JIM: Jurnal Ilmu Multidisiplin
E-ISSN : 2829-4580
P-ISSN : 2829-4599
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/jim.v5i1

Analisis Risiko Keamanan pada Infrastruktur Internet of Things (IoT) yang Potensial Diterapkan dalam Smart City Kupang

Bonie Empy Giri[1]
[1]Universitas Citra Bangsa, Indonesia, bonieangi28@gmail.com

Corresponding Author: bonieangi28@gmail.com[1]

Abstract: *Implementation of Smart City in various parts of the world shows great potential in improving the quality of urban life. However, the adoption of Internet of Things (IoT) technology as the backbone of Smart City also brings complex security challenges. This paper provides a comprehensive analysis of various inherent security risks in IoT infrastructure potentially implemented within the context of Kupang Smart City. This study identifies critical cyber threats such as Denial of Service (DoS)/Distributed Denial of Service (DDoS), data injection and manipulation, device hijacking, botnet creation, as well as data privacy breaches and illegal surveillance. The vulnerability analysis covers technical aspects (devices, networks, data) and non-technical aspects (policies, human resources, user awareness). A qualitative risk analysis approach is used to identify threats, analyze vulnerabilities, and propose mitigation strategies. The results of this research are expected to provide guidance for the Kupang city government and related stakeholders in designing and implementing a secure and resilient Smart City infrastructure.*

Keywords*: Internet of Things (IoT), Cybersecurity, Smart City, Risk Analysis, Kupang*

Abstrak: Penerapan Kota Cerdas di berbagai belahan dunia menunjukkan potensi besar dalam meningkatkan kualitas hidup perkotaan. Namun, penerapan teknologi Internet of Things (IoT) sebagai tulang punggung Kota Cerdas juga menghadirkan tantangan keamanan yang kompleks. Makalah ini menyajikan analisis komprehensif mengenai berbagai risiko keamanan yang melekat pada infrastruktur IoT yang berpotensi diterapkan dalam konteks Kota Cerdas Kupang. Studi ini mengidentifikasi ancaman siber kritis seperti Denial of Service (DoS)/Distributed Denial of Service (DDoS), injeksi dan manipulasi data, pembajakan perangkat, pembentukan botnet, serta pelanggaran privasi data dan pengawasan ilegal. Analisis kerentanan mencakup aspek teknis (perangkat, jaringan, data) dan aspek non-teknis (kebijakan, sumber daya manusia, kesadaran pengguna). Pendekatan analisis risiko kualitatif digunakan untuk mengidentifikasi ancaman, menganalisis kerentanan, dan mengusulkan strategi mitigasi. Hasil penelitian ini diharapkan dapat memberikan panduan bagi pemerintah Kota Kupang dan pemangku kepentingan terkait dalam merancang dan mengimplementasikan infrastruktur Kota Cerdas yang aman dan tangguh.

Kata Kunci: Internet of Things (IoT), Cybersecurity, Smart City, Risk Analysis, Kupang

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi tata kelola perkotaan melalui konsep *Smart City*, yang bertujuan meningkatkan kualitas hidup masyarakat, efisiensi pelayanan publik, serta keberlanjutan pembangunan. Salah satu komponen utama dalam implementasi *Smart City* adalah *Internet of Things* (IoT), yaitu teknologi yang memungkinkan berbagai perangkat fisik, sensor, dan sistem saling terhubung serta bertukar data secara real time. Pemanfaatan IoT dalam konteks perkotaan mencakup berbagai sektor strategis, seperti sistem transportasi cerdas, pengawasan keamanan melalui CCTV, pengelolaan infrastruktur kota, serta pemantauan lingkungan. Studi menunjukkan bahwa integrasi teknologi berbasis IoT mampu mendukung pengelolaan keamanan kota secara lebih responsif dan partisipatif, terutama ketika didukung oleh peran aktif masyarakat sebagai bagian dari elemen *smart people* dalam ekosistem *Smart City* (Akbar et al., 2024; Budiman & Satria, 2020).

Seiring dengan meningkatnya adopsi IoT, *Smart City* juga berkembang menuju pemanfaatan teknologi lanjutan seperti *Big Data* dan kecerdasan buatan (*Artificial Intelligence*) untuk mendukung pengambilan keputusan berbasis data secara cepat dan akurat (Irfan Fajri et al., 2025). Integrasi teknologi-teknologi tersebut memperkuat kemampuan pemerintah kota dalam mengelola sumber daya dan layanan publik. Namun, kompleksitas sistem yang semakin tinggi juga berimplikasi pada meningkatnya risiko keamanan siber. Infrastruktur IoT terdiri atas beragam perangkat dengan keterbatasan sumber daya komputasi, protokol komunikasi yang bervariasi, serta keterhubungan yang masif, sehingga memperluas *attack surface* dan meningkatkan kerentanan terhadap serangan siber.

Berbagai penelitian menegaskan bahwa tantangan keamanan, privasi, dan keselamatan merupakan isu fundamental dalam pengembangan *Smart City*. Ancaman seperti pencurian data, serangan *Denial of Service* (DoS), manipulasi data sensor, serta pengambilalihan kendali perangkat IoT dapat berdampak langsung pada stabilitas layanan kota dan keselamatan warga (Elmaghraby & Losavio, 2014). Selain itu, pengelolaan data dalam skala besar yang mencakup data pribadi masyarakat menimbulkan risiko serius terkait perlindungan privasi dan penyalahgunaan informasi apabila tidak disertai dengan mekanisme keamanan yang memadai (Ilhami, 2022). Oleh karena itu, aspek keamanan dan privasi tidak dapat dipisahkan dari perencanaan dan implementasi *Smart City*.

Kota Kupang sebagai ibu kota Provinsi Nusa Tenggara Timur tengah berupaya mengadopsi konsep *Smart City* melalui berbagai inisiatif digital untuk meningkatkan kualitas pelayanan publik dan tata kelola pemerintahan. Implementasi teknologi IoT dalam konteks ini menjadi kebutuhan strategis, namun juga membawa potensi risiko keamanan yang harus dikelola secara sistematis. Literatur menunjukkan bahwa tanpa analisis risiko yang komprehensif, penerapan teknologi *Smart City* justru dapat memperbesar kerentanan sistem dan menurunkan tingkat kepercayaan publik (Rana & Dwivedi, 2020). Oleh karena itu, diperlukan pendekatan analisis risiko keamanan siber yang mampu mengidentifikasi ancaman utama, mengevaluasi tingkat kerentanan infrastruktur IoT, serta merumuskan strategi mitigasi yang sesuai dengan karakteristik lokal dan mengacu pada standar internasional.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis risiko keamanan pada infrastruktur IoT yang potensial diterapkan dalam *Smart City* Kupang. Penelitian ini diharapkan dapat memberikan gambaran menyeluruh mengenai ancaman keamanan siber yang paling kritis, tingkat kerentanan sistem IoT baik dari aspek teknis maupun non-teknis, serta rekomendasi strategi mitigasi berbasis risiko yang realistis dan terukur untuk mendukung terwujudnya *Smart City* Kupang yang aman, andal, dan berkelanjutan.

METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode utama berupa studi literatur (*literature review*). Pendekatan ini dipilih karena mampu memberikan pemahaman yang komprehensif dan mendalam terhadap isu keamanan siber yang bersifat kompleks dan multidimensional, khususnya dalam konteks implementasi Internet of Things (IoT) pada lingkungan *Smart City*. Melalui kajian literatur, penelitian ini berupaya mengkaji konsep, temuan empiris, serta kerangka teoretis yang relevan untuk mengidentifikasi risiko keamanan yang potensial dan strategi mitigasinya.

Pengumpulan data dilakukan melalui studi pustaka dengan menelusuri dan menganalisis berbagai sumber data sekunder yang kredibel dan relevan. Sumber-sumber tersebut meliputi jurnal ilmiah nasional dan internasional yang membahas keamanan IoT, *Smart City*, serta risiko dan privasi data, seperti karya Rana dan Dwivedi (2020), Ilhami (2022), serta Elmaghraby dan Losavio (2014). Selain itu, penelitian ini juga memanfaatkan laporan penelitian dan *white paper* dari organisasi global, antara lain National Institute of Standards and Technology (NIST) yang menyediakan kerangka kerja keamanan siber berbasis risiko, serta Open Web Application Security Project (OWASP) yang merilis daftar OWASP IoT Top 10 sebagai rujukan utama dalam identifikasi ancaman. Dokumen kebijakan dan regulasi nasional, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), turut dianalisis sebagai landasan hukum dalam perlindungan data pada sistem berbasis IoT. Selain itu, studi kasus penerapan *Smart City* berbasis IoT di beberapa kota, baik di Indonesia maupun di luar negeri, digunakan sebagai pembanding kontekstual untuk menilai kesiapan dan tantangan yang relevan dengan kondisi Kota Kupang.

Data yang diperoleh dianalisis menggunakan metode analisis tematik dengan cara mengidentifikasi, mengelompokkan, dan menginterpretasikan tema-tema utama yang muncul dari literatur. Analisis diawali dengan mengidentifikasi dan mengklasifikasikan berbagai jenis ancaman keamanan siber berdasarkan pola serangan, target, serta dampaknya terhadap infrastruktur IoT, dengan mengacu pada temuan literatur dan kerangka OWASP IoT Top 10. Selanjutnya, dilakukan analisis kerentanan yang mencakup aspek teknis, seperti perangkat, jaringan, protokol komunikasi, dan pengelolaan data, serta aspek non-teknis, meliputi sumber daya manusia, kebijakan, tata kelola, dan tingkat kesadaran pengguna. Pendekatan holistik dalam analisis kerentanan ini mengacu pada kerangka interaksi risiko keamanan *Smart City* yang dikembangkan oleh Rana dan Dwivedi (2020). Berdasarkan hasil identifikasi ancaman dan analisis kerentanan tersebut, penelitian ini merumuskan rekomendasi strategi mitigasi berbasis risiko dengan mengadaptasi standar internasional, seperti NIST Cybersecurity Framework dan OWASP, serta mempertimbangkan karakteristik geografis, sosial, dan infrastruktur Kota Kupang.

Untuk menjaga validitas dan kredibilitas data, penelitian ini menerapkan triangulasi sumber dengan membandingkan temuan dari berbagai literatur dan dokumen yang berbeda guna memastikan konsistensi informasi. Selain itu, pendekatan logikal-koherensif digunakan untuk memastikan adanya keselarasan antara ancaman yang diidentifikasi, kerentanan yang dianalisis, dan strategi mitigasi yang diusulkan, sehingga hasil penelitian dapat dipertanggungjawabkan secara ilmiah dan relevan dengan konteks implementasi *Smart City* Kupang.

HASIL DAN PEMBAHASAN

4.1 Identifikasi dan Klasifikasi Ancaman Keamanan Siber Kritis pada Infrastruktur IoT Smart City Kupang

Ancaman keamanan siber pada infrastruktur IoT Smart City di Kupang dapat dikategorikan berdasarkan sifat serangan dan targetnya. Berdasarkan tinjauan literatur dan

karakteristik ekosistem IoT, ancaman paling kritis yang harus diwaspadai adalah sebagai berikut:

1. **Serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS):** Ancaman ini bertujuan untuk mengganggu ketersediaan layanan dengan membanjiri sistem atau jaringan dengan lalu lintas palsu, membuatnya tidak dapat diakses oleh pengguna yang sah. Dalam konteks Smart City Kupang, serangan DDoS dapat melumpuhkan sistem vital seperti kontrol lalu lintas pintar, sistem penerangan jalan, atau bahkan layanan darurat berbasis IoT. Mengingat ketergantungan Smart City pada ketersediaan data *real-time* dan operasional tanpa henti, serangan DoS/DDoS pada infrastruktur kunci (misalnya, platform pusat data kota, *gateway* komunikasi IoT) dapat menyebabkan disrupsi layanan publik yang parah, kemacetan, atau bahkan membahayakan keselamatan jiwa jika sistem darurat terpengaruh.
2. **Injeksi dan Manipulasi Data (*Data Tampering*):** Ancaman ini melibatkan penyisipan data palsu atau modifikasi data asli yang dikirimkan oleh perangkat IoT. Tujuannya adalah untuk menyesatkan sistem dan memicu tindakan yang salah. Jika data sensor di Smart City Kupang dimanipulasi (misalnya, data kualitas udara yang dimanipulasi untuk menunjukkan kondisi aman padahal berbahaya, atau data volume sampah yang salah), keputusan yang diambil oleh sistem otomatis atau petugas kota akan keliru, berdampak langsung pada kesehatan masyarakat, efisiensi operasional, dan kepercayaan publik.
3. **Pembajakan Perangkat (*Device Hijacking*) dan Pembuatan Botnet:** Penyerang berhasil menguasai kendali perangkat IoT yang rentan dan menggunakannya untuk tujuan jahat, seringkali sebagai bagian dari *botnet* besar untuk melancarkan serangan siber lainnya. Perangkat IoT yang tersebar luas di lingkungan kota (lampu pintar, kamera CCTV, sensor lingkungan) dapat menjadi target utama. Jika perangkat ini dibajak, mereka bisa digunakan untuk memata-matai, melancarkan serangan DoS ke target lain, atau bahkan menjadi *pivot* untuk masuk lebih dalam ke jaringan infrastruktur vital kota. Kerentanan umum seperti kata sandi *default* yang lemah atau *firmware* yang tidak diperbarui menjadi pintu masuk utama.
4. **Pelanggaran Privasi Data dan Pengawasan Ilegal:** Ancaman ini berfokus pada pengumpulan, akses, atau penyalahgunaan data pribadi yang dikumpulkan oleh perangkat IoT tanpa persetujuan subjek data. Ini termasuk data lokasi, pola perilaku, atau informasi sensitif lainnya. Dengan penerapan Smart City, perangkat IoT akan mengumpulkan volume data yang sangat besar tentang pergerakan warga, penggunaan fasilitas, dan kebiasaan. Tanpa perlindungan privasi yang kuat, data ini rentan disalahgunakan untuk pengawasan massal yang tidak sah, profilasi individu, atau bahkan dijual ke pihak ketiga, yang dapat menimbulkan kekhawatiran etika dan hukum yang serius bagi masyarakat Kupang.

4.2. Analisis Tingkat Kerentanan Infrastruktur IoT di Kupang melalui Pendekatan Holistik

Analisis kerentanan infrastruktur IoT di Kupang harus mempertimbangkan baik aspek teknis maupun non-teknis untuk memberikan gambaran yang komprehensif. Pendekatan holistik ini memastikan bahwa tidak hanya celah dalam teknologi yang diidentifikasi, tetapi juga kelemahan dalam proses, kebijakan, dan sumber daya manusia.

4.2.1. Kerentanan Teknis

a. **Perangkat IoT yang Tidak Aman Secara *Default*:** Banyak perangkat IoT komersial dirancang dengan prioritas fungsionalitas dan biaya rendah, seringkali mengabaikan keamanan sebagai fitur inti. Ini termasuk penggunaan *credential default* yang tidak pernah diubah, tidak adanya mekanisme *update firmware* yang aman, atau port terbuka yang tidak perlu. Dalam konteks Kupang, pengadaan perangkat yang tidak memenuhi standar keamanan dasar ini dapat menjadi sumber kerentanan masif.

b. **Jaringan Komunikasi yang Rentan:** Ketergantungan pada jaringan nirkabel (Wi-Fi publik, seluler, LoRaWAN) yang kurang terenkripsi atau tanpa autentikasi yang kuat akan membuka celah untuk penyadapan data (*sniffing*) dan serangan *man-in-the-middle*.
c. **Platform dan Aplikasi dengan Celah Keamanan:** Jika *platform cloud* atau aplikasi Smart City dibangun tanpa mengikuti praktik *secure coding* atau tanpa audit keamanan rutin, kerentanan umum seperti SQL injection, Broken Authentication, atau *misconfiguration* dapat dieksploitasi. Kurangnya segmentasi jaringan dan kontrol akses yang tidak memadai pada *platform* pusat juga akan memperburuk risiko.
d. **Keterbatasan Sumber Daya Perangkat:** Perangkat IoT seringkali memiliki daya komputasi dan memori yang terbatas, membuat implementasi algoritma enkripsi yang kuat atau fitur keamanan kompleks menjadi sulit atau tidak efisien.

4.2.2. Kerentanan Non-Teknis

1. **Keterbatasan Sumber Daya Manusia (SDM) dan Keahlian:** Ketersediaan tenaga ahli keamanan siber yang kompeten di Kupang, khususnya yang memahami seluk-beluk keamanan IoT, mungkin masih terbatas. Kurangnya pelatihan dan kesadaran keamanan di antara personel pengelola infrastruktur Smart City dapat menyebabkan kesalahan konfigurasi atau respons insiden yang lambat.
2. **Kurangnya Kebijakan dan Regulasi yang Jelas:** Tanpa kerangka kebijakan dan regulasi yang kuat mengenai pengadaan IoT, standar keamanan minimum, dan pengelolaan data, implementasi IoT dapat berjalan tanpa arah yang jelas, meninggalkan celah risiko. Ini termasuk kebijakan privasi data yang belum matang atau tidak terimplementasi dengan baik.
3. **Anggaran dan Prioritas:** Alokasi anggaran yang tidak memadai untuk keamanan siber IoT dapat menghambat investasi pada teknologi keamanan yang diperlukan, *penetration testing* rutin, dan program pelatihan SDM. Prioritas yang terlalu fokus pada fungsionalitas dan implementasi cepat tanpa mempertimbangkan keamanan dapat meningkatkan eksposur risiko.
4. **Ketergantungan pada Vendor:** Ketergantungan yang tinggi pada vendor tunggal tanpa diversifikasi atau klausul keamanan yang ketat dalam kontrak dapat menimbulkan *vendor lock-in* dan risiko jika vendor tersebut memiliki praktik keamanan yang buruk atau bangkrut.

4.3. Pengembangan Rekomendasi Strategi Mitigasi Berbasis Risiko yang Relevan dan Terukur

Strategi mitigasi risiko yang efektif untuk Smart City Kupang harus didasarkan pada analisis risiko di atas, mempertimbangkan karakteristik unik Kupang, mengacu pada standar internasional, dan dapat diimplementasikan secara terukur.

4.3.1.Mempertimbangkan Karakteristik Unik Infrastruktur Kupang

a. **Prioritas pada Keamanan Perangkat *Edge*:** Mengingat banyaknya perangkat IoT yang tersebar di area publik Kupang, fokus harus diberikan pada pengamanan perangkat di level *edge*. Ini berarti pemilihan perangkat harus ketat, dengan kriteria keamanan bawaan yang kuat (misalnya, *secure boot*, *hardware root of trust*), dan mekanisme *over-the-air (OTA) update* yang aman dan otomatis.
b. **Adaptasi Jaringan Komunikasi Lokal:** Pertimbangkan penggunaan teknologi komunikasi yang paling efisien dan aman sesuai kondisi geografis Kupang (misalnya, LoRaWAN untuk area luas, seluler untuk *bandwidth* tinggi) dengan memastikan enkripsi *end-to-end* yang kuat pada setiap saluran komunikasi, sesuai dengan kapasitas jaringan lokal.

c. **Pelatihan SDM Lokal:** Fokus pada pengembangan kapasitas SDM lokal di Kupang melalui program pelatihan dan sertifikasi khusus keamanan IoT, bekerja sama dengan universitas lokal atau lembaga pelatihan vokasi. Ini akan menciptakan keahlian yang berkelanjutan dan mengurangi ketergantungan pada tenaga ahli dari luar.

4.3.2,Sesuai dengan Standar Internasional

1) **Adopsi Kerangka Keamanan NIST:** Pemerintah Kota Kupang dapat mengadopsi dan mengadaptasi *NIST Cybersecurity Framework* (CSF) atau *NIST Special Publication 800-213: IoT Device Cybersecurity Guidance* sebagai panduan utama. Kerangka ini menyediakan pendekatan berbasis risiko untuk mengelola keamanan siber, mencakup fungsi Identify, Protect, Detect, Respond, dan Recover.
2) **Penerapan Rekomendasi OWASP IoT Top 10:** Pedoman OWASP IoT Top 10 dapat digunakan sebagai daftar periksa (*checklist*) untuk mengidentifikasi dan mengatasi kerentanan umum pada perangkat dan aplikasi IoT.
3) **Pematuhan Regulasi Privasi Data (UU PDP):** Pastikan seluruh implementasi IoT mematuhi Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022. Ini berarti adanya mekanisme persetujuan yang jelas untuk pengumpulan data, hak subjek data, dan penunjukan Pejabat Pelindungan Data Pribadi (DPO).

4.3.3. Terukur dalam Implementasi

1. **Pendekatan Bertahap (*Phased Approach*):** Implementasikan langkah-langkah keamanan secara bertahap, dimulai dengan risiko paling kritis yang memiliki dampak tertinggi dan probabilitas tinggi. Contoh: Memprioritaskan pengamanan pada sistem transportasi cerdas sebelum sistem yang dampaknya lebih rendah.
2. **Indikator Kinerja Utama (KPI) Keamanan:** Tetapkan KPI yang jelas untuk mengukur efektivitas mitigasi, seperti:
   a. Persentase perangkat IoT yang telah diperbarui *firmware*-nya secara berkala.
   b. Jumlah insiden keamanan yang berhasil dicegah atau dideteksi.
   c. Waktu rata-rata untuk merespons insiden keamanan (*Mean Time To Respond/MTTR*).
   d. Tingkat kepatuhan terhadap kebijakan keamanan internal.

KESIMPULAN

Analisis risiko keamanan pada infrastruktur Internet of Things (IoT) yang berpotensi diterapkan dalam Smart City Kupang menunjukkan bahwa meskipun IoT menawarkan peluang transformatif untuk peningkatan layanan publik, efisiensi operasional, dan kualitas hidup, implementasinya juga dihadapkan pada serangkaian ancaman keamanan siber kritis. Ancaman-ancaman seperti Denial of Service (DoS)/Distributed Denial of Service (DDoS), injeksi dan manipulasi data, pembajakan perangkat (*device hijacking*) dan pembuatan *botnet*, serta pelanggaran privasi data dan pengawasan ilegal memiliki potensi untuk melumpuhkan sistem vital, mengganggu layanan esensial, dan merusak kepercayaan publik.

Tingkat kerentanan infrastruktur IoT di Kupang tidak hanya berasal dari aspek teknis—seperti perangkat yang tidak aman secara *default*, jaringan komunikasi yang rentan, serta platform dan aplikasi dengan celah keamanan—tetapi juga dari aspek non-teknis. Keterbatasan sumber daya manusia dan keahlian lokal, absennya kebijakan dan regulasi yang jelas, serta alokasi anggaran yang belum memadai untuk keamanan siber, menjadi faktor-faktor krusial yang memperbesar risiko.

Oleh karena itu, pengembangan strategi mitigasi berbasis risiko yang relevan dan terukur adalah sebuah keharusan. Strategi ini harus mempertimbangkan karakteristik unik infrastruktur Kupang, mengutamakan keamanan pada level *edge* (perangkat), mengadaptasi

teknologi komunikasi lokal, dan berinvestasi pada peningkatan kapasitas sumber daya manusia lokal. Adopsi kerangka kerja keamanan siber internasional seperti NIST Cybersecurity Framework dan OWASP IoT Top 10, serta kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP), akan menjadi pilar utama dalam membangun pertahanan siber yang kuat. Implementasi harus dilakukan secara bertahap, dengan penetapan indikator kinerja utama (KPI) yang jelas untuk memantau efektivitas mitigasi.

REFERENSI

Akbar, D. N., Saladin, S., Dewantara, K. S., & Darmawan, I. (https://www.google.com/search?q=2024). Optimalisasi peran smart people dalam pengelolaan keamanan kota melalui implementasi CCTV sebagai pilar smart city. *Triwikrama: Jurnal Ilmu Sosial*, 6(1), 110-120. (DOI: 10.6578/triwikrama.v6i1.8094)

Budiman, A., & Satria, H. (2020). Pemanfaatan IoT untuk Keamanan Perkotaan dalam Konsep Smart City: Studi Kasus di Jakarta. *Jurnal Sistem dan Teknologi*, 12(1), 78-90.

Elmaghraby, A., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491–497.

Ilhami, D. A. S. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, 2(1), 51–60. (DOI: 10.20885/snati.v2i1.19)

Irfan Fajri, T., Rahayu, N., Eldo, H., Chrisnawati, G., & Shaulita, R. (2025). Integrasi Big Data dan AI untuk Pengambilan Keputusan dalam Smart City. *Jurnal Teknologi Informasi dan Komunikasi*, 9(2), 783–789.

Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Interaction Framework. *Information Systems Frontiers*. (DOI: 10.1007/%0As10796-020- 10044-1)