The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 6, December 2024
https://doi.org/10.33022/ijcs.v13i6.4524

Identifikasi Tren Risiko Keamanan Siber dan Mitigasinya dalam Pembangunan *Smart city*

Yoga Adi Pratama[1], Dana Indra Sensuse[2], Franky Juhar[3]
yoga.adi22@ui.ac.id[1], dana@cs.ui.ac.id[2,], franky.juhar@ui.ac.id[3]
[1,2,3] Fakultas Ilmu Komputer, Universitas Indonesia

Informasi Artikel

Diterima : 30 Nov 2024
Direvisi : 10 Des 2024
Disetujui : 30 Des 2024

Kata Kunci

smart city, keamanan siber, tren dan mitigasi keamanan siber, TOE

Abstrak

Pembangunan *smart city* Ibu Kota Nusantara (IKN) menghadirkan tantangan baru dalam menjaga keamanan siber. Penelitian bertujuan untuk mengidentifikasi tren risiko keamanan siber sekaligus mitigasi risiko keamanan siber pada *smart city* dengan menggunakan metodologi *Systematic Literature Review* (SLR). *Framework* TOE *(Technology, Organization, Environtment*) digunakan untuk menghasilkan daftar risiko keamanan siber yang komprehensif berdasarkan kategori teknologi, organisasi, dan lingkungan. Hasil penelitian menunjukkan terdapat 58 risiko keamanan siber yang didominasi oleh risiko keamanan siber teknologi yaitu 81%. Mitigasi risiko keamanan siber dikelompokkan juga berdasarkan kategori teknologi, organisasi dan lingkungan. Standar internasional ISO 27002: 2022 digunakan sebagai metode validasi kontrol keamanan atas mitigasi risiko yang diidentifikasi sebagai bentuk *best practice*. Hasil penelitian ini memberikan rekomendasi kepada pemerintah dalam menyusun kebijakan keamanan dengan mendorong penggunaan kriptografi secara efektif, menyelaraskan dengan standar kebijakan yang aman dan audit berkala, serta selalu meningkatkan kualitas SDM keamanan siber sehingga dapat membantu pengembangan *smart city* IKN yang aman dan berkelanjutan.

Keywords

Smart city, cybersecurity, cybersecurity risks and trends, TOE

Abstract

The development of the Ibu Kota Nusantara (IKN) as a smart city introduces new challenges in maintaining cybersecurity. This research aims to identify cybersecurity risk trends and mitigation strategies in smart cities using a Systematic Literature Review methodology. The TOE framework (Technology, Organization, Environment) is employed to generate a comprehensive list of cybersecurity risks categorized TOE. The results show 58 cybersecurity risks, with technology-related risks dominating at 81%. Cybersecurity mitigation strategies are also categorized based on TOE. The international standard ISO 27002:2022 is used as a method to validate security controls for identified risk mitigations as a form of best practice. This research provides recommendations to the government for developing security policies by promoting the effective use of cryptography, aligning with secure policy standards and periodic audits, and continuously improving the quality of cybersecurity human resources to support the development of a secure and sustainable IKN smart city.

A. Pendahuluan

Presiden Republik Indonesia, Joko Widodo telah mengumumkan pemindahan Ibu Kota Negara Indonesia ke wilayah Provinsi Kalimantan Timur tepatnya di Kutai Kertanegara dan Penajam Paser Utara. Ibu Kota Negara Indonesia yang baru bernama Nusantara yang selanjutnya dikenal sebagai Ibu Kota Nusantara (IKN) [1]. Pembangunan Ibu Kota Nusantara diharapkan menjadi katalisator pertumbuhan ekonomi Indonesia di masa mendatang, dengan mengedepankan inovasi dan daya saing di berbagai aspek seperti teknologi, arsitektur, tata kota, dan sosial. Pemerintah Republik Indonesia tengah mengembangkan Ibu Kota Nusantara sebagai sebuah kota cerdas (*smart cities*) yang mengoptimalkan penggunaan teknologi informasi dan komunikasi untuk menciptakan lingkungan yang efisien dan nyaman bagi pemerintahan, bisnis, dan masyarakat [2].

Smart city adalah sebuah kota yang memadukan kebijakan dan teknologi untuk meningkatkan kemampuan masyarakatnya. Peningkatan yang dimaksud antara lain tata kelola pemerintahan yang baik, layanan masyarakat yang lebih baik, peningkatan ekonomi dan pendidikan, serta kesetaraan sosial bagi seluruh masyarakat [3]. *Smart city* seharusnya bisa lebih aktif melibatkan masyarakat dalam menghasilkan ide-ide cerdas, produk, ataupun layanan untuk meningkatkan kualitas hidup masyarakat ataupun mengoptimalkan pemanfaatan infrastruktur teknologi dan informasi. [4]. Dalam pengembangannya, *smart city* harus mengunci faktor pengembangan kota dengan baik. Faktor pengembangan *smart city* paling penting adalah teknologi, termasuk pembangunan infrastruktur, layanan data terbuka, dan ketersediaan sumber daya informasi [5]. Infrastruktur yang baik diharapkan dapat melibatkan IoT, teknologi sensor, dan komputasi awan untuk mengimplementasikan *smart city* yang saling terhubung [6].

Infrastruktur *smart city* yang saling terhubung menjadi konsep yang sangat menjanjikan namun menawarkan peluang terjadinya serangan siber [6].dan meningkatkan risiko ancaman keamanan jaringan dengan kerentanan utama termasuk antarmuka yang tidak aman, *firmware* yang belum dilakukan *patch* dan enkripsi yang tidak memadai [7]. Pembangunan kota cerdas atau *smart city*, khususnya Ibu Kota Nusantara membutuhkan strategi keamanan siber yang kuat dan kokoh. Strategi keamanan dikembangkan berdasarkan faktor-faktor yang terkait dengan teknologi, manusia, dan institusi, dengan fokus pada penerapan strategi keamanan siber untuk mendukung pengembangan *smart city* [8].

Keamanan siber adalah aspek penting dalam teknologi informasi modern karena membantu melindungi data sensitif, program, *file*, dan perangkat lunak dari akses tidak sah dan potensi bahaya dari penyerang siber yang mencakup pencurian data, gangguan sistem, atau kegiatan berbahaya lainnya [9]. Keamanan siber untuk *smart city* mencakup kombinasi teknologi yang muncul untuk menghadapi tantangan yang sangat kompleks dari perangkat dan jaringan yang tidak aman, yang dapat menyebabkan serangan yang tidak terbatas [10].

Pemerintah telah menerbitkan sebuah kebijakan tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber yang melibatkan semua stakeholder untuk menerapkan keamanan siber nasional [11]. Pembangunan konsep *smart city* di Ibu Kota Nusantara tidak boleh mengabaikan strategi keamanan siber untuk mengantisipasi ancaman serangan siber, seperti *malware*, *phising, ransomware, brute force attack,* dan lainnya. Pada tahun 2024, Indonesia dihebohkan dengan

insiden siber. Setelah kasus serangan peretasan Pusat Data Nasional Sementara (PDNS) KOMINFO pada Juli 2024, Indonesia juga dihadapkan pada kasus kebocoran data 6 juta Wajib Pajak dari DJP. Ini menunjukkan kelemahan Indonesia dalam manajemen risiko dan perlu dilakukan manajemen terhadap risiko.

Risiko keamanan siber adalah risiko kerugian finansial, gangguan operasional, atau kerusakan reputasi suatu organisasi akibat pelanggaran sistem teknologi informasinya karena serangan eksternal. Contoh risiko keamanan siber antara lain kehilangan data sensitif, gangguan pada jaringan, sistem, dan layanan perusahaan, serta kerusakan fisik elektronik [12]. Jenis pengendalian keamanan yang digunakan untuk keamanan siber mirip dengan keamanan informasi; namun, digunakan untuk mengurangi risiko keamanan siber di dunia maya, seperti kejahatan siber dan keselamatan [13].

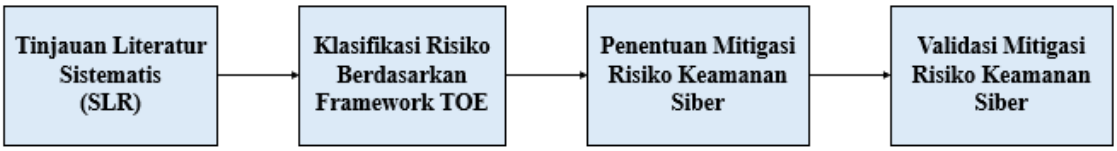
Risiko perlu dilakukan identifikasi melalui kategori risiko berdasarkan beragam risiko yang muncul dari *smart city*. Salah satu studi menyebutkan bahwa risiko dikategorikan dalam teknologi, organisasi, dan eksternal, dengan kontribusi risiko teknologi secara siginfikan berpengaruh terhadap tata kelola [6]. Standar internasional lain juga menjelaskan konsep manajemen terhadap risiko secara umum terdiri dari penentuan konteks dan *scope*, *risk assessment* (yang terdiri dari *risk identification, risk analysis, dan risk evaluation*) *serta risk treatment* [14] [15] [16] [17].

Manajemen risiko merupakan suatu pendekatan sistematis yang mempertimbangkan konteks organisasi secara menyeluruh, meliputi faktor internal seperti budaya organisasi dan perilaku individu, serta faktor eksternal seperti kondisi pasar dan regulasi. ISO 31000: 2018 menjelaskan proses manajemen risiko dan pelaksanaannya selalu memadukan penggunaan standar internasional lainnya seperti ISO 27001: 2022, ISO 27002: 2022, dan ISO 27005: 2018. ISO 27001: 2022, sebagai standar untuk Sistem Manajemen Keamanan Informasi (SMKI), menyajikan persyaratan spesifik untuk membangun, menerapkan, memelihara, dan meningkatkan SMKI. ISO 27002: 2022, sebagai kode praktik, memberikan panduan tentang kontrol keamanan informasi yang dapat diimplementasikan dalam SMKI. Sementara itu, ISO 27005: 2018 memberikan panduan terperinci mengenai proses manajemen risiko keamanan informasi, mulai dari identifikasi hingga penanganan risiko. Dengan demikian, keempat standar ini membentuk suatu sistem yang terintegrasi untuk memastikan keamanan informasi dalam organisasi.

Penelitian ini bertujuan untuk mengidentifikasi tren ancaman siber dan mitigasi risiko keamanan siber dalam pembangunan *Smart city* di Ibu Kota Nusantara yang dilakukan melalui tinjauan literatur sistematis. Tinjauan Literatur Sistematis (SLR) adalah metode studi literatur yang terstruktur dan terencana berdasarkan pada hasil penelitian tertentu [18]. Tujuan dari tinjauan literatur sistematis ini bukan hanya mengumpulkan bukti-bukti terkait pertanyaan penelitian, tetapi juga untuk mengusulkan mitigasi risiko yang komprehensif dengan dengan mempertimbangkan faktor teknologi, organisasi, dan lingkungan, khususnya di *smart city.* Hasil penelitian ini memberikan rekomendasi kepada pemerintah dalam menyusun kebijakan keamanan siber sehingga dapat membantu pengembangan *smart city* IKN yang aman dan berkelanjutan.

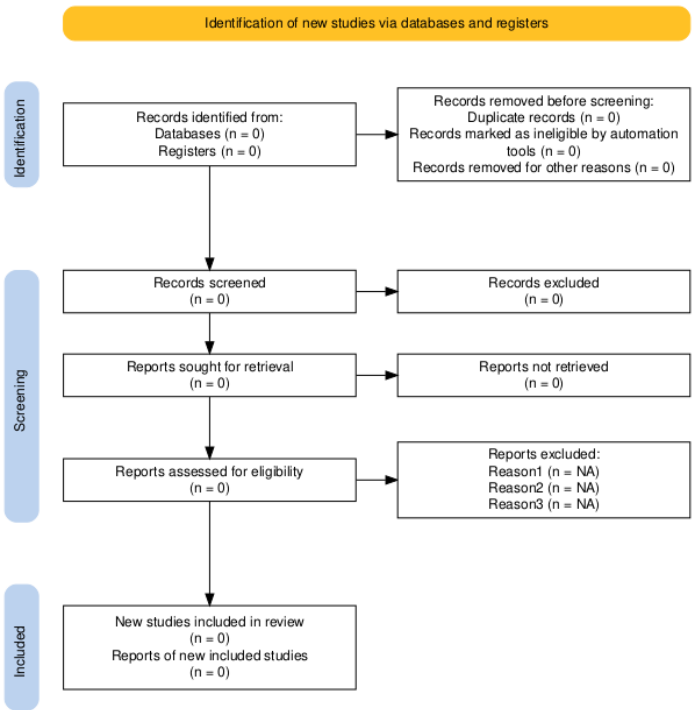
B. Metode Penelitian

Penelitian disusun melalui empat tahapan yaitu Tinjauan Literatur Sistematis (SLR), Klasifikasi risiko berdasarkan kerangka kerja TOE (*Technology, Organization, Environtment),* Penentuan mitigasi risiko keamanan siber, dan Validasi mitigasi risiko keamanan siber. Tahapan penelitian ini disusun untuk menjawab pertanyaan penelitian yaitu (1) Apa saja tren risiko keamanan siber di lingkungan *smart city*? (2) Apa saja mitigasi risiko keamanan siber yang perlu harus diterapkan dalam pengembangan *Smart city* khususnya di Ibu Kota Negara (IKN)?



Gambar 1. Metodologi Penelitian

Tinjauan Literatur Sistematis atau *Systematic Literature Review* (SLR) dilakukan untuk mencari literatur secara komprehensif dan terstruktur. Metode ini melibatkan serangkaian langkah yang ketat, mulai dari perumusan pertanyaan penelitian, pencarian literatur, seleksi artikel, ekstraksi data, hingga sintesis temuan. Peneliti mengikuti pedoman protokol P*referred Reporting Items for Systematic reviews and Meta-Analyses* (PRISMA) untuk memastikan kualitas dan transparansi dalam proses tinjauan literatur. Data berupa referensi paper dilakukan pencarian secara sistematis melalui prsoes *identification* menggunakan database *Journal* dan *Conference*, kemudian dilakukan inklusi dan eksklusi data sesuai dengan konteks penelitian melalui proses *screening* hingga didapatkan penelitian dengan kriteria terbaik sesuai penelitian untuk dilakukan ekstraksi data dan sistensis temuan.



Gambar 2. Proses SLR menggunakan PRISMA

Pada tahap identifikasi awal, pencarian literatur dilakukan dengan menggunakan kata kunci dan kriteria yang telah ditetapkan dalam kriteria pencarian menggunakan protokol PRISMA pada Tabel 1.

Tabel 1. Kriteria Pencarian Literatur

Atribut	Deskripsi
Kata kunci	*(risk AND management) AND cybersecurity AND ((smart AND city) AND TOE OR (ISO AND 31000))*
Tipe publikasi	*Journal Article* dan *Conference Proceedings*
Tahun	2020 to 2024
Bahasa	Bahasa Inggris
Subjek	*Cybersecurity, smart city, risk assessment, risk management, iso standards*
Database	Scopus, IEEE Xplore, ProQuest, ScienceDirect

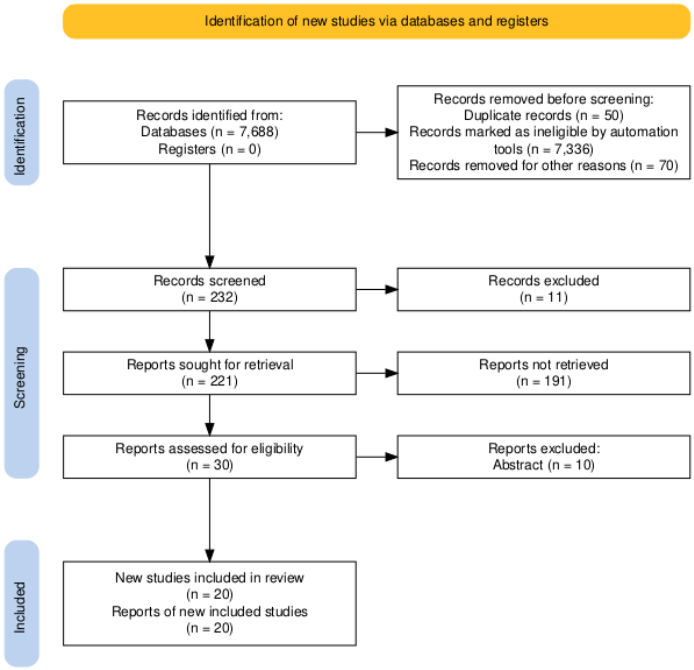
Tahap selanjutnya adalah klasifikasi risiko keamanan siber berdasarkan *framework* TOE. Setelah proses SLR dan ekstraksi data selesai dilakukan, risiko keamanan yang teridentifikasi kemudian diklasifikasikan berdasarkan kategori teknologi, organisasi, dan lingkungan. Setelah terpetakan, tahap selanjutnya adalah menambahkan mitigasi risiko keamanan siber sesuai dengan hasil pencarian dan klasifikasi TOE. Hasil identifikasi risiko dan mitigasi terhadap risiko keamanan siber kemudian dilakukan validasi menggunakan kontrol risiko yang terdapat dalam ISO 27002: 2022 untuk memeriksa kesesuaian data yang dihasilkan penelitian dibandingkan dengan *best practice.*

C. Hasil dan Pembahasan

Bab Hasil dan pembahasan dijelaskan menjadi lima subbab yaitu hasil pengumpulan data menggunakan SLR protokol PRISMA, Tren Risiko Keamanan Siber, Klasifikasi Risiko Keamanan Siber, Mitigasi Risiko Keamanan Siber, dan Validasi Mitigasi Risiko Keamanan Siber.

1. Tinjauan Literatur Sistematis

Proses SLR menggunakan protokol PRISMA dilakukan untuk memastikan kualitas dan transparansi dalam proses tinjauan literatur. Dari tahap identifikasi awal, ditemukan 7688 artikel dari pencarian pada Scopus, IEEE Xplore, ScienceDirect dan ProQuest dengan menggunakan kata kunci. Hasil ini kemudian dipersempit dengan menghilangkan penelitian duplikasi (50 penelitian) dan menghilangkan penelitian yang tidak masuk kriteria menggunakan autom*ation tools* yaitu bukan *Journal* dan/atau *Conference Proceedings*, bukan penelitian pada tahun 2020-2024, dan bukan penelitian dengan penulisan bahasa inggris (7406 penelitian). Tahap selanjutnya menghilangkan penelitian dengan subjek yang tidak sama dengan penelitian penulis dan penelitian yang tidak *Open Access/Full Text* (202 penelitian). Tahap akhir adalah menghilangkan penelitian dengan abstrak yang tidak sesuai dengan penelitian penulis (10 penelitian). Dengan demikian didapatkan penelitian untuk diekstraksi data adalah 20 penelitian.



Gambar 3. Hasil SLR protokol PRISMA

2. Tren Risiko Keamanan Siber

Tren risiko keamanan siber dilakukan identifikasi melalui beberapa penelitian rujukan yang telah dilakukan reviu. Tren ini menjadi sangat beragam dikarenakan kompleks dan canggihnya teknologi yang akan diterapkan pada *smart city* nantinya. Pada pelaksanannya, pembangunan *smart city* lebih banyak memanfaatkan (dengan tidak mengesampingkan manusia dan juga lingkungan) teknologi. Berbagai inovasi teknologi selalu berkembang seiring dengan berjalannya waktu.

Penelitian ini melakukan studi literatur berdasarkan teknik SLR sehingga menghasilkan 20 penelitian terdahulu dan serupa yang ditunjukkan dalam Tabel 2.

Tabel 2. Penelitian Terdahulu

Judul Penelitian	Referensi
Risk management in sustainable smart cities governance: A TOE framework	[6]
Blue Seaports: The Smart, Sustainable and Electrified Ports of the Future	[19]
Context-Based and Adaptive Cybersecurity Risk Management Framework	[20]
Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk	[21]
E-Governance in Smart cities: Global Trends and Key Enablers	[22]
Factors of Risk Analysis for IoT Systems	[23]
From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden	[24]
Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments	[25]
Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools	[26]
Leveraging cyber threat intelligence for a dynamic risk framework	[27]
On the Identification, Evaluation and Treatment of Risks in Smart Homes A Systematic Literature Review	[28]
PRISM a strategic decision framework for cybersecurity risk assessment	[29]

Judul Penelitian	Referensi
Robotics cyber security vulnerabilities, attacks, countermeasures, and recommendations	[30]
The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity A Case Study of Greece	[31]
Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network	[32]
Hybrid quantum architecture for smart city security	[33]
Improved sand cat swarm optimization with deep learning based enhanced malicious activity recognition for cybersecurity	[34]
Optimizing risk mitigation: A simulation-based model for detecting fake IoT clients in smart city environments	[35]
Role of net-zero renewable-based transportation systems in smart cities toward enhancing cultural diversity Realistic model	[36]
Towards a sustainable built environment industry in Singapore: Drivers, barriers, and strategies in the adoption of smart facilities management	[37]

Pada penelitian [19], membahas mengenai jenis risiko yang mungkin dapat masuk ke dalam lingkungan Pelabuhan Pintar seperti kerentanan terhadap serangan siber atas penggunaan 5G dan *Digital Twin*, potensi kerusakan barang dan orang, risiko keamanan, privasi, dan distribusi fungsi jaringan data *real time*, risiko bagi integritas dan keselamatan operasional, risiko aksesibilitas fisik seperti CCTV dan RFID, serta risiko terkait dengan akurasi dan keamanan data.

Penelitian [20] menyelidiki penerapan nilai berisiko dalam domain *cyber*, memperkenalkan konsep nilai *cyber at risk* (CY-Var) untuk mengukur risiko *cyber* dan mendukung keputusan investasi keamanan. Dari hasil penelitian ditemukan beberapa risiko yang muncul seperti kerentanan aset, kegagalan dalam mengidentifikasi ancaman, kerentanan sistem, serangan siber, kegagalan dalam memahami konsekuensi dari serangan siber, serta kegagalan dalam memantau risiko secara berkelanjutan.

Dalam penelitian lain, [21] mengidentifikasi beberapa risiko yang mungkin terjadi di masa mendatang. Risiko tersebut seperti perkembangan teknologi yang cepat, evolusi teknik serangan, ketergantungan pada sistem, perubahan regulasi dan persaingan, kemudian sumber ancaman seperti *hacker* dan kelompok kriminal. Selain itu, penelitian [22] mengidentifikasi risiko ke dalam beberapa jenis yaitu seperti serangan siber, pelanggaran data, ancaman infrastruktur yang mendukung *e-governance*, ketergantungan secara berlebihan terhadap teknologi, visi pimpinan yang kurang kuat dan kurang jelas, perbedaan budaya, tingkat literasi digital yang beragam, faktor penerimaan masyarakat terhadap teknologi, stabilitas politik, korupsi, dan perubahan kebijakan pemerintah.

Selanjutnya, penelitian [23] melakukan identifikasi risiko ke dalam beberapa jenis diantaranya kelemahan pada perangkat IoT, kuantitas perangkat yang tinggi sejalan dengan luasnya area serangan siber, interkoneksi yang kompleks, kurangnya SDM dalam mengelola risiko keamanan, tantangan organisasi dalam mengadopsi metodologi manajemen risiko, kurangnya kerangka kerja tata kelola yang jelas untuk keamanan IoT, ketergantungan pada sistem eksternal dan interkoneksi yang luas, kurangnya regulasi yang jelas dan standar keamanan IoT yang buruk, serta perubahan cepat dalam teknologi dan lanskap ancaman.

Kemudian, penelitian [24] membagi risiko ke dalam beberapa jenis yaitu kerentanan *cloud*, konfigurasi yang tidak tepat, kurangnya keahlian dalam

mengelola risiko keamanan *cloud* di dalam organisasi, proses bisnis yang tidan efisien, budaya keamanan yang tidak kuat, risiko pihak ketiga atau penyedia, serta ancaman dari luar organisasi seperti serangan siber yang ditargetkan.

Penelitian [31] mengidentifikasi risiko keamanan siber seperti *natural disaster*, *cyberattack*, dan *economic fluctuation*. Penelitian [30] lebih menonjolkan risiko keamanan siber secara teknologi yang meliputi *Wireless jamming, Reconnaissance and scanning, Information disclosure, Information disclosure, Information gathering, Information interception, Physical damage, Service disruption or denial, Sabotage and espionage, Security and system flaws, Back-doors, Remote-access, Device theft, Fake applications, Insecure backup and data storage, Battery constraints, Inaccurate activity threshold, Nature's disruption*.

Pada penelitian lain, [29] mengidentifikasi risiko seperti *Loss or Theft of Equipment, Malware and Viruses, Data Breaches, dan Phising Attacks*. Penelitian [28] hampir sama mengidentifikasikan risiko yaitu seperti *Theft, Waste of resources, Privacy Risk, Performance Risk, Depedence Risk, Access to technology risk, Social Isolation Risk, Legal Risk, Time Risk, Fire, Water Damage, Property Damage*. Di sisi lain, penelitian [25] melakukan penelitian dengan mengkombinasikan beberapa standar internasional untuk mengidentifikasi risiko sehingga dihasilkan risiko seperti *Malicious executable File, Malicious email, Malicious URL, Suspicious Domain Name System,* dan *Phising*. Penelitian lain, [26] dan [27] mengidentifikasi risiko ke dalam beberapa jenis yaitu *Malicious* URL *where aWindows* (exe) *Installer* (*Cyber*Observable of Class URL in STIX™), *Data Breach, Data Leak, Network Traffic Data Leaked from Outside, Server Sabotage, Ransomware, Physical Treat, Earthquake, System Down*.

Dalam pencarian tren risiko keamanan siber, terdapat penelitian sebelumnya yang telah melakukan kegiatan yang sama yaitu mengidentifikasi risiko-risiko apa saja yang mungkin muncul di masa mendatang. Penelitian [6] telah melakukan penelitian dengan menghasilkan tren risiko. Dalam penelitian ini juga mempunyai kemiripan dengan penelitian yang penulis lakukan yaitu membagi risiko ke dalam kategori risiko teknologi, organisasi dan lingkungan. Risiko tersebut adalah IoT *management, big data integration, blockchain management, cybersecurity management, GIS and remote sensing implementation, UAV's management, Digital platform management, Fintech adoption, AI management, Cyberphysical component management, Digital information management, Crowd density management, Wireless sensors management, Next generation internet adoption, Technology optimisation, Fog computing management, virtual reality adoption, user data security, data safety, cloud management, IT management, Willingnesss to digitalise, Differing stakeholder perception, Schedule Optimisation, Transparent dashboards, accountability, Financial Management, Resource management, disaster management, transport management, emergency management, Wellbeing monitoring, Public awareness and perception, Air Quality monitoring, Healthcare management, Smart infrastructure management, City Governance, Pedestrians Crossings, Policy making, environtment management, City administrations, History persevations, Social attributes, urban safety, national security, Population management, public and user safety, smart media monitoring, samrt parking, Energy optimisation, Green design management, pandemic management, Crime investigation, Food security, Techno politice, Noise monitoring*.

Penelitian ini mengidentifikasi risiko secara umum dan belum spesifik ke risiko keamanan siber.

Penelitian [32] melakukan penelitian terkait dengan secure *public data-smart network* dan menemukan beberapa risiko keamanan siber seperti *wifiphiser*, *man-in-the-middle attacker* (MITM), *malware, denial-of-service attack* (DoS). Dalam penelitian lain, [33] berfokus pada arsitektur kuantum dan menemukan risiko seperti *distributed-denial-of-service attack* (DDoS), *cross-site scipting* (XSS), SQL *injection*, dan *port scan*. Hampir mirip dengan penelitian sebelumnya, penelitian [34] dan [35] juga menemukan risiko keamanan siber seperti *malicious attack*, *malware*, DDoS, MITM, dan risiko yang baru muncul seperti IoT *fake client*, *botnet attack*, dan *data manipulation*. Selanjutnya penelitian [36] menemukan risko *false data injection attack dan data security and privacy* dalam penelitiannya serta penelitian [37] menemukan risiko *data breach, high comsumption energy*, dan *low interoperability.*

Dari seluruh penelitian yang dilakukan ekstraksi data diatas, ditemukan banyak sekali risiko, khususnya risiko keamanan siber. Dari temuan risiko tersebut kemudian dilakukan pengklasifikasian risiko berdasarkan kerangka TOE lalu kemudian dikhususkan ke dalam risiko kemanan siber.

3. Klasifikasi Risiko Keamanan Siber

Klasifikasi risiko dilakukan berdasarkan kerangka TOE dengan membagi risiko ke dalam tiga jenis yaitu teknologi, organisasi, dan lingkungan. Berbagai risiko yang ditemukan dari paper rujukan penulis dirangkum dalam Tabel 3.

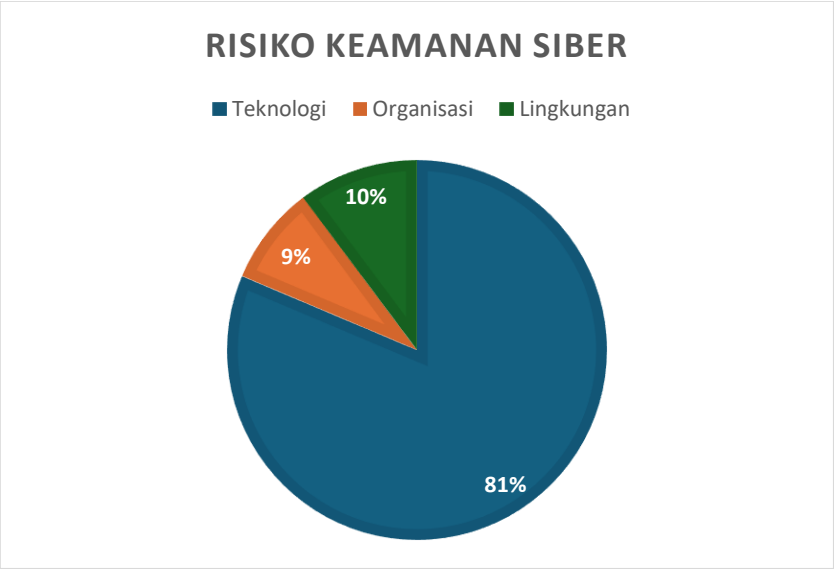
Tabel 3. Klasifikasi risiko berdasarkan TOE

Kategori Risiko	Macam Risiko
Teknologi	*SQL Injection, XSS, Information Gathering, Information Disclosure, Data Leak, Insecure Backup and Storage, Data Security and Privacy, Phising, Data Manipulation, Data Breach, DoS, DdoS, Malware, Virus, Ransonware, Backdoors, Remote-access, Security and system flaws, Botnet Attack, Cloud Vulnerability, Service disruption or denial, MITM, User data security, Data Safety, Cloud Management, IT Management, IoT Management, Blockchain Management, UAV's Management, Digital Platform Management, AI Manegement, Cyberphysical component management, Crowd Density Management, Wireless Sensors Management, Fog Computing Management, Digital Information Management, 5G usage, Big Data Integration, GIS and Remote Sensing Implementation, Fintech adoption, Next Generation Internet Adoption, Technology Optimisation, Virtual Reality Adoption, Fake Application, IoT fake client, Noise Monitoring, Wireless Jamming*
Organisasi	*Failure to understand the consequences of cyberattack, failure to monitor risks on an ongoing basis, diverse levels of digital literacy, third party or provider risk, smart infrastructure management*
Lingkungan	*Loss or Theft of Equipment, rapid changes in technology and threat landscape, physical demage (sabotage and espionage), city governance, policy making, technopolitics*

Penerapan kerangka kerja TOE di *smart city* melibatkan pemeriksaan faktor teknologi, organisasi, dan lingkungan. Teknologi menjadi faktor penting dalam implementasi *smart city*, salah satunya Integrasi AI dan IoT. Integrasi ini mengatasi

masalah utama kota dan meningkatkan kualitas hidup masyarakat [38]. Faktor organisasi seperti dukungan manajemen puncak juga menjadi salah satu faktor yang penting. Keberhasilan inisiatif *smart city* seringkali bergantung pada dukungan dari manajemen puncak dalam pemerintah lokal. Dukungan ini sangat penting untuk adopsi alat dan teknologi digital untuk kolaborasi masyarakat [39]. Kemudian faktor lingkungan juga memegang peranan penting dalam pembangunan *smart city*, salah satunya adalah pengaruh Politik. Lingkungan politik memainkan peran penting dalam adopsi teknologi *smart city* karena dapat memfasilitasi atau menghambat implementasi proyek *smart city* [39].

Hasil identifikasi risiko keamanan siber yang disebutkan pada Tabel 3 menunjukkan bahwa risiko keamanan siber teknologi sangat mendominasi (47 risiko)daripada risiko keamanan siber organisasi (5 risiko) dan risiko keamanan siber lingkungan.(6 risiko).



Gambar 3. Perbandingan jumlah risiko keamanan siber

4. Mitigasi Risiko Keamanan Siber

Mitigasi risiko merupakan salah satu langkah yang dapat dilakukan dalam rangka meminimalisir dampak yang mungkin terjadi akibat terjadinya risiko. Mitigasi risiko yang dituliskan berikut merupakan mitigasi risiko yang diambil dari beberapa paper rujukan. Mitigasi risiko disesuaikan dengan risiko pada masing-masing kategori teknologi, organisasi, dan lingkungan yang ditunjukkan pada Tabel 4.

Tabel 4. Mitigasi Risiko Kemanan Siber

Kategori Risiko	Macam Risiko	Mitigasi Risiko
Teknologi	*SQL Injection*	Implementasi validasi input yang ketat dan penggunaan kueri berparameter untuk mencegah injeksi SQL [26]

Kategori Risiko	Macam Risiko	Mitigasi Risiko
	XSS	Penggunaan escape dan encoding pada data yang ditampilkan di halaman web untuk mencegah eksekusi skrip berbahaya [26]
	Information Gathering	Melakukan audit keamanan secara bertahap dan menggunakan alat deteksi intrusi untuk mengidentifikasi dan mencegah upaya pengumpulan informasi [26]
	Information Disclosure	Menggunakan enkripsi data dan kontrol akses yang ketat untuk mencegah pengambilan informasi yang tidak sah [26]
	Data Leak	Penerapan kebijakan keamanan data yang ketat dan penggunaan alat deteksi kebocoran data untuk memantau dan mencegah kebocoran data [26]
	Insecure Backup dan Storage	Menggunakan metode enkripsi yang kuat dan memastikan cadangan data disimpan di lokasi yang aman dan terisolasi [40]
	Data Security and Privacy	Mengimplementasikan kebijakan privasi data yang komprehensif dan menerapkan teknologi enkripsi untuk mengamankan data sensitif [26]
	Phising	Melakukan pelatihan kesadaran keamanan siber bagi karyawan dan menggunakan filter email untuk mendeteksi dan memblokir email phishing [26]
	Data Manipulation	Menerapkan mekanisme deteksi anomali dan validasi data untuk mencegah manipulasi data yang tidak sah [30]
	Data Breach	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data dari pelanggaran keamanan [26]
	DoS	Menggunakan firewall dan sistem deteksi intrusi untuk memantau dan mencegah serangan DoS [26]
	DDoS	Menggunakan layanan mitigasi DDoS yang dapat diaktifkan dan mengalihkan lalu lintas serangan [26]
	Malware	Menggunakan perangkat lunak antivirus dan anti-*malware* yang diperbarui secara berkala untuk mendeteksi dan menghapus *malware* [26]
	Virus	Menggunakan perangkat lunak antivirus yang diperbarui dan melakukan pemindaian sistem secara bertahap untuk mendeteksi dan menghapus virus [26]
	Ransomware	Melakukan pencadangan data secara bertahap dan menggunakan perangkat lunak anti-*ransomware* untuk mencegah serangan *ransomware* [26]
	Backdoors	Melakukan audit keamanan secara bertahap dan menutup akses yang tidak sah untuk mencegah pintu belakang [40]

Kategori Risiko	Macam Risiko	Mitigasi Risiko
	Remote-access	Menggunakan autentikasi multi-faktor dan enkripsi untuk mengamankan akses jarak jauh [40]
	Security and system flaws	Melakukan pembaruan dan patch sistem secara bertahap untuk memperbaiki kerentanan keamanan [40]
	Botnet Attack	Melindungi jaringan dengan firewall dan sistem deteksi intrusi untuk mencegah serangan botnet [40]
	Kerentanan Cloud	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data di lingkungan *cloud* [26]
	Service disruption or denial	Menggunakan layanan mitigasi DDoS dan sistem deteksi intrusi untuk mencegah gangguan layanan [26]
	MITM	Menggunakan enkripsi end-to-end dan sertifikat SSL/TLS untuk melindungi komunikasi dari serangan MITM [26]
	User data security	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data pengguna [26]
	Data Safety	Mengimplementasikan kebijakan keamanan data yang komprehensif dan menerapkan teknologi enkripsi untuk mengamankan data [26]
	Cloud Management	Menggunakan enkripsi data dan kontrol akses ketat untuk mengelola keamanan data di *cloud* [26]
	IT Management	Melakukan audit keamanan secara bertahap dan menggunakan alat deteksi intrusi untuk mengelola risiko keamanan TI [26]
	IoT Management	Menggunakan enkripsi data dan kontrol akses ketat untuk mengelola keamanan perangkat IoT [26]
	Blockchain Management	Menerapkan langkah-langkah keamanan yang lebih kuat di luar tanda tangan digital untuk mengatasi kerentanan seperti kompromi kunci pribadi dalam sistem Blockchain-IoT [24]
	UAV's Management	Memanfaatkan protokol komunikasi yang aman dan enkripsi untuk melindungi transmisi data antara UAV dan sistem kontrol [35]
	Digital Platform Management	Melakukan audit keamanan secara berkala dan menerapkan kontrol akses yang ketat untuk melindungi platform digital dari akses tidak sah dan pelanggaran data [35]
	AI Management	Memastikan sistem AI dilatih pada kumpulan data yang aman dan terverifikasi untuk mencegah manipulasi data dan akses tidak sah [35]
	Cyberphysical component management	Menerapkan pemantauan waktu nyata dan sistem deteksi anomali untuk mengidentifikasi dan mengurangi risiko dalam komponen *cyber*-fisik [24]

Kategori Risiko	Macam Risiko	Mitigasi Risiko
	Crowd Density Management	Menggunakan sensor IoT untuk memantau dan mengelola kepadatan kerumunan, memastikan integritas dan keamanan data melalui enkripsi dan transmisi data yang aman [24]
	Wireless Sensors Management	Menggunakan protokol komunikasi yang aman dan pembaruan *firmware* reguler untuk melindungi jaringan sensor nirkabel dari ancaman *cyber* [24]
	Fog Computing Management	Menerapkan enkripsi yang kuat dan mekanisme kontrol akses untuk mengamankan pemrosesan dan penyimpanan data di lingkungan Fog Computing [35]
	Digital Information Management	Memanfaatkan enkripsi data yang komprehensif dan kebijakan kontrol akses untuk melindungi informasi digital dari akses dan pelanggaran yang tidak sah [35]
	5G Usage	Menerapkan pemotongan jaringan dan protokol komunikasi yang aman untuk melindungi jaringan 5G dari ancaman dunia maya [35]
	Big Data Integration	Memastikan integritas dan keamanan data melalui enkripsi dan praktik penanganan data yang aman selama integrasi data besar [35]
	GIS and Remote Sensing Implementation	Menggunakan metode transmisi dan penyimpanan data yang aman untuk melindungi GIS dan data penginderaan jauh dari akses yang tidak sah [35]
	Fintech adoption	Menerapkan otentikasi dan enkripsi multi-faktor untuk mengamankan transaksi keuangan dan data dalam aplikasi *fintech* [35]
	Next Generation Internet Adoption	Menggunakan protokol keamanan canggih dan pembaruan keamanan reguler untuk melindungi infrastruktur internet generasi berikutnya dari ancaman *cyber* [35]
	Technology Optimisation	Melakukan penilaian dan pembaruan keamanan rutin untuk mengoptimalkan infrastruktur teknologi dan mengurangi potensi risiko [35]
	Virtual Reality Adoption	Menggunakan protokol komunikasi yang aman dan enkripsi untuk melindungi data dan privasi pengguna dalam aplikasi realitas virtual [35]
	Fake Application	Menerapkan verifikasi aplikasi dan pemeriksaan keamanan untuk mendeteksi dan mencegah distribusi aplikasi palsu [35]
	IoT fake client	Memanfaatkan model simulasi dan pembelajaran mesin untuk mendeteksi dan mengurangi keberadaan IoT fake client di lingkungan *smart city* [24] [35]
	Noise Monitoring	Menggunakan protokol komunikasi yang aman dan enkripsi untuk melindungi data

Kategori Risiko	Macam Risiko	Mitigasi Risiko
		yang dikumpulkan dari sistem pemantauan kebisingan, memastikan integritas dan kerahasiaan data [30]
	Wireless Jamming	Menerapkan protokol komunikasi yang aman dan pembaruan *firmware* reguler untuk melindungi jaringan nirkabel dari serangan gangguan [6]
Organisasi	*Kegagalan dalam memahami konsekuensi dari serangan siber*	Melakukan penilaian risiko komprehensif dan mendidik manajemen puncak tentang dampak potensial serangan *cyber* untuk memastikan pengambilan keputusan dan kesiapan yang terinformasi [40]
	Kegagalan dalam memantau risiko secara berkelanjutan	Menerapkan sistem pemantauan berkelanjutan dan audit keamanan rutin untuk mengidentifikasi dan mengurangi risiko yang muncul segera [20]
	Tingkat literasi digital yang beragam	Menyediakan pelatihan keamanan siber berkelanjutan dan program kesadaran yang disesuaikan dengan berbagai tingkat literasi digital dalam organisasi untuk memastikan semua karyawan memahami dan dapat menanggapi ancaman *cyber* secara efektif [24]
	Risiko pihak ketiga atau penyedia	Menetapkan persyaratan keamanan yang ketat dan melakukan penilaian keamanan rutin untuk penyedia pihak ketiga untuk memastikan mereka mematuhi standar keamanan siber organisasi [24]
	Smart infrastructure management	Memanfaatkan kerangka kerja manajemen risiko canggih dan model berbasis simulasi untuk mendeteksi dan mengurangi risiko yang terkait dengan infrastruktur pintar, memastikan keamanan dan ketahanan lingkungan *smart city* [35]
Lingkungan	*Loss or Theft of Equipment*	Menerapkan proses otentikasi multi-faktor yang kuat dan kebijakan kontrol akses yang kuat untuk mencegah akses tidak sah ke peralatan dan data [20]
	Perubahan cepat dalam teknologi dan lanskap ancaman	Melakukan penilaian dan pembaruan keamanan rutin untuk beradaptasi dengan teknologi yang berkembang dan lanskap ancaman, memastikan bahwa langkah-langkah keamanan tetap efektif [6]
	Physical damage (sabotage and espionage)	Memanfaatkan sistem pemantauan real-time dan deteksi anomali untuk mengidentifikasi dan mengurangi risiko kerusakan fisik akibat sabotase atau spionase [20]
	City Governance	Mengusulkan dan menerapkan kerangka kerja manajemen risiko komprehensif yang disesuaikan dengan tata kelola kota pintar untuk mengatasi dan mengurangi berbagai risiko secara efektif [35]
	Policy making	Menetapkan dan menegakkan kebijakan dan pedoman keamanan yang ketat untuk memastikan praktik keamanan siber yang

Kategori Risiko	Macam Risiko	Mitigasi Risiko
		konsisten dan efektif di seluruh organisasi [24]
	Technopolitics	Mendidik pembuat kebijakan dan pemangku kepentingan tentang implikasi risiko keamanan siber dan pentingnya langkah-langkah keamanan yang kuat untuk mempengaruhi pengambilan keputusan yang terinformasi [24]

5. Validasi Mitigasi Risiko Keamanan Siber

Seluruh risiko yang telah teridentifikasi berdasarkan kerangka kerja TOE, sebagaimana dijelaskan pada bagian sebelumnya, telah diidentifikasi juga mitgasi risiko berdasarkan penelitian yang dijadikan rujukan. Terdapat 47 risiko keamanan siber teknologi, 5 risiko keamanan siber organisasi, dan 6 risiko keamanan siber lingkungan. Untuk memperkuat hasil penelitian, dilakukan validasi tambahan melalui pendekatan *best practice.* Badan Siber dan Sandi Negara (BSSN) merupakan salah satu lembaga pemerintahan yang bertugas di bidang keamanan siber dan sandi nasional. Selain keamanan siber, BSSN juga mengelola kebijakan terkait dengan manajemen risiko.

Berdasarkan keterangan dari Tim Pengelola Manajemen Risiko di BSSN, proses manajemen risiko selalu dipusatkan menggunakan standar internasional ISO 31000: 2018 tentang *Risk Managem*ent dan ISO 27005: 2018 tentang *Information security Risk Management*. Disebutkan juga dalam mengidentifikasi kontrol terhadap risiko, menggunakan standar internasional yaitu ISO 27001: 2022 tentang *Information Security Management System* dan ISO 27002:2022 tentang *Information Security Controls*. Pada penelitian ini dilakukan juga validasi terhadap hasil penelitian menggunakan standar internasional ISO 27002: 2022. Yang ditunjukkan pada Tabel 5.

Tabel 5. Validasi kesesuaian mitigasi risiko

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
Teknologi	*SQL Injection*	Implementasi validasi input yang ketat dan penggunaan kueri berparameter untuk mencegah injeksi SQL [26]	*Information access restriction (8.3), use of cryptography (8.24), Application security requirements (8.26), Security testing in development and acceptance (8.29),*	Sesuai
	XSS	Penggunaan escape dan encoding pada data yang ditampilkan di halaman web untuk mencegah eksekusi skrip berbahaya [26]	*Management of technical vulnerabilities (8.8), use of cryptography (8.24), Secure coding (8.28), Security testing in development and acceptance (8.29)*	Sesuai
	Information Gathering	Melakukan audit keamanan secara bertahap dan menggunakan alat deteksi intrusi untuk mengidentifikasi dan mencegah upaya pengumpulan informasi [26]	*User endpoint device (8.1), information security awareness, education and training (6.3), web filtering (8.23)*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
	Information Disclosure	Menggunakan enkripsi data dan kontrol akses yang ketat untuk mencegah pengambilan informasi yang tidak sah [26]	*Information access restriction (8.3), use of cryptography (8.24)*	Sesuai
	Data Leak	Penerapan kebijakan keamanan data yang ketat dan penggunaan alat deteksi kebocoran data untuk memantau dan mencegah kebocoran data [26]	*Secure authentication (8.5), Data leakage prevention (8.12), use of cryptography (8.24)*	Sesuai
	Insecure Backup dan Storage	Menggunakan metode enkripsi yang kuat dan memastikan cadangan data disimpan di lokasi yang aman dan terisolasi [40]	*Capacity management (8.6), Information backup (8.13), use of cryptography (8.24)*	Sesuai
	Data Security and Privacy	Mengimplementasikan kebijakan privasi data yang komprehensif dan menerapkan teknologi enkripsi untuk mengamankan data sensitif [26]	*Legal, statutory, regulatory and contractual requirements (5.31), Privacy and protection of PII (5.34), use of cryptography (8.24)*	Sesuai
	Phising	Melakukan pelatihan kesadaran keamanan siber bagi karyawan dan menggunakan filter email untuk mendeteksi dan memblokir email phishing [26]	*information security awareness, education and training (6.3), web filtering (8.23)*	Sesuai
	Data Manipulation	Menerapkan mekanisme deteksi anomali dan validasi data untuk mencegah manipulasi data yang tidak sah [30]	*Monitoring activities (8.16), Data leakage prevention (8.12), use of cryptography (8.24)*	Sesuai
	Data Breach	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data dari pelanggaran keamanan [26]	*Secure authentication (8.5), Data leakage prevention (8.12), use of cryptography (8.24)*	Sesuai
	DoS	Menggunakan firewall dan sistem deteksi intrusi untuk memantau dan mencegah serangan DoS [26]	*Management of technical vulnerabilities (8.8), use of cryptography (8.24)*	Sesuai
	DDoS	Menggunakan layanan mitigasi DDoS yang dapat diaktifkan dan mengalihkan lalu lintas serangan [26]	*Management of technical vulnerabilities (8.8), use of cryptography (8.24)*	Sesuai
	Malware	Menggunakan perangkat lunak antivirus dan anti-*malware* yang diperbarui secara berkala untuk mendeteksi dan menghapus *malware* [26]	*Protection againts malware (8.7), Management of technical vulnerabilities (8.8), use of cryptography (8.24)*	Sesuai
	Virus	Menggunakan perangkat lunak antivirus yang diperbarui dan melakukan pemindaian sistem secara bertahap untuk mendeteksi dan menghapus virus [26]	*Protection againts malware (8.7), Management of technical vulnerabilities (8.8), use of cryptography (8.24)*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
	Ransomware	Melakukan pencadangan data secara bertahap dan menggunakan perangkat lunak anti-*ransomware* untuk mencegah serangan *ransomware* [26]	*Protection againts malware (8.7)*, *Capacity management (8.6)*, *Management of technical vulnerabilities (8.8)*, *Information backup (8.13)*, *use of cryptography (8.24)*	Sesuai
	Backdoors	Melakukan audit keamanan secara bertahap dan menutup akses yang tidak sah untuk mencegah pintu belakang [40]	*Access control (5.18)*, *Compliance with policies, rules and standards for information security (5.36)*, *information access restriction (8.3)*	Sesuai
	Remote-access	Menggunakan autentikasi multi-faktor dan enkripsi untuk mengamankan akses jarak jauh [40]	*Access control (5.18)*, *secure authentication (8.5)*, *use of cryptography (8.24)*	Sesuai
	Security and system flaws	Melakukan pembaruan dan patch sistem secara bertahap untuk memperbaiki kerentanan keamanan [40]	*Compliance with policies, rules and standards for information security (5.36)*, *Management of technical vulnerabilities (8.8)*	Sesuai
	Botnet Attack	Melindungi jaringan dengan firewall dan sistem deteksi intrusi untuk mencegah serangan botnet [40]	*Management of technical vulnerabilities (8.8)*, *use of cryptography (8.24)*	Sesuai
	Kerentanan Cloud	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data di lingkungan *cloud* [26]	*Management of technical vulnerabilities (8.8)*, *use of cryptography (8.24)*	Sesuai
	Service disruption or denial	Menggunakan layanan mitigasi DDoS dan sistem deteksi intrusi untuk mencegah gangguan layanan [26]	*Management of technical vulnerabilities (8.8)*, *use of cryptography (8.24)*	Sesuai
	MITM	Menggunakan enkripsi end-to-end dan sertifikat SSL/TLS untuk melindungi komunikasi dari serangan MITM [26]	*Network security (8.20)*, *use of cryptography (8.24)*	Sesuai
	User data security	Menggunakan enkripsi data dan kontrol akses ketat untuk melindungi data pengguna [26]	*Access control (5.18)*, *secure authentication (8.5)*, *use of cryptography (8.24)*	Sesuai
	Data Safety	Mengimplementasikan kebijakan keamanan data yang komprehensif dan menerapkan teknologi enkripsi untuk mengamankan data [26]	*Legal, statutory, regulatory and contractual requirements (5.31)*, *use of cryptography (8.24)*	Sesuai
	Cloud Management	Menggunakan enkripsi data dan kontrol akses ketat untuk mengelola keamanan data di *cloud* [26]	*Access control (5.18)*, *information security for use of cloud service (5.23)*, *secure authentication (8.5)*, *use of cryptography (8.24)*,	Sesuai
	IT Management	Melakukan audit keamanan secara bertahap dan	*Compliance with policies, rules and standards for*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
		menggunakan alat deteksi intrusi untuk mengelola risiko keamanan TI [26]	*information security (5.36), protecting againts physical and environtmental threats (7.5)*	
	IoT Management	Menggunakan enkripsi data dan kontrol akses ketat untuk mengelola keamanan perangkat IoT [26]	*Access control (5.18), secure authentication (8.5), use of cryptography (8.24)*	Sesuai
	Blockchain Management	Menerapkan langkah-langkah keamanan yang lebih kuat di luar tanda tangan digital untuk mengatasi kerentanan seperti kompromi kunci pribadi dalam sistem Blockchain-IoT [24]	*Manging information security in the ICS supply chain (5.21), Management of technical vulnerabilities (8.8), use of cryptography (8.24)*	Sesuai
	UAV's Management	Memanfaatkan protokol komunikasi yang aman dan enkripsi untuk melindungi transmisi data antara UAV dan sistem kontrol [35]	*use of cryptography (8.24), Secure system architechture and engineering principles (8.27),*	Sesuai
	Digital Platform Management	Melakukan audit keamanan secara berkala dan menerapkan kontrol akses yang ketat untuk melindungi platform digital dari akses tidak sah dan pelanggaran data [35]	*Compliance with policies, rules and standards for information security (5.36), Access control (5.18), secure authentication (8.5)*	Sesuai
	AI Management	Memastikan sistem AI dilatih pada kumpulan data yang aman dan terverifikasi untuk mencegah manipulasi data dan akses tidak sah [35]	*Compliance with policies, rules and standards for information security (5.36), Access control (5.18), secure authentication (8.5)*	Sesuai
	Cyberphysical component management	Menerapkan pemantauan waktu nyata dan sistem deteksi anomali untuk mengidentifikasi dan mengurangi risiko dalam komponen *cyber*-fisik [24]	*protecting againts physical and environtmental threats (7.5), monitoring activitis (8.16), Clock syncrhronization (8.17),*	Sesuai
	Crowd Density Management	Menggunakan sensor IoT untuk memantau dan mengelola kepadatan kerumunan, memastikan integritas dan keamanan data melalui enkripsi dan transmisi data yang aman [24]	*use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Wireless Sensors Management	Menggunakan protokol komunikasi yang aman dan pembaruan *firmware* reguler untuk melindungi jaringan sensor nirkabel dari ancaman *cyber* [24]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Fog Computing Management	Menerapkan enkripsi yang kuat dan mekanisme kontrol akses untuk mengamankan	*Access control (5.18), use of cryptography (8.24)*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
		pemrosesan dan penyimpanan data di lingkungan *Fog Computing* [35]		
	Digital Information Management	Memanfaatkan enkripsi data yang komprehensif dan kebijakan kontrol akses untuk melindungi informasi digital dari akses dan pelanggaran yang tidak sah [35]	*Compliance with policies, rules and standards for information security (5.36), Access control (5.18), use of cryptography (8.24)*	Sesuai
	5G Usage	Menerapkan pemotongan jaringan dan protokol komunikasi yang aman untuk melindungi jaringan 5G dari ancaman dunia maya [35]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Big Data Integration	Memastikan integritas dan keamanan data melalui enkripsi dan praktik penanganan data yang aman selama integrasi data besar [35]	*use of cryptography (8.24), security testing in development and acceptance (8.29)*	Sesuai
	GIS and Remote Sensing Implementation	Menggunakan metode transmisi dan penyimpanan data yang aman untuk melindungi GIS dan data penginderaan jauh dari akses yang tidak sah [35]	*Access control (5.18), secure authentication (8.5), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Fintech adoption	Menerapkan otentikasi dan enkripsi multi-faktor untuk mengamankan transaksi keuangan dan data dalam aplikasi *fintech* [35]	*secure authentication (8.5), use of cryptography (8.24),*	Sesuai
	Next Generation Internet Adoption	Menggunakan protokol keamanan canggih dan pembaruan keamanan reguler untuk melindungi infrastruktur internet generasi berikutnya dari ancaman *cyber* [35]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Technology Optimisation	Melakukan penilaian dan pembaruan keamanan rutin untuk mengoptimalkan infrastruktur teknologi dan mengurangi potensi risiko [35]	*Compliance with policies, rules and standards for information security (5.36), protecting againts physical and environtmental threats (7.5), use of cryptography (8.24), Secure system architechture and engineering principles (8.27),*	Sesuai
	Virtual Reality Adoption	Menggunakan protokol komunikasi yang aman dan enkripsi untuk melindungi data dan privasi pengguna dalam aplikasi realitas virtual [35]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
			and engineering principles (8.27)	
	Fake Application	Menerapkan verifikasi aplikasi dan pemeriksaan keamanan untuk mendeteksi dan mencegah distribusi aplikasi palsu [35]	*Secure authentication (8.5), application security requirements (8.26), secure development life cycle (8.25)*	Sesuai
	IoT fake client	Memanfaatkan model simulasi dan pembelajaran mesin untuk mendeteksi dan mengurangi keberadaan IoT fake client di lingkungan *smart city* [24] [35]	*Information security awareness, education and training (6.3)*	Sesuai
	Noise Monitoring	Menggunakan protokol komunikasi yang aman dan enkripsi untuk melindungi data yang dikumpulkan dari sistem pemantauan kebisingan, memastikan integritas dan kerahasiaan data [30]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
	Wireless Jamming	Menerapkan protokol komunikasi yang aman dan pembaruan *firmware* reguler untuk melindungi jaringan nirkabel dari serangan gangguan [6]	*Compliance with policies, rules and standards for information security (5.36), use of cryptography (8.24), Secure system architechture and engineering principles (8.27)*	Sesuai
Organisasi	*Kegagalan dalam memahami konsekuensi dari serangan siber*	Melakukan penilaian risiko komprehensif dan mendidik manajemen puncak tentang dampak potensial serangan *cyber* untuk memastikan pengambilan keputusan dan kesiapan yang terinformasi [40]	*Management responsibilities (5.4), Information security awareness, education and training (6.3)*	Sesuai
	Kegagalan dalam memantau risiko secara berkelanjutan	Menerapkan sistem pemantauan berkelanjutan dan audit keamanan rutin untuk mengidentifikasi dan mengurangi risiko yang muncul segera [20]	*Management responsibilities (5.4), Compliance with policies, rules and standards for information security (5.36), Information security awareness, education and training (6.3)*	Sesuai
	Tingkat literasi digital yang beragam	Menyediakan pelatihan keamanan siber berkelanjutan dan program kesadaran yang disesuaikan dengan berbagai tingkat literasi digital dalam organisasi untuk memastikan semua karyawan memahami dan dapat menanggapi ancaman *cyber* secara efektif [24]	*Information security awareness, education and training (6.3)*	Sesuai
	Risiko pihak ketiga atau penyedia	Menetapkan persyaratan keamanan yang ketat dan melakukan penilaian	*Compliance with policies, rules and standards for information security (5.36),*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
		keamanan rutin untuk penyedia pihak ketiga untuk memastikan mereka mematuhi standar keamanan siber organisasi [24]	*protecting againts physical and environtmental threats (7.5), Outsourced development (8.30)*	
	Smart infrastructure management	Memanfaatkan kerangka kerja manajemen risiko canggih dan model berbasis simulasi untuk mendeteksi dan mengurangi risiko yang terkait dengan infrastruktur pintar, memastikan keamanan dan ketahanan lingkungan *smart city* [35]	*Compliance with policies, rules and standards for information security (5.36), ICT readiness for business continuity (5.30), Information security awareness, education and training (6.3)*	Sesuai
Lingkungan	*Loss or Theft of Equipment*	Menerapkan proses otentikasi multi-faktor yang kuat dan kebijakan kontrol akses yang kuat untuk mencegah akses tidak sah ke peralatan dan data [20]	*Access control (5.18), physical security perimeters (7.1), protecting againts physical and environtmental threats (7.5)*	Sesuai
	Perubahan cepat dalam teknologi dan lanskap ancaman	Melakukan penilaian dan pembaruan keamanan rutin untuk beradaptasi dengan teknologi yang berkembang dan lanskap ancaman, memastikan bahwa langkah-langkah keamanan tetap efektif [6]	*Policies for information security (5.1), Threat intelligence (5.7), Compliance with policies, rules and standards for information security (5.36),*	Sesuai
	Physical damage (sabotage and espionage)	Memanfaatkan sistem pemantauan real-time dan deteksi anomali untuk mengidentifikasi dan mengurangi risiko kerusakan fisik akibat sabotase atau spionase [20]	*Access control (5.18), physical security perimeters (7.1), protecting againts physical and environtmental threats (7.5)*	Sesuai
	City Governance	Mengusulkan dan menerapkan kerangka kerja manajemen risiko komprehensif yang disesuaikan dengan tata kelola kota pintar untuk mengatasi dan mengurangi berbagai risiko secara efektif [35]	*Policies for information security (5.1), Threat intelligence (5.7), Compliance with policies, rules and standards for information security (5.36)*	Sesuai
	Policy making	Menetapkan dan menegakkan kebijakan dan pedoman keamanan yang ketat untuk memastikan praktik keamanan siber yang konsisten dan efektif di seluruh organisasi [24]	*Policies for information security (5.1), Threat intelligence (5.7), Compliance with policies, rules and standards for information security (5.36)*	Sesuai
	Technopolitics	Mendidik pembuat kebijakan dan pemangku kepentingan tentang implikasi risiko keamanan siber dan pentingnya langkah-langkah keamanan yang kuat untuk	*Management responsibilities (5.4), Information security awareness, education and training (6.3)*	Sesuai

Kategori Risiko	Macam Risiko	Mitigasi Risiko (Hasil Penelitian)	Kontrol Risiko (ISO 27002: 2022)	Ket.
		mempengaruhi pengambilan keputusan yang terinformasi [24]		

D. Simpulan

Penelitian ini bertujuan untuk melakukan identifikasi risiko keamanan siber berdasarkan kerangka kerja TOE (Technology, Organization, Environment) berdasarkan tren keamanan siber lima tahun terakhir serta analisis mitigasi setiap risiko. Hasil penelitian didapatkan 58 risiko keamanan siber dengan 47 risiko keamanan siber teknologi, 5 risiko keamanan siber organisasi dan 6 risiko keamanan siber lingkungan. Penelitian ini juga telah mengidentifikasi mitigasi risiko untuk masing masing risiko keamanan siber. Untuk memperkuat hasil penelitian, dilakukan validasi tambahan melalui pendekatan *best practice* (Tim Pengelola Manajemen Risiko di BSSN) yaitu dengan menggunakan pendekatan ISO 27002: 2022. Hasil validasi menunjukkan bahwa mitigasi terhadap 58 risiko tersebut sesuai atau terdapat pada kontrol keamanan di ISO 27002: 2022.

Dengan dominasinya risiko keamanan siber teknologi, penulis merekomendasikan kepada pemerintah terkait dengan perencanaan kekebijakan keamanan siber di *smart city* IKN dengan menekankan tiga aspek yaitu teknologi, organisasi, dan lingkungan. Aspek teknologi menekankan pentingnya penggunaan kriptografi yang aman di setiap proses bisnis. Aspek organisasi menekankan pentingnya kepatuhan terhadap regulasi dan standar keamanan yang berlaku, pelaksanaan audit kepatuhan secara berkala dan selalu menerapkan manajemen risiko untuk mengatasi dan mengurangi berbagai risiko secara efektif. Aspek lingkungan menekankan pentingnya kesadaran keamanan informasi dan pelatihan keamanan siber berkelanjutan yang disesuaikan dengan berbagai tingkat literasi digital dalam organisasi untuk menjamin kualitas SDM yang mumpuni.

Informasi berupa tren risiko keamanan siber beserta mitigasi risiko yang dihasilkan, menjadi implikasi penelitian berupa rekomendasi saran dan masukan sebagai dasar pemerintah dalam menetapkan kebijakan keamanan siber di *smart city* IKN dengan menekankan pada tiga aspek yaitu teknologi, organisasi, dan lingkungan. Penelitian dengan mengadopsi *framework* TOE dan kombinasi dengan standar internasional ISO 27002:2022 dilakukan sebagai upaya melengkapi pengetahuan terkait risiko keamanan siber untuk *smart city* IKN yang masih belum banyak didefinisikan, sementara ancaman keamanan siber terus berkembang.

Penelitian ini hanya berfokus pada identifikasi risiko keamanan siber dan identifikasi mitigasi atas risiko yang ditemukan, dan masih belum secara komprehensif melakukan kuantifikasi terhadap risiko serta analisis dampak untuk masing-masing risiko keamanan siber yang muncul. Oleh karenanya, masih banyak mempunyai kekurangan dan perlu dilakukan penelitian lanjutan untuk memperdalam proses *risk management* yang komprehensif terhadap risiko keamanan siber secara utuh.

E. Ucapan Terima Kasih

Ucapan terima kasih penulis sampaikan kepada seluruh pihak yang berkontribusi dalam melengkapi dan menyelesaikan penelitian ini.

F. Referensi

[1] Indonesia, Pemerintah Pusat. "Undang-Undang Nomor 3 Tahun 2022 tentang Ibu Kota Negara", https://peraturan.bpk.go.id/Details/198400/uu-no-3-tahun-2022, 2022, ditetapkan pada 15 Februari 2022.

[2] Indonesia, Pemerintah Pusat. "Undang-Undang Nomor 21 Tahun 2023 tentang Ibu Kota Negara", https://peraturan.bpk.go.id/Details/269494/uu-no-21-tahun-2023, 2023, ditetapkan pada 31 Oktober 2023.

[3] S. Mcclellan, J. A. Jimenez, and G. Koutitas, "*Smart cities* Applications, Technologies, Standards, and Driving Factors," doi:10.1007/978-3-319-59381-4.

[4] R. Eskhita, V. K. Manda, and A. Hlali, "Dubai and Barcelona as *Smart cities*: Some Reflections on Data Protection Law and Privacy," *Environmental Policy and Law*, vol. 51, no. 6, pp. 403–407, 2021, doi: 10.3233/EPL-210023.

[5] A. Chaudhuri and S. Bozkus Kahyaoglu, "*Cyber*security Assurance In *Smart Cities*: A Risk Management Perspective," *EDPACS*, vol. 67, no. 4, pp. 1–22, 2023. doi: 10.1080/07366981.2023.2165293.

[6] F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman, and S. M. E. Sepasgozar, "Risk management in sustainable *smart cities* governance: A TOE *framework*," *Technol Forecast Soc Change*, vol. 167, 2021, doi: 10.1016/j.techfore.2021.120743.

[7] M. Wright, H. Chizari, and T. Viana, "A Systematic Review of *Smart city* Infrastructure Threat Modelling Methodologies: A Bayesian Focused Review," *Sustainability (Switzerland)*, vol. 14, no. 16, Aug. 2022, doi: 10.3390/su141610368.

[8] R. G. G. Alam and H. Ibrahim, "*Cyber*security Strategy for *Smart city* Implementation," in *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, 2019, pp. 3–6. doi: 10.5194/isprs-archives-XLII-4-W17-3-2019.

[9] G. S. . Tomar, *Proceedings, 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT 2023), Madhya Pradesh Section Flagship Conference*. IEEE, 2023.

[10] J. Lloret *et al.*, "*Cyber*security and *Cyber* Forensics for *Smart cities*: A Comprehensive Literature Review and Survey," 2023, doi: 10.3390/s23073681.

[11] Indonesia, Pemerintah Pusat. "Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber", https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023, 2023, ditetapkan pada 20 Juli 2023.

[12] C. Florackis, C. Louca, R. Michaely, and M. Weber, "*Cyber*security Risk," *Review of Financial Studies*, vol. 36, no. 1, pp. 351–407, Jan. 2023, doi: 10.1093/rfs/hhac024.

[13] D. I. Sensuse, P. A. W. Putro, R. Rachmawati, and W. D. Sunindyo, "Initial *Cyber*security *Framework* in the New Capital City of Indonesia: Factors, Objectives, and Technology," Dec. 01, 2022, *MDPI*. doi: 10.3390/info13120580.

[14] R. Vorst, D.S. Priyarsono, A. Budiman, "Manajemen Risiko Berbasis SNI ISO 31000," Badan Standardisasi Nasional, 2018, https://perpustakaan.bsn.go.id/repository/ca09e618c360ecd38f4f0ccfc828a2ff.pdf .
[15] British, The British Standards Institution, "Risk Management – Guidelines," 2018, https://lpm.uin-suka.ac.id/media/dokumen_akademik/011_20191007_ISO%2031000.2018%20-%20Risk%20Management%20-%20Guidelines.pdf.
[16] Internasional Standard, "ISO 31000: 2018 Risk Management - Guidelines", 2018, https://www.iso.org/standard/65694.html.
[17] "Risk management-Principles and guidelines," 1994, [Online]. Available: www.saiglobal.com.au
[18] B. Kitchenham *et al.*, "Systematic literature reviews in software engineering – A tertiary study," *Inf Softw Technol*, vol. 52, no. 8, pp. 792–805, Aug. 2010, doi: 10.1016/J.INFSOF.2010.03.006.
[19] D. Clemente, T. Cabral, P. Rosa-Santos, and F. Taveira-Pinto, "Blue Seaports: The Smart, Sustainable and Electrified Ports of the Future," Jun. 01, 2023, *MDPI*. doi: 10.3390/smartcities6030074.
[20] H. M. Melaku, "Context-Based and Adaptive *Cyber*security Risk Management *Framework*," *Risks*, vol. 11, no. 6, 2023, doi: 10.3390/risks11060101.
[21] A. Orlando, "*Cyber* risk quantification: Investigating the role of *cyber* value at risk," *Risks*, vol. 9, no. 10, Oct. 2021, doi: 10.3390/risks9100184.
[22] A. Kuzior, O. Pakhnenko, I. Tiutiunyk, and S. Lyeonov, "E-Governance in *Smart cities*: Global Trends and Key Enablers," *Smart cities*, vol. 6, no. 4, pp. 1663–1689, Aug. 2023, doi: 10.3390/smartcities6040078.
[23] R. Andrade, I. Ortiz-Garcés, X. Tintin, and G. Llumiquinga, "Factors of Risk Analysis for IoT Systems," *Risks*, vol. 10, no. 8, Aug. 2022, doi: 10.3390/risks10080162.
[24] A. Faizi, A. Padyab, and A. Naess, "From rationale to lessons learned in the *cloud* information security risk assessment: a study of organizations in Sweden," *Information and Computer Security*, vol. 30, no. 2, pp. 190–205, Mar. 2022, doi: 10.1108/ICS-03-2021-0034.
[25] J. Simola, A. Takala, R. Lehkonen, T. Frantti, and R. Savola, "Impact of *Cyber* Security Operations on Hardware Requirements for Stable and Workable Industrial Environments."
[26] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness *Framework*s and Application Tools," *Risks*, vol. 10, no. 8, Aug. 2022, doi: 10.3390/risks10080165.
[27] R. Riesco and V. A. Villagrá, "Leveraging *cyber* threat intelligence for a dynamic risk *framework*: Automation by using a semantic reasoner and a new combination of standards (STIXTM, SWRL and OWL)," *Int J Inf Secur*, vol. 18, no. 6, pp. 715–739, Dec. 2019, doi: 10.1007/s10207-019-00433-2.
[28] R. Iten, J. Wagner, and A. Z. Röschmann, "On the identification, evaluation and treatment of risks in smart homes: A systematic literature review," Jun. 01, 2021, *MDPI AG*. doi: 10.3390/risks9060113.

[29] R. Goel, A. Kumar, and J. Haddow, "PRISM: a strategic decision *framework* for *cyber*security risk assessment," *Information and Computer Security*, vol. 28, no. 4, pp. 591–625, Oct. 2020, doi: 10.1108/ICS-11-2018-0131.

[30] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics *cyber* security: vulnerabilities, attacks, countermeasures, and recommendations," *Int J Inf Secur*, vol. 21, no. 1, pp. 115–158, Feb. 2022, doi: 10.1007/s10207-021-00545-8.

[31] S. Kalogiannidis, D. Kalfas, O. Papaevangelou, G. Giannarakis, and F. Chatzitheodoridis, "The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece," *Risks*, vol. 12, no. 2, Feb. 2024, doi: 10.3390/risks12020019.

[32] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing *cyber*–physical systems with hybrid *smart city cyber* security architecture for secure public data-smart network," *Future Generation Computer Systems*, vol. 112, pp. 724–737, Nov. 2020, doi: 10.1016/j.future.2020.06.028.

[33] V. S. Barletta, D. Caivano, M. De Vincentiis, A. Pal, and M. Scalera, "Hybrid quantum architecture for *smart city* security," *Journal of Systems and Software*, vol. 217, Nov. 2024, doi: 10.1016/j.jss.2024.112161.

[34] R. Devi E. M, N. Almakayeel, and E. L. Lydia, "Improved sand cat swarm optimization with deep learning based enhanced malicious activity recognition for *cyber*security," *Alexandria Engineering Journal*, vol. 98, pp. 187–198, Jul. 2024, doi: 10.1016/j.aej.2024.04.053.

[35] M. AlJamal, A. Mughaid, B. Al shboul, H. Bani-Salameh, S. Alzubi, and L. Abualigah, "Optimizing risk mitigation: A simulation-based model for detecting fake IoT clients in *smart city* environments," *Sustainable Computing: Informatics and Systems*, vol. 43, Sep. 2024, doi: 10.1016/j.suscom.2024.101019.

[36] B. Li, X. Yang, and X. Wu, "Role of net-zero renewable-based transportation systems in *smart cities* toward enhancing cultural diversity: Realistic model in digital twin," *Sustainable Energy Technologies and Assessments*, vol. 65, May 2024, doi: 10.1016/j.seta.2024.103715.

[37] H. Zhan, B. G. Hwang, H. Zhu, and S. H. P. Ang, "Towards a sustainable built environment industry in Singapore: Drivers, barriers, and strategies in the adoption of smart facilities management," *J Clean Prod*, vol. 425, Nov. 2023, doi: 10.1016/j.jclepro.2023.138726.

[38] D. Lee, S. L. Chao, and H. M. Chen, "Development of the AI Implementation *Framework* in Taipei City," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jun. 2024, pp. 90–103. doi: 10.1145/3657054.3657065.

[39] D. Adade and W. T. de Vries, "An extended TOE *framework* for local government technology adoption for citizen participation: insights for city digital twins for collaborative planning," 2024, *Emerald Publishing*. doi: 10.1108/TG-01-2024-0025.

[40] G. Bour, C. Bosco, R. Ugarelli, and M. G. Jaatun, "Water-Tight IoT–Just Add Security," *Journal of Cybersecurity and Privacy*, vol. 3, no. 1, pp. 76–94, Mar. 2023, doi: 10.3390/jcp3010006.