jaringan internet. Teknologi ini menghadirkan berbagai keunggulan, seperti kemampuan skalabilitas, efisiensi biaya operasional, dan kemudahan akses dari berbagai lokasi. Meskipun demikian, di balik keunggulan tersebut muncul permasalahan serius terkait keamanan data, mengingat data tidak lagi tersimpan secara lokal melainkan pada server milik penyedia layanan pihak ketiga. Kondisi ini memunculkan perubahan paradigma

keamanan, di mana tanggung jawab atas pengelolaan dan perlindungan data beralih sebagian kepada penyedia layanan, sehingga mengurangi kontrol langsung organisasi terhadap infrastruktur dan akses data. Ketergantungan ini memperbesar potensi risiko terhadap berbagai ancaman siber seperti malware, phishing, dan Distributed Denial of Service (DDoS), serta memperluas area serangan yang memerlukan pengawasan intensif (Gorgulla et al., 2020). Tantangan lainnya mencakup pemenuhan regulasi yang semakin kompleks, risiko kehilangan data akibat gangguan sistem, serta pentingnya penerapan strategi cadangan dan pemulihan yang efektif guna menjaga integritas dan ketersediaan data. Oleh karena itu, selain penerapan langkah-langkah teknis seperti enkripsi end-to-end dan otentikasi multi-faktor, diperlukan pula kolaborasi yang kuat antara organisasi dan penyedia layanan cloud dalam merumuskan kebijakan keamanan serta melakukan pemantauan berkelanjutan untuk menghadapi dinamika ancaman di lingkungan cloud computing (X. Wang et al., 2020).

Oleh karena itu, diperlukan analisis yang komprehensif terhadap aspek keamanan data pada sistem informasi berbasis cloud. Penelitian ini bertujuan untuk mengidentifikasi ancaman utama yang muncul, menilai efektivitas mekanisme perlindungan yang telah diterapkan, serta merumuskan rekomendasi mitigasi yang optimal. Pertanyaan penelitian difokuskan pada identifikasi jenis-jenis ancaman keamanan data dalam cloud computing serta strategi yang paling efektif untuk menanganinya. Fokus analisis meliputi ancaman kritis seperti kebocoran data, pembajakan akun, serangan DDoS, dan kerentanan pada API maupun antarmuka yang tidak aman (S. Wang et al., 2021). Selain itu, perhatian khusus juga diberikan pada kesalahan konfigurasi serta akses tidak sah yang umumnya disebabkan oleh kelalaian pengguna atau lemahnya pengelolaan identitas. Dengan menelaah akar penyebab dan karakteristik ancaman tersebut, penelitian ini diharapkan dapat menghasilkan kerangka mitigasi yang menyeluruh mencakup dimensi teknis, organisasional, dan kebijakan, guna memperkuat keamanan serta keandalan penerapan teknologi cloud computing (Kalvari et al., 2021).

Sejumlah penelitian terdahulu telah mengkaji aspek keamanan dalam penerapan cloud computing dari berbagai perspektif. Kartini (2021), misalnya, menitikberatkan penelitiannya pada isu keamanan dan privasi data di platform Google Drive melalui pendekatan studi literatur untuk mengidentifikasi potensi risiko serta solusi yang relevan (Ferrag et al., 2022). Sementara itu, Suhendar (2022) mengevaluasi implementasi cloud computing dan dampaknya terhadap keamanan sistem, dengan menekankan pentingnya penerapan enkripsi dan mekanisme otentikasi yang kuat. Selanjutnya, Masyhur (2021) mengemukakan bahwa meskipun cloud computing mampu meningkatkan efisiensi operasional, penerapannya tetap menghadirkan tantangan keamanan yang kompleks, seperti kebocoran data dan akses tidak sah akibat kelemahan konfigurasi maupun pengelolaan identitas (Tawalbeh et al., 2020). Di sisi lain, penelitian oleh Essy Malysa (2021) menegaskan bahwa ancaman utama dalam lingkungan cloud meliputi serangan siber, peretasan, dan kebocoran informasi, yang menuntut penerapan kebijakan keamanan komprehensif, termasuk enkripsi data, manajemen akses, serta pemantauan sistem secara berkelanjutan. Berdasarkan kajian terhadap penelitian-penelitian sebelumnya, dapat disimpulkan bahwa meskipun topik keamanan pada cloud computing telah banyak diteliti, masih dibutuhkan analisis yang lebih menyeluruh dan sistematis terhadap berbagai aspek keamanan data dalam sistem informasi berbasis cloud. Penelitian ini berupaya memberikan kontribusi dengan mengintegrasikan temuan dari berbagai studi guna menghasilkan pemahaman yang komprehensif serta rekomendasi yang

aplikatif. Integrasi keamanan dalam cloud computing menuntut penerapan pendekatan holistik yang menggabungkan elemen teknologi, kebijakan, prosedur, dan kontrol untuk melindungi data, aplikasi, serta infrastruktur yang dioperasikan dalam lingkungan cloud. Pendekatan tersebut mencakup pengelolaan identitas dan akses (IAM), enkripsi data, penerapan firewall berbasis cloud, serta mekanisme pemulihan data, yang harus dikelola secara terpadu untuk membangun postur keamanan yang tangguh (Chen et al., 2021)..

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi signifikan bagi organisasi dalam mengelola risiko keamanan data pada proses adopsi cloud computing, sekaligus mendukung pengambilan keputusan yang lebih tepat dalam penerapan sistem informasi berbasis cloud yang aman dan andal. Temuan penelitian ini dapat dijadikan landasan bagi pengembangan kebijakan keamanan yang lebih efektif, khususnya dalam menghadapi kompleksitas dan dinamika teknologi cloud yang terus berkembang (Zhao et al., 2021). Selain itu, hasil kajian ini dapat membantu organisasi dalam menentukan platform cloud yang paling sesuai dengan kebutuhan keamanan dan kepatuhan terhadap regulasi, serta dalam merancang arsitektur keamanan yang terintegrasi dan adaptif terhadap ancaman siber yang terus berevolusi. Dengan pendekatan yang berbasis bukti dan bersifat komprehensif, penelitian ini tidak hanya memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang akademik, tetapi juga pada peningkatan praktik keamanan siber di sektor publik maupun swasta (Phan et al., 2020).

METODE

Penelitian ini menerapkan pendekatan kualitatif dengan menggunakan metode studi literatur sistematis serta analisis komparatif untuk mengkaji aspek keamanan data pada sistem informasi berbasis cloud computing. Jenis penelitian yang bersifat deskriptif-analitis ini bertujuan untuk mengidentifikasi, menganalisis, serta mengevaluasi berbagai dimensi keamanan data dalam lingkungan cloud computing dengan mengacu pada hasil-hasil penelitian dan sumber teknis yang kredibel (Shoeibi et al., 2021).

Subjek dalam penelitian ini mencakup berbagai sumber literatur yang relevan, meliputi jurnal ilmiah, buku akademik, laporan teknis, serta dokumentasi resmi dari penyedia layanan cloud computing. Adapun objek penelitian difokuskan pada mekanisme keamanan data yang mencakup penerapan enkripsi, otentikasi multi-faktor, kontrol akses, serta kebijakan dan praktik keamanan yang digunakan dalam sistem informasi berbasis cloud (Abou-Nassar et al., 2020).

Instrumen utama dalam penelitian ini berupa checklist analisis literatur yang disusun berdasarkan kerangka kerja analisis komparatif (Kasongo, 2023). Checklist tersebut mencakup sejumlah kriteria evaluatif, antara lain jenis teknik keamanan yang digunakan, tingkat enkripsi yang diterapkan, metode otentikasi yang diimplementasikan, kebijakan pengendalian akses, serta tingkat kepatuhan terhadap standar keamanan internasional seperti ISO 27001 dan NIST (Or-Meir et al., 2020).

Proses pengumpulan data dilakukan melalui pencarian literatur secara sistematis pada basis data akademik seperti Google Scholar, Scopus, dan Crossref, dengan menggunakan kata kunci “keamanan data cloud”, “enkripsi cloud”, serta “manajemen akses cloud” (J. Wang et al., 2020).

Metode analisis data dalam penelitian ini menerapkan pendekatan sintesis dan analisis kritis terhadap literatur yang telah dikumpulkan. Proses analisis dilakukan melalui tiga tahapan utama, yaitu reduksi data, kategorisasi temuan, dan interpretasi hasil (Egala et al., 2021).

Analisis komparatif dilaksanakan

dengan menelaah dan membandingkan hasil temuan dari berbagai sumber berdasarkan variabel yang telah ditetapkan, seperti efektivitas teknik enkripsi, tingkat kompleksitas penerapan, serta level keamanan yang dihasilkan (You & Dong, 2020).

HASIL DAN PEMBAHASAN

Tabel 1. Analisis Kritis Potensi Celah Keamanan, Pola Penerapan Teknologi, dan Strategi Mitigasi dalam Keamanan Data Cloud Computing

No	Potensi Celah Keamanan	Pola Penerapan Teknologi	Strategi Mitigasi
1	Kesalahan konfigurasi layanan cloud	Pengaturan izin akses terlalu longgar	Audit konfigurasi berkala dan perbaikan segera
2	Penggunaan kredensial yang dicuri (credential stuffing)	Otentikasi berbasis password lama tanpa MFA	Implementasi autentikasi multi-faktor (MFA), pemantauan aktivitas login mencurigakan
3	API yang tidak aman	API terbuka tanpa autentikasi dan enkripsi	Pengamanan API dengan otentikasi kuat, enkripsi, dan pemantauan penggunaan
4	IAM yang tidak memadai	Hak akses berlebihan dan tidak sesuai prinsip kebutuhan	Pengelolaan hak akses berbasis peran, penerapan least privilege, dan MFA
5	Kurangnya pemantauan keamanan cloud	Minimnya sistem deteksi intrusi dan pemantauan real-time	Penerapan sistem pemantauan keamanan cloud berbasis AI dan analitik anomali
6	Kebocoran data akibat insiden	Kesalahan konfigurasi dan penyimpanan data sensitif tidak aman	Pelatihan keamanan karyawan, enkripsi end-to-end, dan kebijakan ketat
7	Kurangnya transparansi dari penyedia layanan	Informasi praktik keamanan yang minim	Negosiasi SLA dengan klausul keamanan tegas dan audit regular terhadap penyedia
8	Kelemahan dalam pemenuhan regulasi seperti GDPR	Implementasi parsial terhadap standar privasi	Pembentukan tim kepatuhan dan audit internal yang rutin
9	Ketergantungan berlebihan pada penyedia cloud	Relatif minim kontrol keamanan di sisi pengguna	Edukasi pengguna, pengembangan kebijakan pengelolaan keamanan internal

No	Potensi Celah Keamanan	Pola Penerapan Teknologi	Strategi Mitigasi
10	Serangan siber yang semakin adaptif	Penggunaan teknologi AI dan botnet dalam serangan	Penggunaan AI untuk deteksi dini dan tanggapan insiden cybersec

Penelitian ini menunjukkan bahwa meskipun cloud computing memberikan sejumlah keuntungan seperti skalabilitas, efisiensi biaya, dan fleksibilitas operasional, penerapannya tetap disertai dengan risiko keamanan yang signifikan terhadap integritas serta kerahasiaan data (Zhang et al., 2020). Berdasarkan hasil kajian literatur, ancaman utama yang teridentifikasi mencakup kesalahan konfigurasi, akses tidak sah, kebocoran data, dan serangan DDoS, yang secara konsisten ditemukan di berbagai sektor dan konteks organisasi. Selain ancaman eksternal, faktor internal seperti rendahnya kesadaran keamanan serta kelemahan dalam manajemen identitas turut berkontribusi terhadap kerentanan sistem, menegaskan bahwa unsur manusia masih menjadi komponen paling rentan dalam struktur keamanan cloud (Çalık, 2021).

Hasil interpretasi analisis menunjukkan bahwa tidak terdapat satu pun platform cloud yang secara absolut unggul dalam seluruh aspek keamanan, melainkan masing-masing memiliki keunggulan yang bersifat kontekstual sesuai dengan karakteristik dan kebutuhan penggunaannya (Bera et al., 2020). Platform AWS menampilkan kelebihan dalam hal intelijen ancaman dan kemampuan skalabilitas, Azure unggul dalam integrasi dengan ekosistem Microsoft serta penerapan keamanan menyeluruh, sedangkan Google Cloud Platform (GCP) menawarkan kemudahan operasional dan inovasi tinggi dalam analitik data. Temuan ini menegaskan bahwa pemilihan platform cloud sebaiknya didasarkan pada kesesuaian dengan kebutuhan organisasi dan kapasitas teknologinya, bukan semata pada tingkat popularitas atau jumlah fitur yang disediakan (Soni et al., 2022).

Hasil penelitian juga menunjukkan bahwa pemenuhan terhadap standar keamanan internasional seperti ISO 27001 dan NIST masih menjadi tantangan signifikan bagi banyak organisasi, terutama akibat keterbatasan sumber daya, kurangnya dokumentasi yang memadai, serta rendahnya transparansi dari pihak penyedia layanan cloud (C. Wang et al., 2020). Minimnya keterbukaan terkait praktik keamanan penyedia layanan tersebut menghambat kemampuan organisasi untuk melakukan audit dan penilaian risiko secara independen, sehingga meningkatkan tingkat ketergantungan sekaligus memperbesar potensi kerentanan sistem. Dengan demikian, diperlukan langkah evaluatif yang komprehensif sebelum proses adopsi layanan cloud dilakukan, termasuk negosiasi Service Level Agreement (SLA) yang secara eksplisit mencantumkan ketentuan mengenai aspek keamanan data dan tanggung jawab bersama (Tong et al., 2020).

Analisis kritis terhadap validitas dan reliabilitas sumber menunjukkan bahwa mayoritas temuan penelitian didukung oleh literatur yang berasal dari jurnal bereputasi, khususnya yang terindeks Scopus dan IEEE dengan faktor dampak yang memadai, sehingga memperkuat tingkat kredibilitas dan keandalan hasil studi ini (Amini et al., 2022). Meskipun demikian, masih terdapat kekosongan dalam literatur yang membahas implementasi keamanan cloud pada sektor publik dan usaha mikro, kecil, dan menengah (UMKM), menandakan perlunya kajian lebih lanjut dalam konteks tersebut. Selain itu, kecenderungan meningkatnya penerapan zero trust architecture dan cloud security

posture management (CSPM) mencerminkan adanya pergeseran paradigma keamanan cloud dari pendekatan perimeter tradisional menuju model yang lebih adaptif, kontekstual, dan berbasis manajemen risiko (Bi et al., 2022).

Penelitian ini turut menegaskan peran krusial penyedia layanan cloud dalam memastikan perlindungan data pengguna, meskipun tanggung jawab keamanan tetap berada dalam kerangka shared responsibility model (Karar et al., 2021). Dengan demikian, organisasi tidak dapat sepenuhnya mengandalkan penyedia layanan, melainkan harus berperan aktif dalam pengelolaan konfigurasi sistem, pengaturan akses, serta penerapan kebijakan keamanan internal. Kondisi ini mengindikasikan bahwa keamanan cloud tidak semata-mata bergantung pada aspek teknologi, tetapi juga menuntut tata kelola yang efektif serta manajemen risiko yang terencana dan berkesinambungan (Heidari et al., 2022).

Meskipun demikian, penelitian ini memiliki sejumlah keterbatasan, terutama karena tidak melakukan pengujian hipotesis secara empiris akibat pendekatannya yang bersifat kualitatif, sehingga hasil temuan belum dapat digeneralisasi secara statistik. Selain itu, pembatasan pada literatur dalam kurun waktu lima tahun terakhir berpotensi mengesampingkan dinamika dan evolusi jangka panjang dalam bidang keamanan cloud. Oleh karena itu, untuk penelitian berikutnya disarankan dilakukan studi empiris, seperti studi kasus atau survei terhadap organisasi pengguna cloud, guna memperkuat hasil kualitatif dengan dukungan data kuantitatif yang lebih representatif (Alam, 2021).

Dengan demikian, penelitian ini memberikan kontribusi yang berarti dalam memperdalam pemahaman mengenai tantangan serta strategi mitigasi terkait keamanan data pada sistem informasi berbasis cloud computing. Hasil temuan dan rekomendasi yang diperoleh dapat dijadikan acuan bagi organisasi dalam menyusun strategi keamanan cloud yang efisien dan adaptif, sekaligus berfungsi sebagai landasan bagi perumusan kebijakan serta penerapan praktik terbaik dalam pengelolaan keamanan data di masa mendatang (C. Wang et al., 2021).

SIMPULAN

Berdasarkan hasil penelitian yang diperoleh melalui studi literatur sistematis dan analisis komparatif, dapat disimpulkan bahwa meskipun cloud computing menawarkan manfaat signifikan dalam hal skalabilitas, efisiensi biaya, dan fleksibilitas, adopsinya juga membawa berbagai risiko keamanan yang kompleks terhadap integritas, kerahasiaan, dan ketersediaan data. Ancaman utama yang diidentifikasi meliputi kesalahan konfigurasi infrastruktur, akses tidak sah, kebocoran data, dan serangan DDoS, yang sering kali diperparah oleh faktor internal seperti kurangnya kesadaran keamanan dan pengelolaan identitas yang lemah. Analisis komparatif terhadap platform utama (AWS, Azure, GCP) menunjukkan bahwa tidak ada satu platform yang unggul secara mutlak, melainkan masing-masing memiliki keunggulan kontekstual dalam aspek seperti intelijen ancaman, integrasi ekosistem, atau kemudahan penggunaan. Penerapan mekanisme keamanan seperti enkripsi end-to-end, otentikasi multi-faktor, dan Zero Trust Architecture terbukti efektif, namun keberhasilannya sangat bergantung pada implementasi yang konsisten dan pemahaman terhadap model tanggung jawab bersama (shared responsibility model). Penelitian ini juga mengungkap tantangan dalam kepatuhan terhadap standar seperti ISO 27001 dan NIST, serta celah dalam literatur mengenai implementasi di sektor publik dan UMKM. Dengan demikian, pendekatan holistik yang mengintegrasikan aspek teknis, organisasional, dan tata kelola menjadi kunci dalam membangun postur

keamanan cloud yang tangguh, adaptif, dan berbasis risiko, guna mendukung transformasi digital yang aman dan berkelanjutan di era Industri 4.0.Bagian simpulan harus berbentuk paragraf yang menjawab tujuan penelitian, menceritakan bagaimana pekerjaan Anda dapat memajukan pengetahuan terkini.

DAFTAR PUSTAKA

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *8*, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468

Ahmed, I., Jeon, G., & Piccialli, F. (2022). From Artificial Intelligence to Explainable Artificial Intelligence in Industry 4.0: A Survey on What, How, and Where. *IEEE Transactions on Industrial Informatics*, *18*(8), 5031–5042. https://doi.org/10.1109/TII.2022.3146552

Alam, T. (2021). Cloud-Based IoT Applications and Their Roles in Smart Cities. *Smart Cities*, *4*(3), 1196–1219. https://doi.org/10.3390/smartcities4030064

Albahri, A. S., Alwan, J. K., Taha, Z. K., Ismail, S. F., Hamid, R. A., Zaidan, A. A., Albahri, O. S., Zaidan, B. B., Alamoodi, A. H., & Alsalem, M. A. (2021). IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. *Journal of Network and Computer Applications*, *173*, 102873. https://doi.org/10.1016/j.jnca.2020.102873

Amini, S., Saber, M., Rabiei-Dastjerdi, H., & Homayouni, S. (2022). Urban Land Use and Land Cover Change Analysis Using Random Forest Classification of Landsat Time Series. *Remote Sensing*, *14*(11), 2654. https://doi.org/10.3390/rs14112654

Arthurs, P., Gillam, L., Krause, P., Wang, N., Halder, K., & Mouzakitis, A. (2022). A Taxonomy and Survey of Edge Cloud Computing for Intelligent Transportation Systems and Connected Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6206–6221. https://doi.org/10.1109/TITS.2021.3084396

Bera, B., Chattaraj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communications*, *153*, 229–249. https://doi.org/10.1016/j.comcom.2020.02.011

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

Çalık, A. (2021). A novel Pythagorean fuzzy AHP and fuzzy TOPSIS methodology for green supplier selection in the Industry 4.0 era. *Soft Computing*, *25*(3), 2253–2265. https://doi.org/10.1007/s00500-020-05294-9

Chen, C., Liu, B., Wan, S., Qiao, P., & Pei, Q. (2021). An Edge Traffic Flow Detection Scheme Based on Deep Learning in an Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems*, *22*(3), 1840–1852. https://doi.org/10.1109/TITS.2020.3025687

Cui, Y., Kara, S., & Chan, K. C. (2020). Manufacturing big data ecosystem: A systematic literature review. *Robotics and Computer-Integrated Manufacturing*, *62*, 101861. https://doi.org/10.1016/j.rcim.2019.1

01861

Dhanaraju, M., Chenniappan, P., Ramalingam, K., Pazhanivelan, S., & Kaliaperumal, R. (2022). Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture. *Agriculture*, *12*(10), 1745. https://doi.org/10.3390/agriculture12101745

Ding, Y., Jin, M., Li, S., & Feng, D. (2021). Smart logistics based on the internet of things technology: an overview. *International Journal of Logistics Research and Applications*, *24*(4), 323–345. https://doi.org/10.1080/13675567.2020.1757053

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet of Things Journal*, *8*(14), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, *10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

Ghorbanian, A., Kakooei, M., Amani, M., Mahdavi, S., Mohammadzadeh, A., & Hasanlou, M. (2020). Improved land cover map of Iran using Sentinel imagery within Google Earth Engine and a novel automatic workflow for land cover classification using migrated training samples. *ISPRS Journal of Photogrammetry and Remote Sensing*, *167*, 276–288. https://doi.org/10.1016/j.isprsjprs.2020.07.013

Gomes, V., Queiroz, G., & Ferreira, K. (2020). An Overview of Platforms for Big Earth Observation Data Management and Analysis. *Remote Sensing*, *12*(8), 1253. https://doi.org/10.3390/rs12081253

Heidari, A., Navimipour, N. J., & Unal, M. (2022). Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: A systematic literature review. *Sustainable Cities and Society*, *85*, 104089. https://doi.org/10.1016/j.scs.2022.104089

Jalili, V., Afgan, E., Gu, Q., Clements, D., Blankenberg, D., Goecks, J., Taylor, J., & Nekrutenko, A. (2020). The Galaxy platform for accessible, reproducible and collaborative biomedical analyses: 2020 update. *Nucleic Acids Research*, *48*(W1), W395–W402. https://doi.org/10.1093/nar/gkaa434

Kalvari, I., Nawrocki, E. P., Ontiveros-Palacios, N., Argasinska, J., Lamkiewicz, K., Marz, M., Griffiths-Jones, S., Toffano-Nioche, C., Gautheret, D., Weinberg, Z., Rivas, E., Eddy, S. R., Finn, R. D., Bateman, A., & Petrov, A. I. (2021). Rfam 14: expanded coverage of metagenomic, viral and microRNA families. *Nucleic Acids Research*, *49*(D1), D192–D200. https://doi.org/10.1093/nar/gkaa1047

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*, 113–125. https://doi.org/10.1016/j.comcom.2022.12.010

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., & Das, S. K. (2023). Edge-computing-driven Internet of Things: A Survey. *ACM Computing Surveys*, *55*(8), 1–41. https://doi.org/10.1145/3555308

Li, Y., Dai, J., & Cui, L. (2020). The impact of digital technologies on economic and environmental

performance in the context of industry 4.0: A moderated mediation model. *International Journal of Production Economics*, *229*, 107777. https://doi.org/10.1016/j.ijpe.2020.107777

Mamta, Gupta, B. B., Li, K.-C., Leung, V. C. M., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System. *IEEE/CAA Journal of Automatica Sinica*, *8*(12), 1877–1890. https://doi.org/10.1109/JAS.2021.1004003

Mansour, R. F., Amraoui, A. El, Nouaouri, I., Diaz, V. G., Gupta, D., & Kumar, S. (2021). Artificial Intelligence and Internet of Things Enabled Disease Diagnosis Model for Smart Healthcare Systems. *IEEE Access*, *9*, 45137–45146. https://doi.org/10.1109/ACCESS.2021.3066365

Pereira, L. S., Paredes, P., & Jovanovic, N. (2020). Soil water balance models for determining crop water and irrigation requirements and irrigation scheduling focusing on the FAO56 method and the dual Kc approach. *Agricultural Water Management*, *241*, 106357. https://doi.org/10.1016/j.agwat.2020.106357

Phan, T. N., Kuch, V., & Lehnert, L. W. (2020). Land Cover Classification using Google Earth Engine and Random Forest Classifier—The Role of Image Composition. *Remote Sensing*, *12*(15), 2411. https://doi.org/10.3390/rs12152411

Ren, L., Dong, J., Wang, X., Meng, Z., Zhao, L., & Deen, M. J. (2021). A Data-Driven Auto-CNN-LSTM Prediction Model for Lithium-Ion Battery Remaining Useful Life. *IEEE Transactions on Industrial Informatics*, *17*(5), 3478–3487. https://doi.org/10.1109/TII.2020.3008223

Rodrigues, T. K., Suto, K., Nishiyama, H., Liu, J., & Kato, N. (2020). Machine Learning Meets Computation and Communication Control in Evolving Edge and Cloud: Challenges and Future Perspective. *IEEE Communications Surveys & Tutorials*, *22*(1), 38–67. https://doi.org/10.1109/COMST.2019.2943405

Sharma, A., Singh, P. K., & Kumar, Y. (2020). An integrated fire detection system using IoT and image processing technique for smart cities. *Sustainable Cities and Society*, *61*, 102332. https://doi.org/10.1016/j.scs.2020.102332

Sharma, R., Kamble, S. S., Gunasekaran, A., Kumar, V., & Kumar, A. (2020). A systematic literature review on machine learning applications for sustainable agriculture supply chain performance. *Computers & Operations Research*, *119*, 104926. https://doi.org/10.1016/j.cor.2020.104926

Soni, G., Kumar, S., Mahto, R. V., Mangla, S. K., Mittal, M. L., & Lim, W. M. (2022). A decision-making framework for Industry 4.0 technology implementation: The case of FinTech and sustainable supply chain finance for SMEs. *Technological Forecasting and Social Change*, *180*, 121686. https://doi.org/10.1016/j.techfore.2022.121686

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2021). IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network. *IEEE Internet of Things Journal*, *8*(7), 5164–5171. https://doi.org/10.1109/JIOT.2020.3033131

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Tian, Z., Luo, C., Qiu, J., Du, X., & Guizani, M. (2020). A Distributed Deep Learning System for Web Attack Detection on Edge Devices. *IEEE Transactions on Industrial Informatics*, *16*(3), 1963–1971. https://doi.org/10.1109/TII.2019.2938778

Tong, Z., Chen, H., Deng, X., Li, K., & Li, K. (2020). A scheduling scheme in the cloud computing environment using deep Q-learning. *Information Sciences*, *512*, 1170–1191. https://doi.org/10.1016/j.ins.2019.10.035

Wang, C., Qin, J., Qu, C., Ran, X., Liu, C., & Chen, B. (2021). A smart municipal waste management system based on deep-learning and Internet of Things. *Waste Management*, *135*, 20–29. https://doi.org/10.1016/j.wasman.2021.08.028

Wang, J., Wu, L., Choo, K.-K. R., & He, D. (2020). Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure. *IEEE Transactions on Industrial Informatics*, *16*(3), 1984–1992. https://doi.org/10.1109/TII.2019.293

Wang, S., Guo, Y., Zhang, N., Yang, P., Zhou, A., & Shen, X. (2021). Delay-Aware Microservice Coordination in Mobile Edge Computing: A Reinforcement Learning Approach. *IEEE Transactions on Mobile Computing*, *20*(3), 939–951. https://doi.org/10.1109/TMC.2019.2957804

Wang, X., Han, Y., Leung, V. C. M., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of Edge Computing and Deep Learning: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *22*(2), 869–904. https://doi.org/10.1109/COMST.2020.2970550

Wazid, M., Das, A. K., Bhat K, V., & Vasilakos, A. V. (2020). LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, *150*, 102496. https://doi.org/10.1016/j.jnca.2019.102496

Xia, S., Yao, Z., Li, Y., & Mao, S. (2021). Online Distributed Offloading and Computing Resource Management With Energy Harvesting for Heterogeneous MEC-Enabled IoT. *IEEE Transactions on Wireless Communications*, *20*(10), 6743–6757. https://doi.org/10.1109/TWC.2021.3076201

You, N., & Dong, J. (2020). Examining earliest identifiable timing of crops using all available Sentinel 1/2 imagery and Google Earth Engine. *ISPRS Journal of Photogrammetry and Remote Sensing*, *161*, 109–123. https://doi.org/10.1016/j.isprsjprs.2020.01.001

Zhang, Z., Wang, Z., Shi, T., Bi, C., Rao, F., Cai, Y., Liu, Q., Wu, H., & Zhou, P. (2020). Memory materials and devices: From concept to application. *InfoMat*, *2*(2), 261–290. https://doi.org/10.1002/inf2.12077

Zhao, Y., Zhao, J., Yang, M., Wang, T., Wang, N., Lyu, L., Niyato, D., & Lam, K.-Y. (2021). Local Differential Privacy-Based Federated Learning for Internet of Things. *IEEE Internet of Things Journal*, *8*(11), 8836–8853. https://doi.org/10.1109/JIOT.2020.3037194

Zhou, Y., Shen, M., Cui, X., Shao, Y., Li, L., & Zhang, Y. (2021). Triboelectric nanogenerator based self-powered sensor for artificial intelligence. *Nano Energy*, *84*, 105887. https://doi.org/10.1016/j.nanoen.2021.105887