Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 5550 – 5559 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

SYSTEMATIC LITERATURE REVIEW TERHADAP KERANGKA TATA KELOLA KEAMANAN DAN PRIVASI BERBASIS RISIKO PADA EKOSISTEM SMART CITY DAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

Agus Indra Cahaya, S.Kom[1], Taufik Fredy Kristianto, S.Kom[2], Prof. Dr. Aji Supriyanto, S.T., M.Kom[3]
Universitas Stikubank, Semarang
e-mail: [1]goeroeku@gmail.com, [2]fredytaufik@gmail.com, [3]ajisup@edu.unisbank.ac.id

Abstract: *This study aims to identify, evaluate, and synthesize risk-based security and privacy governance frameworks implemented in Smart City and Electronic-Based Government System (SPBE) ecosystems. The method used is a Systematic Literature Review (SLR) by adapting PRISMA guidelines on selected literature related to Smart City, e-Government, cybersecurity, privacy, Internet of Things (IoT), Big Data, and risk management. The literature extraction results indicate that the implementation of integrated security governance frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, ENISA guidelines, and risk-based evaluation models was identified as an important factor in improving information security maturity and mitigating privacy risks in digital public services. Furthermore, the increasing integration of IoT devices, Big Data platforms, and interconnected public service infrastructures introduces new security challenges that require comprehensive governance approaches. The findings indicate that successful Smart City and SPBE implementation requires integrated risk-based security and privacy governance frameworks. Furthermore, this study proposes a conceptual framework that may serve as an initial reference for developing secure, adaptive, and sustainable digital public services.*

Keyword: *Smart City; cybersecurity; privacy; risk management; Internet of Things; ISO/IEC 27001.*

Abstrak: Penelitian ini bertujuan mengidentifikasi, mengevaluasi, dan mensintesis kerangka tata kelola keamanan dan privasi berbasis risiko yang diterapkan pada ekosistem *Smart City* dan Sistem Pemerintahan Berbasis Elektronik (SPBE). Metode yang digunakan adalah *Systematic Literature Review* (SLR) dengan mengadaptasi pedoman PRISMA terhadap literatur terpilih yang membahas *Smart City*, *e-Government*, keamanan siber, privasi, *Internet of Things* (IoT), *Big Data*, dan manajemen risiko. Hasil ekstraksi literatur mengindikasikan bahwa penerapan kerangka tata kelola keamanan terintegrasi seperti *ISO/IEC 27001*, *NIST Cybersecurity Framework*, pedoman ENISA, serta model evaluasi berbasis risiko memiliki peran penting dalam meningkatkan kematangan keamanan informasi dan mitigasi risiko privasi pada layanan publik digital. Selain itu, meningkatnya integrasi perangkat *IoT*, platform *Big Data*, dan infrastruktur layanan publik yang saling terhubung menimbulkan tantangan keamanan baru yang memerlukan pendekatan tata kelola yang komprehensif. Penelitian ini juga menghasilkan suatu model konseptual tata kelola keamanan dan privasi berbasis risiko yang dapat dijadikan referensi awal dalam pengembangan layanan publik digital yang aman, adaptif, dan berkelanjutan.

Kata kunci: *Smart City*; keamanan siber; privasi; manajemen risiko; *Internet of Things*; *ISO/IEC 27001*.

PENDAHULUAN

Perkembangan Smart City dan

Sistem Pemerintahan Berbasis Elektronik (SPBE) telah menjadi pilar utama dalam modernisasi tata kelola administrasi publik di Indonesia (Indonesia, 2018). Transformasi ini mendorong digitalisasi tata kelola yang masif, termasuk pengelolaan arsip dinamis di berbagai tingkat pemerintahan (Jusniaty et al., 2025). Meskipun menjanjikan efisiensi tinggi, pergeseran menuju ekosistem pelayanan digital dihadapkan pada tantangan adaptasi sistem warisan (*legacy systems*) serta resistensi budaya birokrasi yang memengaruhi adopsi teknologi oleh masyarakat (Behera et al., 2023; Irani et al., 2023). Oleh karena itu, keberhasilan *e-Government* sangat bergantung pada tingkat kepercayaan publik (*public trust*) yang hanya dapat diraih melalui implementasi tata kelola layanan dan pengamanan infrastruktur yang sangat transparan (Preecha, 2025).

Masifnya pertukaran informasi pada arsitektur e-Government memunculkan profil risiko keamanan siber yang semakin kompleks. Tingginya integrasi layanan publik berbasis *Internet of Things* (IoT), *Big Data*, dan sistem yang saling terhubung menyebabkan ancaman keamanan dan pelanggaran privasi menjadi semakin kompleks. Kondisi tersebut juga dipengaruhi oleh kompleksitas arsitektur IoT yang menjadi fondasi utama berbagai layanan *Smart City modern* (Yaqoob et al., 2017). Kerentanan terhadap kebocoran data, akses tidak sah, serta eksploitasi perangkat IoT telah menjadi perhatian utama dalam pengembangan *Smart City modern* (Sicari et al., 2015; Zhang et al., 2017). Selain itu, karakteristik sistem yang terdistribusi menyebabkan satu titik kelemahan keamanan dapat berdampak terhadap keseluruhan ekosistem layanan publik yang terintegrasi (Roman et al., 2013). Oleh karena itu, penerapan pendekatan keamanan berbasis risiko yang komprehensif sangat direkomendasikan untuk memitigasi ancaman pada lingkungan *Smart City* dan *e-Government* (Alaba et al., 2017; Bhande, 2025). Proses evaluasi tingkat kematangan (*maturity level*) keamanan dan privasi harus diukur secara berkala menggunakan kerangka kerja (*framework*) berstandar internasional guna meminimalkan kerentanan layanan publik. Sebagai langkah preventif terhadap ancaman pada infrastruktur kritis dan perangkat *Internet of Things* (IoT), penerapan rekomendasi keamanan dasar (*baseline security*) menjadi penting (ENISA, 2020). Sejalan dengan hal tersebut, pemanfaatan kerangka kerja (ISO/IEC, 2022) telah menjadi standar global yang diperlukan untuk membangun sistem manajemen keamanan informasi yang andal. Studi oleh (Aminudin & Supriyanto, 2024) memvalidasi bahwa pengukuran risiko menggunakan pendekatan *NIST Cybersecurity Framework* (CSF) yang diintegrasikan dengan standar ISO/IEC terbukti tangguh untuk memetakan level pelindungan data. Lebih jauh, penanganan insiden siber dan manajemen kerentanan privasi juga perlu dimitigasi melalui prosedur penanganan bukti digital yang terstandardisasi menggunakan kerangka kerja NIST (Gunawan & Suryanto, 2022). Di tingkat nasional, penyelarasan instrumen evaluasi seperti Indeks Keamanan Informasi (KAMI) dengan standar global mampu meningkatkan akurasi pemetaan kematangan manajemen risiko pada pemerintah daerah (Sofyan et al., 2024; Supriyanto et al., 2025). Selain dari sisi keamanan siber, siklus operasional layanan teknologi informasi pemerintah juga harus diaudit secara menyeluruh menggunakan kerangka kerja IT *Service Management* seperti ITIL V4 agar penanganan insiden berjalan sistematis (Alfiqhyanto & Supriyanto, 2026; Sari et al., 2025). Selain itu, keberhasilan implementasi *Smart City* juga dipengaruhi oleh kesiapan arsitektur kota cerdas, tata kelola data, serta kemampuan pengelolaan *Big Data* yang aman dan berkelanjutan (Ahvenniemi et al., 2017; Anthopoulos, 2017; Chourabi et al., 2012; Hashem et al., 2016). Peningkatan volume data dan konektivitas perangkat juga memperluas permukaan serangan sehingga

membutuhkan mekanisme keamanan dan perlindungan privasi yang lebih adaptif pada lingkungan *Smart City modern* (Ferrag et al., 2017; Khatoun & Zeadally, 2016).

Selain tantangan pada infrastruktur, perangkat *IoT*, dan layanan digital yang saling terhubung, implementasi SPBE juga menghadapi tantangan pada pengelolaan dokumen elektronik sebagai bagian dari proses administrasi pemerintahan. Oleh karena itu, aspek keamanan tidak hanya perlu diterapkan pada infrastruktur teknologi, tetapi juga pada pengelolaan arsip digital dan sistem persuratan elektronik yang menjadi komponen penting layanan publik.

Saat ini, penerapan aplikasi SPBE nasional seperti SRIKANDI (Sistem Informasi Kearsipan Dinamis Terintegrasi) telah menjadi salah satu langkah penting dalam digitalisasi persuratan di berbagai instansi pemerintah daerah(Febrianto, 2023). Inovasi ini mendorong perubahan pengelolaan arsip dari sistem manual menuju platform digital terintegrasi yang lebih transparan dan efisien (Suprayitno et al., 2024). Pemanfaatan *Artificial Intelligence* dan *Natural Language Processing* juga mulai digunakan untuk mendukung otomasi dokumen persuratan, deteksi anomali, serta peningkatan akurasi klasifikasi dokumen digital (Damaryanti & Supriyanto, 2025; Putri & Handayani, 2025; Sofiyani et al., 2025).

Selain pemanfaatan *Artificial Intelligence*, penguatan keamanan dan integritas data juga memerlukan dukungan teknologi lain seperti *Blockchain*. Beberapa studi memperlihatkan bahwa integrasi *Blockchain* dengan infrastruktur *Smart City* berpotensi memperkuat mekanisme keamanan, transparansi, integritas data, dan akuntabilitas layanan publik melalui pencatatan transaksi yang terdistribusi dan sulit dimanipulasi (Tabuni et al., 2025; Wimal et al., 2025).

Berbagai penelitian sebelumnya telah membahas tata kelola keamanan informasi menggunakan standar seperti ISO/IEC 27001, NIST *Cybersecurity Framework*, ENISA, maupun Indeks KAMI secara terpisah sesuai dengan fokus masing-masing penelitian. Penelitian lain juga mengkaji keamanan *Internet of Things* (IoT), *Big Data*, *Blockchain*, serta pemanfaatan *Artificial Intelligence* dalam mendukung layanan Smart City dan SPBE. Meskipun demikian, belum banyak penelitian yang secara sistematis mengintegrasikan berbagai kerangka tata kelola, faktor risiko, dan teknologi pendukung tersebut ke dalam satu model konseptual yang dapat digunakan sebagai acuan implementasi keamanan dan privasi berbasis risiko pada ekosistem Smart City dan SPBE. Oleh karena itu, penelitian ini dilakukan melalui pendekatan *Systematic Literature Review* untuk mengidentifikasi, mengevaluasi, dan mensintesis berbagai hasil penelitian terdahulu sehingga diperoleh suatu kerangka konseptual tata kelola keamanan dan privasi berbasis risiko yang lebih terintegrasi.

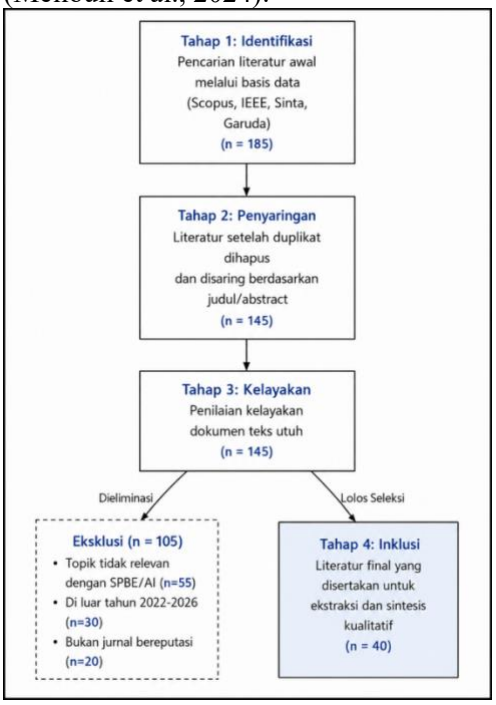
Berbeda dengan penelitian sebelumnya yang umumnya membahas standar keamanan informasi, tata kelola *Smart City*, implementasi SPBE, maupun penerapan teknologi seperti *Artificial Intelligence* dan *Blockchain* secara terpisah, penelitian ini memberikan kontribusi berupa sintesis berbagai kerangka tata kelola keamanan dan privasi berbasis risiko ke dalam suatu model konseptual yang terintegrasi. Model konseptual tersebut menggabungkan tahapan identifikasi risiko, penerapan kerangka tata kelola, pengendalian keamanan, operasional layanan, hingga luaran yang diharapkan dalam implementasi *Smart City* dan SPBE. Dengan demikian, hasil penelitian ini tidak hanya memetakan perkembangan penelitian terdahulu, tetapi juga menyediakan kerangka konseptual yang dapat dijadikan referensi awal bagi pengembangan tata kelola keamanan dan privasi pada layanan publik digital.

METODE

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
August 2026, IX (4): 5550 – 5559 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Penelitian ini menggunakan pendekatan kualitatif dengan metode *Systematic Literature Review* (SLR). SLR merupakan metode tinjauan literatur yang dilakukan secara sistematis, terstruktur, dan transparan untuk mengidentifikasi, mengevaluasi, serta mensintesis temuan-temuan dari berbagai penelitian terdahulu yang relevan dengan pertanyaan penelitian (Albahri et al., 2023; Paul et al., 2021; Snyder, 2019).

Pelaksanaan SLR dalam penelitian ini secara khusus diformulasikan mengikuti panduan standar *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). Alur sistematis dari tahapan pencarian hingga penyeleksian literatur berdasarkan kerangka kerja PRISMA tersebut secara lengkap diilustrasikan pada Gambar 1. Penggunaan metode SLR dengan kerangka PRISMA telah terbukti efektif untuk memetakan tren penelitian, mengevaluasi praktik, dan memberikan rekomendasi yang presisi, khususnya dalam ruang lingkup tata kelola Sistem Pemerintahan Berbasis Elektronik (SPBE) maupun layanan teknologi informasi (Mellouli et al., 2024).



Gambar 1 Diagram Alir PRISMA

Pengumpulan data pada penelitian ini dilakukan dengan metode penelusuran pangkalan data digital (*database searching*). Sumber literatur utama ditarik dari jurnal nasional terakreditasi melalui portal SINTA (*Science and Technology Index*) serta portal Garuda (Garba Rujukan Digital), didukung oleh pangkalan data internasional bereputasi (Puspitaningrum, 2025). Pencarian artikel dilakukan menggunakan kombinasi kata kunci (*search string*) yang disesuaikan dengan rumusan masalah. Kata kunci yang digunakan dalam penelusuran meliputi kombinasi: *("Smart City" OR "E-Government") AND ("Security Governance" OR "Cybersecurity" OR "Privacy") AND ("Risk Management" OR "ISO 27001" OR "NIST" OR "IoT" OR "Big Data"*).

Tabel 1 Kriteria Inklusi dan Eksklusi

Kriteria	Inklusi	Eksklusi
Tahun Terbit	2022–2026 (Kecuali landasan teori pokok dan regulasi).	Sebelum tahun 2022 (Kecuali untuk literatur sekunder).
Jenis Literatur	Jurnal ilmiah internasional (*Scopus/IEEE*), jurnal nasional (SINTA), prosiding, dan dokumen regulasi resmi.	Laporan hibah lokal yang tidak terindeks, artikel opini, dan blog tidak resmi.
Fokus Topik	Tata kelola keamanan (*NIST, ISO/IEC 27001, Indeks KAMI*), Smart City, Cybersecurity, Privacy, Risk Management, IoT, Big Data, NIST, ISO/IEC 27001, dan tata kelola keamanan informasi.	Topik di luar ruang lingkup SPBE, *Smart City*, atau tata kelola layanan TI.
Bahasa	Bahasa Indonesia dan Bahasa Inggris.	Bahasa selain Indonesia

dan Inggris.

Data kualitatif yang diperoleh dari artikel-artikel yang telah lolos tahap seleksi PRISMA kemudian disintesis untuk menjawab *Research Questions*. Analisis kualitatif pada penelitian ini mengadaptasi model interaktif dari Miles dan Huberman, yang terdiri atas tiga kategori dan langkah pada pengolahan data kualitatif, antara lain *data reduction* (reduksi data), *data display* (penyajian data), serta *conclusion drawing and verification* (penarikan kesimpulan) (Miles et al., 2014). Selain itu, untuk memastikan keabsahan dan relevansi dokumen arsip digital yang diekstraksi, penelitian ini juga mengadopsi tinjauan berbasis formative multifaceted evaluation dari perspektif pengguna sistem (Matusiak, 2022).

HASIL DAN PEMBAHASAN

Berdasarkan proses ekstraksi literatur menggunakan panduan PRISMA, sejumlah studi utama (*primary studies*) yang relevan telah diseleksi untuk menjawab pertanyaan penelitian terkait kerangka tata kelola keamanan, privasi, dan implementasi teknologi pada ekosistem *Smart City* dan Sistem Pemerintahan Berbasis Elektronik (SPBE). Sintesis dari literatur terpilih disajikan ke dalam matriks ekstraksi literatur pada Tabel 2 untuk memetakan kerangka kerja yang dominan digunakan.

Tabel 2 Sintesis Literatur Kerangka Tata Kelola Keamanan dan Privasi (n=40)

Penulis	Framework Tata Kelola	Temuan Utama
Supriyanto et al. (2019)	*Multi-layer Security*	Tata kelola keamanan *e-Government*
Aminudin & Supriyanto (2024)	*NIST* + *ISO/IEC 2700*	Evaluasi kematangan risiko TI
Bhande (2025)	*Federated Learning*	Perlindungan privasi *IoT*
Damaryanti & Supriyanto (2025)	*XGBoost* + *OC-SVM*	Deteksi anomali SRIKANDI
Supriyanto et al. (2025)	Indeks KAMI	Evaluasi maturitas keamanan
Zhang et al. (2017)	*Security Architecture*	Ancaman *Smart City*
Alfiqhyanto & Supriyanto (2026)	ITIL V4	Tata kelola layanan TI
Tabuni et al. (2025)	*Blockchain*	Integritas data *Smart City*

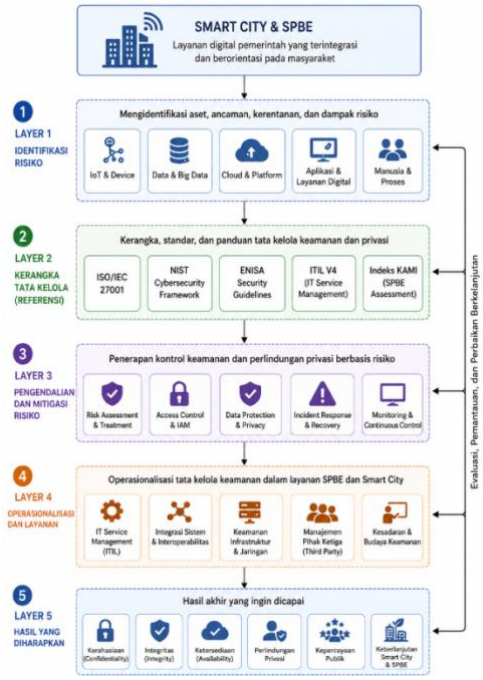
Untuk menjawab RQ2, hasil sintesis menunjukkan bahwa faktor risiko utama pada ekosistem *Smart City* dan SPBE meliputi kebocoran data, kelemahan autentikasi perangkat *IoT*, serangan *Denial of Service* (DoS), anomali data, kelemahan tata kelola layanan TI, serta meningkatnya permukaan serangan akibat integrasi *Big Data* dan layanan digital. Temuan tersebut menunjukkan bahwa risiko keamanan tidak hanya berasal dari aspek teknologi, tetapi juga dipengaruhi oleh tata kelola organisasi, proses operasional, serta kesiapan sumber daya manusia dalam mengelola layanan digital. Oleh karena itu, pendekatan keamanan berbasis risiko perlu diterapkan secara menyeluruh agar setiap risiko dapat diidentifikasi, dievaluasi, dan dikendalikan sesuai tingkat dampaknya terhadap layanan publik.

Untuk menjawab RQ3, hasil sintesis berbagai literatur kemudian dirumuskan ke dalam model konseptual tata kelola keamanan dan privasi berbasis risiko pada *Smart City* dan SPBE. Model ini menempatkan identifikasi risiko sebagai tahap awal sebelum organisasi menerapkan berbagai kerangka tata kelola seperti *ISO/IEC 27001*, *NIST Cybersecurity Framework*, *ENISA*, ITIL V4, dan Indeks KAMI. Integrasi berbagai kerangka tersebut selanjutnya diarahkan untuk mendukung pengendalian keamanan, perlindungan privasi, operasional layanan, serta peningkatan

kualitas layanan publik digital.

Model konseptual tersebut selanjutnya diberi nama **Risk-Based Security and Privacy Governance Framework for Smart City and SPBE** sebagai representasi hasil sintesis utama penelitian ini.

Penyusunan model konseptual tersebut didasarkan pada pola yang konsisten pada berbagai penelitian terdahulu. Hampir seluruh literatur menempatkan identifikasi risiko sebagai fondasi utama sebelum organisasi menentukan kerangka tata kelola yang sesuai. Selanjutnya, penerapan berbagai *framework* keamanan berfungsi sebagai dasar dalam membangun mekanisme pengendalian keamanan, perlindungan privasi, serta operasional layanan secara berkelanjutan. Oleh karena itu, model konseptual yang dihasilkan tidak hanya merepresentasikan hasil sintesis literatur, tetapi juga menggambarkan keterkaitan logis antar komponen tata kelola keamanan berbasis risiko pada implementasi *Smart City* dan SPBE.



Gambar 2 Risk-Based Security and Privacy Governance Framework for Smart City and SPBE

Penelitian ini memiliki keterbatasan karena hanya menggunakan pendekatan *Systematic Literature Review* tanpa melakukan validasi empiris terhadap model konseptual yang dihasilkan. Selain itu, sintesis literatur dibatasi pada artikel yang memenuhi kriteria inklusi sehingga kemungkinan masih terdapat penelitian relevan di luar rentang waktu maupun basis data yang digunakan.

SIMPULAN

Berdasarkan hasil identifikasi, evaluasi, dan sintesis terhadap 40 artikel yang memenuhi kriteria inklusi, penelitian ini menunjukkan bahwa implementasi tata kelola keamanan dan privasi pada ekosistem *Smart City* dan Sistem Pemerintahan Berbasis Elektronik (SPBE) didominasi oleh penerapan kerangka kerja seperti *ISO/IEC 27001*, *NIST Cybersecurity Framework*, ITIL V4, *ENISA*, serta Indeks KAMI. Hasil sintesis juga menunjukkan bahwa berbagai kerangka tersebut saling melengkapi dalam mendukung identifikasi risiko, penerapan pengendalian keamanan, operasional layanan, hingga peningkatan kepercayaan publik terhadap layanan digital.

Lebih lanjut, hasil sintesis menunjukkan bahwa meningkatnya integrasi *Internet of Things* (IoT), *Big Data*, dan layanan digital pemerintah memperluas berbagai risiko keamanan dan privasi sehingga memerlukan pendekatan tata kelola berbasis risiko yang lebih komprehensif. Penerapan teknologi pendukung seperti *Artificial Intelligence*, *Blockchain*, dan *Federated Learning* juga dilaporkan berpotensi memperkuat keamanan, transparansi, dan efisiensi layanan publik, khususnya pada implementasi aplikasi SPBE seperti SRIKANDI.

Hasil sintesis tersebut selanjutnya dirumuskan ke dalam sebuah model konseptual tata kelola keamanan dan privasi berbasis risiko yang mengintegrasikan identifikasi risiko, penerapan kerangka tata kelola, pengendalian keamanan, operasional

layanan, serta luaran implementasi *Smart City* dan SPBE sebagai kontribusi utama penelitian ini.

Model konseptual yang dihasilkan diharapkan dapat menjadi referensi awal bagi pemerintah, akademisi, maupun peneliti dalam merancang tata kelola keamanan dan privasi berbasis risiko yang lebih adaptif terhadap perkembangan ekosistem *Smart City* dan SPBE di masa mendatang.

DAFTAR PUSTAKA

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., & Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities*, *60*, 234–245. https://doi.org/10.1016/j.cities.2016.09.009

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Albahri, A. S., Duhaim, A. M., Fadhel, M. A., Alnoor, A., Baqer, N. S., Alzubaidi, L., Albahri, O. S., Alamoodi, A. H., Bai, J., Salhi, A., Santamaría, J., Ouyang, C., Gupta, A., Gu, Y., & Deveci, M. (2023). A systematic review of trustworthy and explainable artificial intelligence in healthcare: Assessment of quality, bias risk, and data fusion. *Information Fusion*, *96*, 156–191. https://doi.org/10.1016/j.inffus.2023.03.008

Alfiqhyanto, D., & Supriyanto, A. (2026). ANALISA EVALUASI DAN PERANCANGAN MANAJEMEN LAYANAN TI PADA PEMERINTAH DAERAH MENGGUNAKAN FRAMEWORK ITIL V4. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *10*(1), 1168–1175. https://doi.org/10.36040/jati.v10i1.16956

Aminudin, A., & Supriyanto, A. (2024). Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah). *AITI*, *21*(2), 210–229. https://doi.org/10.24246/aiti.v21i2.210-229

Anthopoulos, L. (2017). Smart utopia VS smart reality: Learning by experience from 10 smart city cases. *Cities*, *63*, 128–148. https://doi.org/10.1016/j.cities.2016.10.005

Behera, R. K., Bala, P. K., Rana, N. P., & Irani, Z. (2023). Responsible natural language processing: A principlist framework for social benefits. *Technological Forecasting and Social Change*, *188*, 122306. https://doi.org/10.1016/j.techfore.2022.122306

Bhande, A. (2025). A Systematic Review of Data Security and Privacy-Preserving Models for Smart Cities and Edge Computing Environments. *EPJ Web of Conferences*, *341*, 1024. https://doi.org/10.1051/epjconf/202534101024

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012). Understanding Smart Cities: An Integrative Framework. *2012 45th Hawaii International Conference on System Sciences*, 2289–2297. https://doi.org/10.1109/HICSS.2012.615

Damaryanti, F., & Supriyanto, A. (2025). Optimization of the SRIKANDI E-Government System Using XGBoost-Based Classification and One-Class SVM Anomaly DetectionType. *Information Technology International Journal*, *3*(1). https://doi.org/10.33005/itij.v3i1.50

ENISA. (2020). *Guidelines for Securing the Internet of Things: Secure Supply*

Chain for IoT. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Febrianto, F. A. (2023). *Implementasi program aplikasi Srikandi (Sistem informasi kearsipan dinamis terintegrasi) pada Dinas Perpustakaan dan Kearsipan Kota Salatiga*. Universitas Terbuka.

Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, *2017*, 1–41. https://doi.org/10.1155/2017/6562953

Gunawan, C. T. A., & Suryanto, Y. (2022). Maturity Level Analysis of Digital Evidence Handling on Integrated Criminal Justice System based on NIST SP800-53 Revision 5 Using NIST Maturity. *Budapest International Research and Critics Institute (BIRCI-Journal)*. https://doi.org/10.33258/birci.v5i2.4861

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, *36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Indonesia, P. P. R. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. In *Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia*.

Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. *Government Information Quarterly*, *40*(1), 101784. https://doi.org/10.1016/j.giq.2022.101784

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

Jusniaty, J., Nurmiati, N., Wahid, A., Fitriani, F., & Rosnita, R. (2025). Digital Transformation In Local Government: Implementation Of Integrated Dynamic Archive Information System (Srikandi) At Village Level In Indonesia. *International Conference of Business, Education, Health, and Scien-Tech*, *2*(1), 1073–1082.

Khatoun, R., & Zeadally, S. (2016). Smart cities. *Communications of the ACM*, *59*(8), 46–57. https://doi.org/10.1145/2858789

Matusiak, K. K. (2022). Evaluating a digital community archive from the user perspective: The case of formative multifaceted evaluation. *Library \& Information Science Research*, *44*(3), 101159. https://doi.org/10.1016/j.lisr.2022.101159

Mellouli, S., Janssen, M., & Ojo, A. (2024). Introduction to the Issue on Artificial Intelligence in the Public Sector: Risks and Benefits of AI for Governments. *Digital Government: Research and Practice*, *5*(1), 1–6. https://doi.org/10.1145/3636550

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, *45*(4). https://doi.org/10.1111/ijcs.12695

Preecha, J. (2025). CYBERSECURITY AND PUBLIC TRUST IN DIGITAL GOVERNANCE: FOCUSING ON CITIZEN TRUST. *Proceeding of International Conference on Social Science and Humanity*, *2*(2), 26–37.

https://doi.org/10.61796/icossh.v2i2.27

Puspitaningrum, A. C. (2025). Systematic Literature Review: Implementasi ITSM pada Perguruan Tinggi di Indonesia: Tren Penelitian, Praktik dan Rekomendasi. *JURNAL TECNOSCIENZA*, *10*(1), 169–184.

Putri, N. A., & Handayani, N. S. (2025). Efektivitas Penggunaan Sistem Srikandi dalam Pengelolaan Arsip Dinamis di Dinas Perpustakaan dan Kearsipan Kabupaten Tulungagung. *Librarium: Library and Information Science Journal*, *2*(2), 75–90. https://doi.org/10.53088/librarium.v2i2.1987

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Sari, D. P., Amaliana, I., Nugraha, L., Seftiawan, S., & Dzulfikar, H. (2025). Evaluasi manajemen layanan teknologi informasi dengan framework ITIL V4 pada sistem e-presensi BKPSDM Kabupaten Ciamis. *Jurnal Ilmiah Informatika (JIMI)*, *10*(2), 112–125.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sofiyani, Z., Suprayitno, S., Fahmi, F., & Mahadewi, M. P. (2025). Toward Transparent Bureaucracy: NLP-Based Document Classification and Power Dynamics in the SRIKANDI System. *Proceedings from the Document Academy*, *12*(2). https://doi.org/10.35492/docam/12/2/10

Sofyan, H., Kaswidjanti, W., & Ilmiyah, L. S. (2024). *Information Security Index (ISI) 4.2 for Information Security Evaluation (Case Study: Sleman Regency Communication and Informatics Office)* (pp. 188–200). https://doi.org/10.2991/978-94-6463-366-5_18

Supriyanto, A., Jananto, A., Razaq, J. A., Hartono, B., & Damaryanti, F. (2025). Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation. *Cybernetics and Information Technologies*, *25*(2), 173–192. https://doi.org/10.2478/cait-2025-0018

Wimal, K., Cullen, G., & Donovan, J. (2025). Blockchain-Driven Smart Cities: Review of Key Applications and Emerging Trends. *2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)*, 1–8. https://doi.org/10.1109/ICAISC64594.2025.10959451

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, *24*(3), 10–16. https://doi.org/10.1109/MWC.2017.1

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM