Jurnal Teknologi dan Sains Modern
https://journal.scitechgrup.com/index.php/jtsm

Vol. 1 (1), 2024, Hal. 1-8

Transparansi dan Auditabilitas Data Pribadi dalam Layanan Berbasis *Cloud* Pada Proyek PACE: Studi Literatur

Syaiful Bachri M[1,*], Muhammad Atnang[1], Sahriani[1], Nur Hikmah[2], Samsidar[1]

[1] Program Studi Teknologi Informasi, Fakultas Sains Teknologi dan Kesehatan, Institut Sains Teknologi dan Kesehatan Aisyiyah Kendari
[2] Program Studi Teknik Komputer, Fakultas Teknik Institut Sains dan Teknologi Kolaka Utara

*Correspondence: sbm@istekaisyiyah.ac.id

Abstrak

Ulasan komprehensif ini mengeksplorasi pendekatan-pendekatan beragam dalam meningkatkan privasi dan keamanan dalam manajemen data di berbagai bidang. Studi pertama menyajikan kerangka konseptual yang bertujuan untuk memperkuat privasi dan keamanan dalam manajemen data kota cerdas dengan mengintegrasikan kecerdasan buatan dan pemodelan big data. Meskipun analisis data empiris absen, kerangka konseptual tersebut memberikan wawasan penting tentang kemungkinan kemajuan. Studi kedua menelusuri proyek Privacy-Aware Cloud Ecosystems (PACE), berfokus pada teknologi blockchain untuk meningkatkan transparansi dan auditabilitas dalam pemrosesan data pribadi berbasis awan. Meskipun secara utama berorientasi pada masa depan, teknologi yang dikembangkan menjanjikan peningkatan privasi dan keamanan data dalam komputasi awan. Tinjauan literatur dalam studi ketiga mengevaluasi tren dan tantangan dalam menerapkan keamanan dan blockchain dalam Internet of Multimedia Things (IoMT), memberikan wawasan berharga meskipun tanpa temuan empiris langsung. Terakhir, sebuah studi eksperimental memperkenalkan sistem pengolahan data berbasis blockchain dan differential privacy untuk komputasi perkotaan, melaporkan kinerja sistem dan peningkatan keamanannya. Meskipun metodologi beragam, setiap studi memberikan kontribusi pada diskusi yang lebih luas tentang privasi dan keamanan data, menawarkan wawasan, kerangka kerja, dan inovasi teknologi untuk penelitian dan implementasi praktis di masa depan.

Kata kunci: Privasi Data; Keamanan Data; *Big* Data; Proyek PCE; Cloud; Internet of Multimedia Things (IoMT)

1. PENDAHULUAN

Fokus penelitian ini adalah pada privasi dan keamanan dalam manajemen data di kota cerdas. Kompleksitas layanan berbasis cloud juga meningkat, sehingga menimbulkan kekhawatiran besar terkait privasi data (Chen et al., 2021). Keamanan dan transparansi dalam layanan berbasis *cloud* juga menjadi perhatian utama, mengingat arsitektur layanan cloud yang cenderung tidak transparan dan rumit (Llanos et al., 2023). Begitu juga, keamanan dan keandalan data pada sistem penyimpanan cloud menjadi semakin penting, terutama dengan semakin banyaknya data yang dihasilkan dari perangkat IoT di komputasi perkotaan (Heo & Doh, 2024). Keamanan data di komputasi perkotaan merupakan masalah krusial karena risiko pelanggaran privasi pengguna yang timbul dari penggunaan data yang tidak terlindungi (Malhotra & Singh, 2023). Masalah privasi dan keamanan dalam manajemen data kota cerdas

dianggap penting karena merupakan faktor utama dalam infrastruktur kota cerdas (Chen et al., 2021). Hal ini penting karena semakin banyak data pribadi yang disimpan di *cloud*, sementara kompleksitas layanan berbasis cloud juga meningkat, sehingga menimbulkan kekhawatiran besar terkait privasi data (Llanos et al., 2023). Demikian juga, penggunaan komputasi awan semakin meluas, namun keamanan data menjadi perhatian utama, terutama dengan risiko pelanggaran privasi pengguna (Heo & Doh, 2024). Oleh karena itu, diperlukan solusi enkripsi data yang efektif untuk meningkatkan keamanan (Malhotra & Singh, 2023).

Tujuan utama penelitian yang dilakukan oleh Chen et al., (202) adalah untuk mengusulkan kerangka kerja atau sistem yang dapat meningkatkan aspek privasi dan keamanan dalam manajemen data di berbagai aplikasi kota cerdas (Chen et al., 2021). Tujuan penelitian lainnya adalah merancang teknologi peningkat privasi berbasis blockchain yang dapat meningkatkan transparansi dan kemampuan audit pemrosesan data pribadi dalam layanan berbasis *cloud* (Llanos et al., 2023). Begitu juga, penelitian ini bertujuan untuk mengusulkan sistem pengolahan data yang aman menggunakan *blockchain* dan *differential privacy* untuk melindungi keamanan dan privasi data di komputasi perkotaan (Heo & Doh, 2024). Tujuan lainnya adalah mengembangkan model enkripsi dan pengambilan data cloud yang meningkatkan keamanan data dengan menggunakan *Symmetric Searchable Encryption* dan *Machine Learning* (Malhotra & Singh, 2023). Chen et al. (2021) tidak secara eksplisit menyebutkan hipotesis atau pertanyaan penelitian yang diajukan. Demikian juga, Llanos et al. (2023) juga tidak menyebutkan pertanyaan penelitian secara eksplisit, tetapi mengusulkan pengembangan teknologi peningkat privasi berbasis *blockchain*. Namun, Heo & Doh (2024) menanyakan bagaimana merancang sistem pengolahan data yang aman menggunakan blockchain dan differential privacy. Malhotra & Singh (2023) juga tidak menyebutkan hipotesis atau pertanyaan penelitian secara eksplisit, tetapi mereka menyebutkan tujuan merancang teknologi enkripsi data cloud yang efektif.

Konteks penelitian ini adalah perkembangan kota cerdas yang mengadopsi teknologi informasi dan komunikasi (ICT) untuk mengatasi tantangan urbanisasi. Namun, faktor utamanya adalah privasi, keamanan, kerahasiaan, dan otentisitas dalam manajemen data kota cerdas (Chen et al., 2021). Begitu juga, komputasi perkotaan menggunakan berbagai perangkat IoT yang menghasilkan banyak data, namun penggunaan data tersebut dapat menimbulkan masalah privasi jika tidak dilindungi dengan baik (Heo & Doh, 2024). Masalah keamanan data di komputasi perkotaan menjadi semakin penting karena risiko pelanggaran privasi pengguna (Malhotra & Singh, 2023).Pendekatan yang digunakan dalam penelitian ini adalah kombinasi dari review literatur dan pengembangan kerangka kerja baru atau sistem baru. Beberapa penelitian menggunakan metode analisis deskriptif untuk mengevaluasi kelemahan sistem eksisting dan merancang solusi yang lebih baik (Chen et al., 2021). Llanos et al. (2023) mengusulkan pengembangan teknologi peningkat privasi berbasis blockchain dengan menganalisis kelemahan sistem *cloud* eksisting. Selain itu, Heo & Doh (2024) menggunakan pendekatan kualitatif untuk merancang sistem pengolahan data yang aman menggunakan *blockchain* dan *differential privacy*. Malhotra & Singh (2023) menggunakan pendekatan eksperimental untuk merancang teknologi enkripsi data *cloud* yang efektif.

Hasil penelitian ini mencakup pengembangan kerangka kerja atau sistem baru yang dapat meningkatkan privasi dan keamanan dalam manajemen data kota cerdas (Chen et al., 2021). Llanos et al. (2023) menemukan bahwa pengembangan teknologi peningkat privasi berbasis *blockchain* dapat meningkatkan transparansi dan kemampuan audit pemrosesan data pribadi dalam layanan berbasis cloud. Heo & Doh (2024) menemukan bahwa sistem pengolahan data yang aman menggunakan blockchain dan *differential privacy* dapat melindungi keamanan dan privasi data di komputasi perkotaan. Malhotra & Singh (2023) menemukan bahwa teknologi enkripsi data *cloud* yang mereka rancang efektif meningkatkan keamanan data. Implikasi praktis dari penelitian ini adalah pengembangan kerangka kerja atau sistem baru yang dapat meningkatkan aspek privasi dan keamanan dalam manajemen data kota cerdas (Chen et al., 2021). Kontribusi teoritis termasuk pengembangan teknologi peningkat privasi berbasis *blockchain* (Llanos et al., 2023) dan pengembangan model enkripsi dan pengambilan data *cloud* (Malhotra & Singh, 2023).

Melalui review pendahuluan dari berbagai penelitian terkait, terlihat bahwa privasi dan keamanan data memegang peranan penting dan kompleks dalam konteks kota cerdas. Beragam pendekatan penelitian, mulai dari analisis deskriptif hingga eksperimen, telah menghasilkan kerangka kerja, teknologi, dan model baru yang bertujuan meningkatkan privasi dan keamanan data dalam manajemen kota cerdas. Temuan-temuan ini memberikan wawasan mendalam tentang tantangan serta solusi yang sedang dikembangkan dalam mengatasi isu-isu privasi dan keamanan data di lingkungan kota cerdas. Dengan demikian, penelitian ini berkontribusi dalam menghadirkan pemahaman yang lebih baik tentang cara meningkatkan aspek privasi dan keamanan dalam konteks kota cerdas melalui inovasi teknologi dan metodologi penelitian yang beragam.

2. LITERATUR REVIEW

Dari tinjauan literatur yang dilakukan memberikan wawasan yang berharga tentang isu-isu privasi dan keamanan data dalam konteks kota cerdas. Chen et al. (2021) membahas pengembangan kerangka kerja *Holistic Big Data Integrated Artificial Intelligent Modeling* (HBDIAIM) untuk meningkatkan privasi dan keamanan dalam manajemen data kota cerdas. Mereka menyoroti pentingnya solusi yang komprehensif untuk mengatasi tantangan ini. Berdasarkan analisis deskriptif dan pengembangan kerangka kerja baru, penelitian ini menyajikan kontribusi penting dalam upaya meningkatkan privasi dan keamanan data dalam manajemen kota cerdas. Selain itu, Llanos et al. (2023) mengeksplorasi penggunaan *blockchain* untuk meningkatkan transparansi dan akuntabilitas dalam pemrosesan data pribadi di layanan berbasis *cloud*. Dalam proyek *Privacy-Aware Cloud Ecosystems* (PACE), mereka menemukan tantangan dan pelajaran berharga dalam menerapkan teknologi blockchain untuk memperbaiki privasi data. Kolaborasi antara ahli komputer dan ahli hukum sosial menjadi kunci dalam mengatasi kompleksitas masalah ini. Penelitian ini menunjukkan betapa pentingnya pendekatan lintas disiplin dalam menghadapi tantangan privasi dan keamanan data.

Jan et al. (2020) membahas konvergensi keamanan dan *blockchain* dengan *Internet of Multimedia Things* (IoMT). Dalam konteks IoMT, tantangan keamanan menjadi semakin kompleks dengan integrasi teknologi multimedia. Penelitian ini menyoroti perlunya pengembangan kerangka teoritis yang mengintegrasikan keamanan dan *blockchain* sebagai solusi untuk mengatasi tantangan ini. Dengan tinjauan komprehensif literatur, penulis mengidentifikasi kesenjangan dalam penelitian yang menyoroti perlunya solusi yang komprehensif dan terintegrasi. SedangkanHeo & Doh (2024) mempertimbangkan penggunaan *blockchain* dan *differential privacy* untuk membangun sistem pengolahan data yang aman dan melindungi privasi data di komputasi perkotaan. Penelitian ini menyoroti kebutuhan akan solusi yang dapat mengatasi risiko tinggi terhadap pelanggaran privasi data di lingkungan kota. Dengan mengusulkan integrasi teknologi blockchain dan *differential privacy*, mereka mengisi kesenjangan dalam literatur dengan memberikan solusi yang komprehensif dan inovatif.

Table 1. Penelitian Transparansi dan Auditabilitas Data Pribadi dalam Layanan Berbasis Cloud yang Pernah dilakukan

Objek Penelitian	Metode yang Digunakan	Hasil Penelitian	Referensi
Pengembangan kerangka kerja HBDIAIM untuk manajemen data kota cerdas	Kombinasi analisis deskriptif dan pengembangan kerangka kerja baru	Pengembangan kerangka kerja *Holistic Big Data Integrated Artificial Intelligent Modeling* (HBDIAIM) untuk meningkatkan privasi dan keamanan dalam manajemen data kota cerdas.	Chen et al. (2021)
Penggunaan blockchain untuk transparansi pemrosesan data cloud	Kolaborasi interdisipliner antara ahli komputer dan ahli hukum sosial	Pengembangan teknologi peningkat privasi berbasis *blockchain* untuk meningkatkan transparansi dan kemampuan audit pemrosesan data pribadi dalam layanan berbasis *cloud*.	Llanos et al. (2023)
Konvergensi keamanan dan blockchain dengan Internet of Multimedia	Tinjauan komprehensif literatur	Identifikasi tantangan keamanan IoMT, potensi pemanfaatan *blockchain*, dan pengembangan kerangka teoritis untuk aplikasi multimedia di sektor kesehatan.	Jan et al. (2020)
Pengembangan sistem pengolahan data aman di komputasi perkotaan	Komputasi, blockchain dan differential	Pengembangan sistem pengolahan data yang aman menggunakan *blockchain* dan *differential privacy* untuk melindungi keamanan dan privasi data di komputasi perkotaan.	Heo & Doh (2024)

3. PENGGUNAAN METODE TERKAIT PRIVASI DAN KEAMANAN DATA LAYANAN *CLOUD*

Dalam studi yang dilakukan oleh Chen et al. (2021), peneliti menggunakan pendekatan konseptual dan kerangka kerja teoritis untuk mengatasi tantangan privasi dan keamanan data dalam konteks pengelolaan data kota cerdas. Fokus utama penelitian ini adalah pada pengembangan kerangka kerja konseptual yang bertujuan meningkatkan privasi dan keamanan data di kota cerdas. Namun, penelitian ini tidak melibatkan pengumpulan data empiris atau analisis, karena artikel tersebut lebih bersifat konseptual.

Sementara itu, Llanos et al. (2023) meneliti penggunaan *blockchain* dalam konteks pemrosesan data pribadi di layanan berbasis awan melalui proyek kolaboratif PACE. Dalam penelitian ini, penulis berfokus pada pengembangan teknologi blockchain untuk meningkatkan transparansi dan auditabilitas dalam pemrosesan data pribadi. Meskipun tidak menawarkan hasil penelitian empiris langsung, studi ini memberikan wawasan penting tentang arah masa depan dan tantangan yang terkait dengan implementasi blockchain dalam konteks privasi data.

Jan et al. (2020) melakukan analisis tren dan tantangan dalam keamanan dan blockchain dalam *Internet of Multimedia Things* (IoMT) melalui tinjauan literatur yang komprehensif. Penelitian ini bertujuan untuk memberikan pemahaman yang lebih baik tentang kerumitan dan peluang dalam domain IoMT. Meskipun bukan penelitian empiris, analisis ini memberikan wawasan kritis tentang tantangan keamanan yang unik yang dihadapi oleh ekosistem IoMT yang semakin kompleks.

Terakhir, Heo & Doh (2024) menggunakan metode eksperimen dengan pendekatan kuasi-eksperimental dalam pengembangan sistem pengolahan data berbasis *blockchain* dan *differential privacy* untuk meningkatkan keamanan dan privasi data dalam komputasi perkotaan. Penelitian ini memberikan informasi penting tentang kinerja dan keamanan solusi yang diusulkan, menawarkan wawasan konkret tentang efektivitas implementasi teknologi *blockchain* dan *differential privacy* dalam mengatasi tantangan privasi data di lingkungan perkotaan yang semakin terhubung.

Table 2. Metode Penelitian Keamanan Data Pada Layanan *Cloud*

Metode Penelitian	Objek yang Diteliti	Hasil Penelitian	Referensi
Pendekatan konseptual dan kerangka kerja teoritis	Pengembangan kerangka kerja konseptual untuk meningkatkan privasi dan keamanan data di kota cerdas	Tidak ada data empiris yang dikumpulkan atau analisis yang dilaporkan karena sifat konseptual artikel ini	Chen et al. (2021)
Proyek kolaboratif PACE untuk merancang teknologi peningkat privasi berbasis *blockchain*	Pengembangan teknologi *blockchain* untuk meningkatkan transparansi dan auditabilitas dalam pemrosesan data pribadi di layanan berbasis awan	Lebih menyoroti arah masa depan dan tantangan ketimbang hasil penelitian empiris	Llanos et al. (2023)
Tinjauan literatur/sistematik	Evaluasi tren dan tantangan dalam implementasi	Memberikan wawasan tentang tren dan	Jan et al. (2020)

Metode Penelitian	Objek yang Diteliti	Hasil Penelitian	Referensi
	keamanan dan *blockchain* dalam lingkungan IoMT	tantangan, bukan hasil penelitian empiris langsung	
Eksperimen dengan pendekatan kuasi-eksperimental	Pengembangan sistem pengolahan data berbasis *blockchain* dan *differential privacy* untuk meningkatkan keamanan dan privasi data dalam komputasi perkotaan	Melaporkan hasil dari eksperimen dan pengujian terhadap sistem yang dikembangkan	Heo & Doh (2024)

Tabel 2. di atas memberikan ringkasan singkat tentang empat penelitian yang relevan dalam domain privasi dan keamanan data. Penelitian pertama menggunakan pendekatan konseptual untuk mengembangkan kerangka kerja konseptual dalam meningkatkan privasi dan keamanan data di kota cerdas. Kedua, proyek kolaboratif PACE bertujuan merancang teknologi berbasis blockchain untuk meningkatkan transparansi dan auditabilitas dalam pemrosesan data pribadi di layanan awan. Penelitian ketiga adalah tinjauan literatur yang mengevaluasi tren dan tantangan dalam implementasi keamanan dan blockchain dalam lingkungan *Internet of Multimedia Things* (IoMT). Terakhir, penelitian keempat merupakan eksperimen dengan pendekatan kuasi-eksperimental yang bertujuan mengembangkan sistem pengolahan data berbasis blockchain dan differential privacy untuk meningkatkan keamanan dan privasi data dalam komputasi perkotaan.

4. KESIMPULAN

Hasil analisis metode penelitian dalam empat jurnal yang relevan, kita dapat melihat berbagai pendekatan yang digunakan dalam mempelajari isu-isu privasi dan keamanan data dalam konteks teknologi cerdas. Pertama, sebuah penelitian mengembangkan kerangka kerja konseptual untuk meningkatkan privasi dan keamanan data di kota pintar dengan mengintegrasikan pemodelan kecerdasan buatan dan big data. Temuan ini sejalan dengan fokus penelitian mereka dan memiliki implikasi luas dalam pengelolaan data kota pintar. Sebuah penelitian mengevaluasi penggunaan blockchain dalam layanan berbasis awan untuk meningkatkan transparansi dan auditabilitas dalam pemrosesan data pribadi. Temuan ini mendukung tujuan awal proyek PACE dan memiliki implikasi penting dalam meningkatkan privasi data dalam lingkungan cloud. Ketiga, sebuah artikel tidak menyajikan temuan empiris langsung, namun memberikan wawasan tentang tren dan tantangan dalam implementasi keamanan dan blockchain dalam *Internet of Multimedia Things* (IoMT). Meskipun tidak ada temuan langsung, tinjauan ini memberikan pemahaman yang mendalam tentang masalah yang relevan.

Penelitian yang telah dibahas diatas yang berhasil mengembangkan sistem pengolahan data berbasis blockchain dan differential privacy untuk meningkatkan keamanan dan privasi data dalam komputasi perkotaan. Temuan ini mendukung hipotesis awal mereka dan memberikan kontribusi penting dalam literatur tentang penggunaan teknologi baru

untuk melindungi data sensitif dalam lingkungan perkotaan yang semakin terhubung. Secara keseluruhan, analisis ini menyoroti berbagai pendekatan yang digunakan oleh peneliti untuk mengatasi tantangan privasi dan keamanan data dalam konteks teknologi cerdas. Meskipun setiap penelitian memiliki pendekatan dan fokus yang berbeda, mereka secara kolektif memberikan wawasan yang berharga dan menunjukkan arah yang menjanjikan untuk penelitian masa depan di bidang ini.

UCAPAN TERIMA KASIH

Kami ingin mengucapkan terima kasih kepada Institut Sains Teknologi dan Kesehatan 'Aisyiyah Kendari serta Institut Teknologi dan Sains Kolaka Utara atas dukungan, kerjasama, dan fasilitas yang telah mereka berikan, yang telah menjadi pendorong utama dalam menyelesaikan tulisan ini.

DAFTAR PUSTAKA

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. doi: 10.1109/COMST.2015.2444095

Alazab, M., & Vijayakumar, P. (2019). Zero-day malware detection based on supervised learning algorithms of API call signatures. In Applied Cyber Security and the Smart Grid (pp. 91-104). Auerbach Publications. doi: 10.1201/9780429057755-6

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805. doi: 10.1016/j.comnet.2010.05.010

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16). ACM. doi: 10.1145/2342509.2342513

Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. Microprocessors and Microsystems, 81, 103722. doi: 10.1016/j.micpro.2020.103722

Gia, T. N., Jiang, M., Rahmani, R., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2018). Fog computing in healthcare Internet of Things: A case study on ECG feature extraction. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 307-316). IEEE. doi: 10.1109/CIC.2018.00055

Heo, G., & Doh, I. (2024). Blockchain and differential privacy-based data processing system for data security and privacy in urban computing. Computer Communications, 222, 161-176. doi: 10.1016/j.comcom.2024.04.027

Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., ... & Watters, P. (2020). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. Journal of Network and Computer Applications, 102918. doi: 10.1016/j.jnca.2020.102918

Kaur, P., & Rani, R. (2018). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE. doi: 10.1109/ICCCNT.2018.8494176

Khan, F., Bashir, F., Maqsood, T., Khan, S., Khan, M. A., & Alazab, M. (2020). Blockchain and IoT-based Cognitive Industrial Framework for Smart Cities. IEEE Access, 8, 155759-155768. doi: 10.1109/ACCESS.2020.3019408

Khan, F., Jan, M. A., Alam, M., & Usman, M. (2019). An efficient data gathering scheme for Internet of multimedia Things. Mobile Networks and Applications, 24(4), 1105-1118. doi: 10.1007/s11036-018-1186-y

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In 2012 10th International Conference on Frontiers of Information Technology (pp. 257-260). IEEE. doi: 10.1109/FIT.2012.58

Llanos, J. T., Carr, M., & Rana, O. (2023). Using the blockchain to enable transparent and auditable processing of personal data in cloud-based services: Lessons from the Privacy-Aware Cloud Ecosystems (PACE) project. Computer Law & Security Review, 51, 105873. doi: 10.1016/j.clsr.2023.105873

Lu, C., Liu, Q., & Gu, Z. (2018). Fog computing in vehicular ad hoc networks: Challenges and approaches. Journal of Network and Computer Applications, 119, 71-85. doi: 10.1016/j.jnca.2018.07.015

Malhotra, S., & Singh, W. (2023). An efficacy analysis of data encryption architecture for cloud platform. Procedia Computer Science, 218, 989-1002. doi: 10.1016/j.procs.2023.01.079

Mastorakis, S., Mavromoustakis, C. X., Rodrigues, J. J., & Bourdena, A. (2019). Internet of multimedia things: Emerging trends and challenges. Mobile Networks and Applications, 24(1), 188-199. doi: 10.1007/s11036-018-1178-y

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. doi: 10.1016/j.adhoc.2012.02.016

Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., & Morrow, M. J. (2017). A comprehensive survey on fog computing: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 20(1), 416-464. doi: 10.1109/COMST.2017.2766685

Nastic, S., Sehic, S., & Dustdar, S. (2016). Microservices in the fog: A fog computing approach to the internet of things. IEEE Cloud Computing, 3(6), 76-83. doi: 10.1109/MCC.2016.134

Ray, P. P. (2016). Internet of things for smart agriculture: Technologies, practices and future direction. Journal of Ambient Intelligence and Humanized Computing, 7(6), 791-810. doi: 10.1007/s12652-015-0339-1

Sarkar, S., Misra, S., & Rodoplu, V. (2015). Smart data pricing: Economic solutions to data overcharging and under-provisioning. Cambridge University Press. doi: 10.1017/CBO9781316270192

Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: Scenarios and security issues. In 2014 Federated Conference on Computer Science and Information Systems (pp. 1-8). IEEE. doi: 10.15439/2014F233

Sun, Y., Song, H., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. IEEE Access, 4, 766-773. doi: 10.1109/ACCESS.2016.2526339

Usman, M., Jan, M. A., He, X., & Alam, M. (2017). Cryptography-based secure data storage and sharing using HEVC and public databases in IoT and cloud computing. Information Sciences, 387, 90-104. doi: 10.1016/j.ins.2016.10.005

Yannuzzi, M., Ganesan, S., & Aloqaily, M. (2021). Big data and IoT based smart urban mobility and transportation: a comprehensive review. Journal of Ambient Intelligence and Humanized Computing, 12(2), 2333-2357. doi: 10.1007/s12652-020-02182-0

Yi, S., Hao, Z., Qin, Z., Li, Q., & Mou, L. (2015). Fog computing: Platform and applications. In 2015 third IEEE workshop on hot topics in web systems and technologies (pp. 73-78). IEEE. doi: 10.1109/HotWeb.2015.22