NAVIGATING THE DIGITAL THREAT: A PENTAHELIX APPROACH TO AI-DRIVEN DATA SECURITY IN SMART CITIES

Chasandra Puspitasari[1] and Antonio Heltra Pradana[2]

[1] Computer Science Department, Bina Nusantara University, Jakarta, Indonesia,
[2] Urban and Regional Planning Department, National Institute Technology, Malang, Indonesia
[1] chasandra.puspitasari@binus.ac.id
[2] antonioheltra@lecturer.itn.ac.id

Abstract

Smart cities provide creative approaches to urban growth, but they also face significant security and data management issues. The necessity for cooperative methods to safeguard sensitive data is highlighted by the rising incidence of cyberattacks and data misuse. To develop a shared responsibility for data protection in smart cities, this study uses the Pentahelix framework, which involves the government, academics, industry, communities, and media. A framework that guarantees accountability, transparency, and group control over data is developed by synthesizing pertinent literature, criticisms, and concepts using a qualitative descriptive method. Additionally, the use of artificial intelligence (AI) is examined as a challenge as well as an enabler. While AI improves data security by utilizing anomaly detection, predictive analytics, and automated response, it also poses issues related to ethical governance and privacy. The results imply that multi-stakeholder cooperation combined with AI-driven tactics can improve resilience against digital threats, guaranteeing smarter and safer urban ecosystems.

Keywords: **Smart City, Data Security, Data Management, Pentahelix, Artificial Intelligence Driven**

1. Introduction

The idea of the "smart city" has grown in importance in modern urban planning and government. The concept of smart cities has attracted international attention since its 1994 debut in Amsterdam and is currently being actively embraced worldwide. A smart city is an urban setting that incorporates cutting-edge infrastructure, sophisticated transit systems that improve population mobility, and renewable energy sources (Achmad, Nugroho, Djunaedi, & Widyawan, 2018). By creating energy-efficient homes, environmentally friendly buildings, and electronically integrated public services, these technologies not only maximize efficiency but also enhance people's quality of life. In Indonesia, the rapid digital transformation and growing internet connectivity that have occurred over the past 20 years are closely linked to the development of smart cities (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). The government plans to create at least 100 smart city projects in the next ten years, and it has already started more than fifty (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018). These kinds of projects demonstrate how governments and interested parties share the goal of building more livable, technologically sophisticated, and sustainable cities (Sucitawathi, Joniarta, & Dewi, 2018).

However, there are also significant drawbacks to the benefits presented by smart cities, especially when it comes to data management and security. The cybersecurity threats associated with smart cities are substantial due to the interconnectedness of devices and the vast amount of data produced by IoT sensors, surveillance systems, and digital platforms (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018). Technology's potential for exploitation increases with its sophistication. For both city officials and citizens, cyberattacks, data breaches, and the improper use of private information represent serious risks (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018). The public's confidence in smart city systems may be weakened, for instance, if compromised information on residential addresses, travel habits, or financial transactions were used for illegal activities like identity theft, fraud, or stalking (Braun, Fung, Iqbal, & Babar, 2018). This reality shows that smart cities are dynamic processes that change with their citizens and technology ecosystems, making safe, open, and cooperative data governance essential.

By analyzing how smart cities might use a Pentahelix framework in conjunction with artificial intelligence (AI) to handle digital risks, this article addresses these urgent issues. Government, academics, industry, communities, and the media are the five main stakeholders that the Pentahelix model highlights working together to ensure that data management is shared responsibly and transparently rather than being monopolized by one group (Calzada, 2020) (Founon, Hayar, & Haqiq, 2021).

Furthermore, many governance and security issues are fundamentally data-related challenges that we have traditionally depended on individuals to resolve. Therefore, the substantial burden of such mundane tasks can be alleviated by AI, which can undertake operations such as asset tagging, recognizing unstructured private data, detecting anomalous behavior, and monitoring data quality deviations (McKendrick, 2025) (Agarwal, Kumar, Chilakapati, & Abichandani, 2023). For example, if numerous security operations centers are contending with escalating demands and excessive alert levels AI agents may independently oversee hazards in real time, automate repetitive opera-tions with limited human involvement, and offer contextual decision-making assistance (Zoonen, Rijsohuwer, Leclercq, & Hirzalla, 2022). Also, AI offers revolutionary capabilities inside this cooperative framework by facilitating automated responses, real-time anomaly detection, and predictive analytics, all of which bolster cybersecurity defenses. Nevertheless, AI also presents new difficulties that need to be properly handled during the collaborative process, such as algorithmic bias and moral conundrums pertaining to privacy and surveillance (Calzada, 2020) (Tao & Zhang, 2021).

This study offers a conceptual method to improve resilience, accountability, and transparency in smart city data management by integrating AI-driven tactics into the Pentahelix framework. In the end, the study aims to show that, in a more digital and connected world, protecting the privacy, trust, and safety of its citizens must coexist with creating smarter cities.

1.1. Data Security Issue in Smart Cities

One of the most critical challenges in the systematic development of smart cities lies in the process of data acquisition (McKendrick, 2025). Implementing a smart city requires a vast array of sensors and continuous data inputs to generate smarter, more efficient, and effective urban decision-making. However, this reliance raises crucial questions: where, when, and how is such data collected, and to what extent are citizens informed about the monitoring of their daily activities? Without transparency and secure handling, data collection can become intrusive, undermining both public trust and the quality of governance (Achmad, Nugroho, Djunaedi, & Widyawan, 2018) (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). Furthermore, any disruption in the security of data acquisition or processing can lead to inaccurate insights, flawed decisions, and ultimately negative impacts on urban residents' lives as well as the long-term sustainability of the city (Braun, Fung, Iqbal, & Babar, 2018) (McKendrick, 2025). Thus, for smart cities to truly enhance efficiency and quality of life, citizens must feel both secure and empowered to participate in shaping their digitally connected environments.

The smart city paradigm is fundamentally built on interconnectivity, where diverse systems, services, and devices operate through shared digital platforms. Such connectivity demands robust infrastructure designs to ensure data security and privacy (Oliha, Biu, & Obi, 2024). However, because smart cities rely on heterogeneous and complex networks, they are exposed to diverse and multi-layered security risks. Even seemingly minor attacks or disruptions in data quality and availability can have severe consequences, threatening the reliability of services and the stability of cyberinfrastructure (Braun, Fung, Iqbal, & Babar, 2018) (Haque, Bhushan, & Dhiman, 2021) (Oliha, Biu, & Obi, 2024). The more a city integrates advanced technologies and interconnected systems, the more vulnerable it becomes to cyber threats. For example, disruptions in logistics, emergency response, or transportation systems caused by compromised infrastructure could result in enormous economic losses and erode public confidence in smart city initiatives (Rosenberg & Salam, 2017).

Real-world incidents have already illustrated the tangible risks (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). In Dallas, Texas, there was a case where hackers infiltrated the city's emergency siren system, triggering widespread disruption and panic among residents. Similarly, in Illinois in 2011, a group of hackers injected malicious code into a water utility control system, leaving more than 2,000 residents without access to clean water (Nakasihima, 2011). These examples underscore how breaches in data security within smart cities can move beyond digital inconvenience to real threats against public safety, health, and well-being.

In this context, this paper proposes a Pentahelix approach to navigating digital threats in smart cities, emphasizing shared responsibility among government, academia, industry, communities, and media. Artificial Intelligence (AI) is positioned as a key enabler in this framework, capable of detecting anomalies in real time, predicting potential attacks, and automating defensive responses (Ahmed, et al., 2021) (Bokhari & Myeong, 2023) (Agarwal, Kumar, Chilakapati, & Abichandani, 2023). At the same time, AI must be deployed ethically, with safeguards against misuse or bias. By embedding AI-driven mechanisms within multi-stakeholder collaboration, smart cities can establish a more resilient, transparent, and citizen-centered approach to data security (Calzada, 2016) (Choudhary, 2025) (Bokhari & Myeong, 2023).

The reality of cyber threats in Indonesia further demonstrates the urgency of robust data governance in smart city ecosystems. Table 1 illustrates several major data breach incidents that have occurred in recent years, affecting both private corporations and government institutions. For instance, the 2020 Tokopedia case exposed the personal data of 91 million users, including full names, phone numbers, and dates of birth, which were later traded on the dark web. Similarly, weaknesses in the Electronic Health Alert Card (eHAC) system between 2020–2021 compromised the personal and health information of 1.3 million users, high-lighting the vulnerability of critical public health infrastructure. Other incidents, such as the exposure of ride history and user data from Gojek and Grab (2016–2017), or the breach of Indonesia's universal healthcare program (BPJS) in 2021 affecting 279 million people, underscore the massive scale of potential harm when sensitive data is not adequately protected.

Financial institutions have also been significantly targeted. In 2021, BRI Life suffered a breach that exposed the banking details of 2 million customers, while the same year, over 720GB of health data were leaked from the Ministry of Health, later sold on dark web marketplaces. The 2022 breach of IndiHome and PLN further revealed the risks of compromised infrastructure, exposing 17 million records containing browsing histories, ID numbers, and energy consumption details. Even high-level government agencies were not immune: in 2021, a Chinese hacker infiltrated ten Indonesian government institutions, including the State Intelligence Agency (BIN), demonstrating the severity of state-level cyber vulnerabilities.

These cases emphasize that the threat landscape in Indonesia is both diverse and escalating, spanning personal, financial, health, and even national security data. From a smart city perspective, such breaches highlight the critical need for secure, multi-layered protection systems that can adapt to complex threats (Choudhary, 2025). This paper argues that adopting a Pentahelix framework, strengthened by AI-driven cybersecurity tools, provides a pathway to mitigate these risks. AI's predictive analytics and real-time threat detection can significantly reduce exposure, but sustainable resilience requires collaboration across government, academic, industry, communities, and media to ensure that data management is transparent, ethical, and inclusive (Ariyanto, Dewi, Hasibuan, & Paramadani, 2022) (Choudhary, 2025) (Kukkadapu, 2025). In this way, smart cities can advance toward greater efficiency and innovation without sacrificing the privacy and trust of their citizens.

Table 1. List of data breach in case of Indonesia

No	Year	Description	Data Hacked
1	2020	Personal data in Tokopedia was leaked. In two months, a full database with 91 million records appeared on the darknet for sale.	Full name, Emails, Phone Numbers, Dates of Birth, Marketing Data
2	2020-2021	Independent researchers have found that the electronic Health Alert Card (eHAC) can potentially compromise 1.3 million users. The app stored around 2 gigabytes of records on the unsecured database.	Health status, Personal Data, contact details, COVID-19 test results, Private Hospitals Records, Entire eHAC infrastructure
3	2016-2017	Major security flaws of Gojek and user personal data is exposed.	Ride History, Users Data, Pickup and Drop off points
4	2021	Indonesian universal healthcare program (BPJS) leaked social security data of 279 million people.	Personal Data, Full name, ID Card number, Dates of Birth, Salary Details
5	2021	BRI Life exposed banking details of 2 million customers.	Bank account details, Copies of ID card, Taxpayer details
6	2022	Data breach in ministry of health. There were 720GB of leaked data sold online in dark web market.	Health status, Personal Data, Contact details, Hospitals, Patient Photos, Lab results
7	2022	17 million of user data breached in Indihome and PLN.	ID cards, Name, Address, Energy Consumption, Browsing History, Domains, Platforms, URLs
8	2021	Chinese hacker managed to breach 10 Indonesian Government Agencies including BIN	Various state-confidential information

Source: (https://cyberlands.io/topsecuritybreachesindonesia)

The data breaches illustrated in the chart can be mitigated by more effectively utilizing advanced security technologies like blockchain, alongside enforcing stringent management of access to information and its extent. Pentahelix serves as a mechanism to augment the capacity for monitoring and preventing data leaks or breaches by distributing the responsibilities of oversight and technology necessities among stakeholders (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (Calzada, 2016) (Agung, 2025). Moreover, it can save the time and resources required for data management by decentralizing and enhancing the transparency of the data (Ariyanto, Dewi, Hasibuan, & Paramadani, 2022) (Jyothi, Sreelatha, Thiyagu, Sowndharya, & Arvinth, 2024).

1.2. Pentahelix as a Tool for Managing the Smart City

The Smart City idea is intrinsically multi-disciplinary and multidimensional, with technology, especially data and artificial intelligence (AI), as the main force behind innovation and governance (Calzada, 2020). Smart cities can make things more efficient and improve people's lives, but the quick digitalization of city systems also makes them more vulnerable. Cybercriminals frequently abuse sensitive personal information, financial records, and even vital infrastructure, creating hazards that can erode public trust and impair city operations (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018). The Pentahelix model offers a complete framework for dealing with these concerns by bringing together five important groups: the government, academia, industry, community/NGOs, and the media. This methodology not only encourages new ideas, but it also makes AI-driven data security stronger, which is important for building strong smart cities (Sudiana, Sule, Soemaryani, & Yunizar, 2020).

In the government sector, Public-Private Partnerships (PPP) are important tools for using the skills of the private sector while making sure that public interests and data protection are always the most important things. Governments may take the lead by making clear rules for cybersecurity, ethical AI policy, and quick-response systems to deal with breaches successfully (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). The academic and research sector is very important for coming up with new cybersecurity models, improving AI-driven intrusion detection systems, and coming up with evidence-based ways to prepare for new threats. Universities and research institutes create a knowledge ecosystem that helps smart cities grow safely by connecting theory and practice (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (Sucitawathi, Joniarta, & Dewi, 2018). The business and industry sectors, on the other hand, enable technology by creating safe platforms, encryption tools, and AI-based apps that can find and stop threats in real time (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018). Their innovative business ideas also draw in investors and skilled workers, which speeds up the use of modern security solutions in smart city ecosystems even more. On the other hand, the community and NGO sector make sure everyone is included by speaking up about people's worries about privacy, justice, and equity in how data is used. Their activism makes accountability stronger by making sure that governments and corporations stay open and work in the best interests of the people (Calzada, 2020).

Finally, the media has two jobs: to inform the public about smart city projects and the hazards they may pose, and to act as a watchdog that points out security flaws and calls for more openness. The media helps to establish public trust and get more people involved in protecting digital assets by keeping people informed. Using the Pentahelix model in smart city governance leads to a complete, safe, and citizen-centered way of building cities (Hall, 2015) (Agung, 2025) (Sudiana, Sule, Soemaryani, & Yunizar, 2020). It makes it possible for people to talk to each other, work together across sectors, and take responsibility for dealing with the problems that digital threats cause. For this model to work, cities need to set up collaborative platforms, forums, and digital governance systems that put AI-driven data protection first and make sure that everyone involved is open and accountable (Calzada, 2020) (Edwards, 2016). Smart cities can handle the challenges of digital transformation while protecting their most valuable asset: the trust of their citizens.

2. Methods

This study employs a qualitative descriptive framework, bolstered by an exploratory literature survey and comparative theme analysis. The qualitative method facilitates a comprehensive examination of the intricate socio-technical dynamics associated with AI-driven data security in smart cities, prioritizing interpretation and contextual comprehension rather than numerical generalization. Descriptive qualitative methodology is used to compile a full concept narrative of smart city security potential and data management integration opportunities in urban management through Pentahelix collaboration. This method is used to see from various relevant perspectives a collection of ideas/articles that can be used to build the concept of AI-Driven Smart City Security Data Management.

Data sources were mostly derived from peer-reviewed academic publications, conference proceedings, government policy documents, and industry reports published from 2020 to 2025. Esteemed resources including Scopus, IEEE Xplore, ScienceDirect, and SpringerLink were employed to obtain the latest and potential research concerning Pentahelix collaboration, AI governance, and blockchain-based security frameworks. Each publication was evaluated for its relevance to the primary research issues, concentrating on studies related to multi-stakeholder collaboration in digital governance, cybersecurity methods, and AI ethics in the context of smart cities.

The gathered materials underwent thematic categorization and comparative analysis. Initially, open coding was utilized to identify preliminary notions related to stakeholder roles, governance procedures, and developing security technologies. Thereafter, axial coding was employed to classify these notions into overarching themes, including regulatory synergy, technological innovation, community empowerment, and ethical data governance. A comparative analysis was conducted to examine various models of Pentahelix deployment across geographies and industries, facilitating the identification of common success factors and context-specific obstacles.

To guarantee study rigor and validity, triangulation was employed by contrasting findings from academic literature, policy frameworks, and empirical case studies of AI-driven smart city programs in Asia and Europe. The reliability of the findings was enhanced by cross-validating data interpretations and iteratively refining themes qualitatively. This methodological framework enhances analytical rigor while also offers a comprehensive view on how Pentahelix collaboration can implement secure, ethical, and sustainable digital ecosystems in smart cities.

3. Results and Discussion

3.1. Smart City on the Perspective of Urban Management

Smart cities offer transformative opportunities for more sustainable, efficient, and technology-centric urban environments, representing a paradigm shift in urban management. The primary goal of smart cities from an urban management perspective is to address the intricate challenges that accompany the rapid expansion of urban areas by utilizing advanced technologies, data analytics, and innovative governance models (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (Fernandez-Anez, Fernandez-Guell, & Giffinger, 2018) (Calzada, 2016). These cities endeavor to enhance service delivery, optimize resource allocation, and en-hance the overall quality of life for their residents (Sucitawathi, Joniarta, & Dewi, 2018) (Haque, Bhushan, & Dhiman, 2021). Nevertheless, the integration of AI-driven systems and interconnected infrastructures introduces significant cyber risks that cannot be discounted as cities become more digitally dependent (Tao & Zhang, 2021).

In smart cities, urban management is centered on several fundamental principles. The incorporation of data-driven decision-making is the primary objective, as it involves the use of real-time data from IoT sensors, smart infrastructure, and citizen input to inform urban policies and operations (Achmad, Nugroho, Djunaedi, & Widyawan, 2018) (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). Although this data-centric approach facilitates proactive problem-solving, predictive maintenance, and efficient re-source allocation, it also raises concerns regarding the security of managing and protecting such vast data flows from cyber threats. Furthermore, citizen engagement and inclusivity are essential, as smart cities enable residents to actively engage in urban planning and governance, thereby guaranteeing that their voices are heard and their needs are met. This engagement involves ensuring that communities are also engaged in discussions regarding data ethics, privacy, and digital security within the Pentahelix model.

Finally, smart cities are a comprehensive approach to urban development that considers technology, data, and citizen engagement in order to create more sustainable, efficient, and habitable urban spaces from an urban management perspective (Achmad, Nugroho, Djunaedi, & Widyawan, 2018) (Singh, Solanki, Sharma, Nayyar, & Paul, 2022). Yet, achieving these objectives requires more than just advanced technologies, it requires navigating the digital threats that emerge from increased connectivity. Smart cities can enhance AI-driven data security and guarantee transparency, accountability, and resilience by incorporating the Pentahelix approach, which unites government, academia, industry, community/NGOs, and media (Hall, 2015) (Tao & Zhang, 2021). Therefore, to achieve the desired outcomes of sustainability, inclusiveness, and citizen trust, urban management and digital security must be always coordinated.

3.2. Pentahelix as a Security Data Management in Smart Cities

As one of the latest concepts at the forefront of urban development, utilizing technology and data to improve the quality of life for their residents Smart City has its drawbacks when it comes to Security Data Management (Edwards, 2016). Central to the success of smart cities is the effective management of security data, ensuring the safety and privacy of citizens (Zoonen, Rijsohuwer, Leclercq, & Hirzalla, 2022). The Pentahelix approach, which expands upon the traditional Triple Helix model to include academia, media, and community alongside government and business, offers a comprehensive framework for managing security data in smart cities (Sudiana, Sule, Soemaryani, & Yunizar, 2020) (Agung, 2025). Thus, incorporating the Pentahelix approach into smart city security data management brings a multi-stakeholder perspective to the forefront (Calzada, 2016) (Calzada, 2020). By engaging all five sectors, smart cities can navigate the complex terrain of security data management while fostering innovation, inclusivity, and public trust.

To transform the abstract notion of Pentahelix collaboration into a tangible and operational reality, the framework requires the formation of a formal governing body. The "board of stakeholders" illustrated in the conceptual model must be established as a legally recognized Smart City Data Governance Council or Data Trust. This council then serves as the central node for decision-making, policy creation and enforcement, and stakeholder coordination. Thus, moving the model from an informal partnership to a structured institution for co-creation and shared responsibility.

Furthermore, the role of each stakeholder can be seen in Figure 1 below.

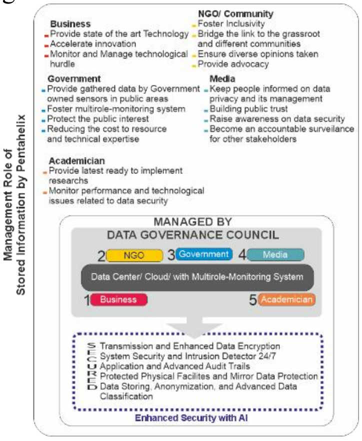
Management Role of Stored Information by Pentahelix
Business
Provide state of the art Technology
Accelerate innovation
Monitor and Manage technological hurdle
NGO/ Community
Foster Inclusivity
Bridge the link to the grassroot and different communities
Ensure diverse opinions taken
Provide advocacy
Government
Provide gathered data by Government owned sensors in public areas
Foster multirole-monitoring system
Protect the public interest
Reducing the cost to resource and technical expertise
Media
Keep people informed on data privacy and its management
Building public trust
Raise awareness on data security
Become an accountable surveilance for other stakeholders
Academician
Provide latest ready to implement researchs
Monitor performance and technological issues related to data security
MANAGED BY
DATA GOVERNANCE COUNCIL
2 NGO
3 Government
4 Media
Data Center/ Cloud/ with Multirole-Monitoring System
1 Business
5 Academician
SECURED
Transmission and Enhanced Data Encryption
System Security and Intrusion Detector 24/7
Application and Advanced Audit Trails
Protected Physical Facilites and Mirror Data Protection
Data Storing, Anonymization, and Advanced Data Classification
Enhanced Security with AI

Fig. 1. Management Role of Stored Information with Pentahelix Approach

To achieve effective security data management in smart cities several critical components should be addressed. First is the establishment of robust cybersecurity measures to protect against data breaches and cyberattacks (Singh, Solanki, Sharma, Nayyar, & Paul, 2022) (McKendrick, 2025). This includes encryption, authentication protocols, and continuous monitoring of data networks (Braun, Fung, Iqbal, & Babar, 2018). Additionally, data anonymization and privacy-enhancing technologies should be employed to safeguard sensitive information while allowing for legitimate data analysis. Regular audits and compliance checks ensure that security measures remain up-to-date and effective. Citizen engagement and education are equally important, as residents should be aware of how their data is used and have a say in security policies. Thus, the Pentahelix approach empowers smart cities to manage security data comprehensively, fostering a safe and resilient urban environment while respecting individual rights and privacy concerns (Agarwal, Kumar, Chilakapati, & Abichandani, 2023) (Calzada, 2016) (Calzada, 2020).

The implementation of the Pentahelix model in AI-driven data security depends on the cohesive integration and interdependence of roles across all five stakeholders. Governments are essential in creating comprehensive digital policies and implementing strong regulatory frameworks that guarantee adherence to international cybersecurity standards, including ISO/IEC 27001, the NIST Cybersecurity Framework, and GDPR-like data protection rules (Ali, et al., 2025) (Bokhari & Myeong, 2023). In addition to regulation, governments enable funding for digital innovation and establish national cybersecurity task groups to monitor threats, coordinate responses, and promote ethical AI implementation in smart city (Choudhary, 2025).

Business or Industries, as the technology facilitators, contribute by designing, developing, and deploying AI-driven cybersecurity solutions that work seamlessly within the smart city framework. This encompasses advanced intrusion detection systems that can detect anomalies in real time, automated threat intelligence platforms utilizing machine learning for predictive protection, and blockchain-based identity management systems that improve data integrity and traceability (Haque, Bhushan, & Dhiman, 2021) (Hayouni & Nasraoui, 2025). While the specifically private sector could engage with public institutions via public–private partnerships (PPP) to jointly construct safe infra-structures and guarantee that this innovation corresponds with national security needs.

The third role, which is academia serves as the intellectual engine of this Pentahelix model. Universities and research institutions promote theoretical and practical investigations in explainable AI (XAI) (Lahby, Kose, & Bhoi, 2021), federated learning, privacy-preserving computation, and secure distributed systems. Academic research offers frameworks for evaluating ethical implications, alleviating algorithmic prejudice, and enhancing AI transparency. Their role can also connect technology innovation and policy implementation through collaborative research funding and inter-disciplinary institutions, generating evidence-based proposals for digital governance (Oliha, Biu, & Obi, 2024).

NGOs or Communities function as both beneficiaries and active contributors within smart city cybersecurity eco-systems. Their tasks encompass active participation in co-designing solutions, involvement in data literacy initiatives, and the promotion of a culture of cyber awareness, rather than only providing data passively. Community-driven efforts, such local digital literacy workshops, citizen reporting systems, and open data hackathons, bolster resilience by instilling security awareness at the grassroots level. This interaction promotes inclusivity by addressing digital barriers that could impede equitable access to safe digital services and the smarter city (Ariyanto, Dewi, Hasibuan, & Paramadani, 2022).

Media organizations serve as the essential link that promotes transparency and accountability inside the system (Oliha, Biu, & Obi, 2024). They distribute validated information regarding cybersecurity events, instruct the public on safe technology usage, and serve as monitors against misinformation. Media institutions utilize investigative journalism and digital campaigns to ensure accountability of both public and private entities in upholding ethical standards in data governance. Furthermore, nascent digital media platforms employ AI for fact-checking and risk communication, thus directly enhancing the resilience of smart city information ecosystems.

The integration of these five components establishes a dynamic and adaptable governance environment in which data security transcends a mere technical issue, becoming a collective social obligation. The efficacy of this operationalization relies on ongoing coordination, transparent data-sharing mechanisms, and reciprocal trust among all Pentahelix stakeholders.

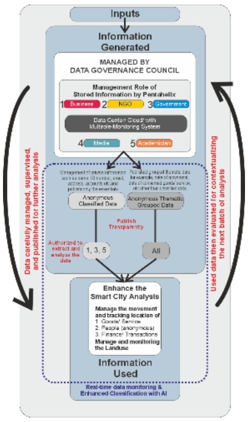
Inputs
Information Generated
MANAGED BY DATA GOVERNANCE COUNCIL
Management Role of Stored Information by Pentahelix
1 Business
2 NGO
3 Government
Data Center Cloud' with Multirole-Monitoring System
4 Media
5 Academician
Management of private information such as name, ID number, email, address, accounts etc and publish only the essentials
Published grouped thematic data for example, data of movement, data of consumed goods/service, etc other than classified data
Anonymous Classified Data
Anonymous Thematic Grouped Data
Publish Transparency
Authorized to extract and analyze the data
1, 3, 5
All
Data carefully managed, supervised, and published for further analysis
Used data then evaluated for contextualizing the next batch of analysis
Enhance the Smart City Analysis
Manage the movement and tracking location of
1. Goods/ Service
2. People (anonymous)
3. Finance/ Transactions
Manage and monitoring the Landuse
Information Used
Real-time data monitoring & Enhanced Classification with AI

Fig. 2. Smart City Security Data Management with Pentahelix Approach and AI Enhancement

3.3. Operation and Technical Implementation

The diagram above (Figure 2) illustrates the management role of data processing in a Smart City to ensure robust AI-driven security and protect citizens' privacy. This conceptual framework operates on three main ideas that align with AI framework of the Pentahelix approach.

- The management of gathered information. The massive volume of data generated from IoT devices, urban sensors, and voluntary citizen input should be managed collaboratively by a board of stakeholders consisting of government agents, industry/business, academia, community/NGOs, and the media. Within this board, AI technologies can be leveraged to continuously monitor, classify, and strengthen data security mechanisms such as blockchain-based validation and anomaly detection (Majumdar & Awasthi, 2025). Data is then published transparently under two classifications. The first is Anonymous Classified Data, where information is published without personal identifiers and can be used by government, academia, and industry for urban management in fields such as health, education, welfare, and public safety. The second is Anonymous Thematic Grouped Data, where data is anonymized and organized thematically, such as traffic flow, congestion points, distribution of goods and services, or financial transaction trends. By embedding AI-driven safeguards, each stakeholder not only manages but also co-secures and validates the availability of trustworthy data for collective decision-making (Bokhari & Myeong, 2023).
- The usage of the gathered information into meaningful AI-driven analysis. From an urban management perspective, the two main concerns are (a) the movement of goods, services, people, and financial transactions, and (b) spatial dynamics such as land use changes. Through AI-based data analytics, the board can filter, contextualize, and translate raw data into actionable insights while preventing overexposure of irrelevant or sensitive details (Majumdar & Awasthi, 2025). This ensures that analysis remains efficient, secure, and purpose-driven, minimizing the risk of data leakage to unauthorized parties while maximizing value for policy and urban innovation.
- The feedback loops for contextualization and resilience. After analysis, the information is reintegrated into the data-gathering stage for validation and refinement. AI models enable continuous learning by identifying patterns, detecting anomalies, and flagging sensitive data that should not be reused. This feedback cycle ensures that only relevant, non-sensitive, and ethically sound datasets are circulated, thus maintaining both contextual relevance and data security across the lifecycle of smart city management.

By embedding AI-driven mechanisms into this Pentahelix-based governance structure, smart cities can not only improve efficiency and inclusivity but also strengthen resilience against digital threats, ensuring that urban transformation remains both innovative and secure (Kumpf, et al., 2025).

3.4. The Hurdle of Implementing the Pentahelix

While the opportunity to implement is high and the potential to safer smart city data management is good, the Pentahelix model, by its very nature, brings together stakeholders with fundamentally different motivations and objectives (Agung, 2025). For example, the tension commonly found between the Public-Private Partnerships (PPPs) that are central to most smart city developments, pitting the public-good mandate of government against the profit-driven motives of the private sector.

These conflicts are not merely theoretical but manifest in tangible, detrimental outcomes that have been observed in early smart city projects. These include the creation of proprietary and isolated "data islands," where valuable information is siloed within a single company's ecosystem; the emergence of significant information security risks as commercial priorities override robust security practices; the development of so-called "zombie apps" that serve a corporate purpose but provide little public value; and, in the worst cases, the complete breakdown of public-private cooperation, leading to stalled projects and wasted public funds (Founon, Hayar, & Haqiq, 2021). Also, the private sector's legitimate need to generate a return on investment can lead to practices such as vendor lock-in, where a city becomes dependent on a single proprietary technology, and the monetization of citizen data in ways that may compromise privacy.

This central conflict can be understood as a multi-party game theory problem focused on the control of data. The primary function of the Pentahelix governance framework, therefore, is to fundamentally change the rules and payoffs of this game, shifting the equilibrium from competition to cooperation. The framework must therefore address both the technical dimension (interoperability protocols) and the social dimension (trust-building mechanisms) of the problem in implementing this conceptual framework (Singh, Solanki, Sharma, Nayyar, & Paul, 2022).

On the other hand, effective Pentahelix collaboration is predicated on the active and meaningful participation of all five stakeholder groups. But the common capacity gaps remain, such as insufficient human resources, particularly a lack of personnel with advanced data science and cybersecurity skills; severe financial constraints, especially for community organizations and smaller academic institutions; inadequate or unevenly distributed digital infrastructure; and persistent low levels of community engagement due to a lack of resources and organizational support. A brief mapping of these asymmetries below reveals the scale of the hurdle to implement the concept.

For the industry, while possesses high technical and financial capacity but may have low capacity for understanding public policy nuances or social equity concerns. While on the Government side, it holds high regulatory and legal capacity but often exhibits low technical agility and operational speed. On the Academia, they have high theoretical and research capacity but often lacks the resources or mandate for rapid, practical implementation. On the Community, they possess high local knowledge and legitimacy but typically have low technical, financial, and organizational capacity in smart city implementation, especially the technology acquisition and adaptation. While the media has high communication and dissemination capacity but may lack the deep technical expertise required for critical analysis and oversight.

If this system is left to its own devices, the inevitable outcome is a de facto technocracy run by a coalition of industry and government actors, with academia serving as an occasional consultant and the community and media relegated to the role of passive observers. This outcome would entirely negate the democratic and inclusive premise of the Pentahelix model. Therefore, a formal, funded Capacity Building Program is not an optional add-on but a core, non-negotiable operational requirement for the framework to succeed.

To address the hurdle and challenges, the program, which should be managed and overseen by the Data Governance Council, must be designed to facilitate cross-helix knowledge transfer and actively rebalance power distribution (Sudiana, Sule, Soemaryani, & Yunizar, 2020). For the first part, it is about leveling the stakeholder's digital literacy to the same playing field (Agung, 2025). This includes technical training for non-technical stakeholders, policy and ethics education for technical stakeholders, actively allocating resources for under-resourced groups such as NGOs and community groups. And lastly, creating programs where media fellows are embedded with the city's technical teams to foster deeper, more accurate reporting, and where community organizers are seconded to government planning departments to ensure local perspectives are integrated into policy development (Bokhari & Myeong, 2023).

This active, intentional, and continuous rebalancing of capacity is essential for the legitimacy, resilience, and ultimate success of the Pentahelix governance framework. Ultimately, these concerns must be weighed against the technical difficulties posed by the implementation of AI and smart city technology. Consequently, ongoing digital literacy and communication must be fostered to enable autonomous operation of smart city data management systems by AI, while ensuring comprehensive oversight by stakeholders on an equitable basis.

4. Conclusion

The integration of a Pentahelix collaboration model with advanced AI and Blockchain technology presents a promising, though intricate, approach to creating secure, resilient, and citizen-focused data governance in smart cities. The implementation of this conceptual framework relies on an advanced technical architecture defined by a cyclical data lifecycle, an interdependent interaction between AI and blockchain, and a structured governance system represented by a multi-stakeholder Data Governance Council.

From the above conceptualization, Pentahelix collaboration in the information collection stage emerges as a crucial strategy to ensure that data published in cyberspace is anonymized yet still relevant for AI-driven urban management analysis. By embedding AI into data governance, the anonymization process can be automated and reinforced through advanced techniques such as machine learning–based anomaly detection, encryption algorithms, and automated credential stripping. This ensures that sensitive information is consistently removed while maintaining the contextual accuracy required for decision-making. At the same time, Pentahelix collaboration strengthens data supervision, as the government, business sector, and academia play key roles in adopting and advancing emerging technologies for encryption, blockchain validation, and cyber-defense. AI systems further support this process by enabling predictive monitoring of potential breaches and continuous adaptation to evolving cyber threats. Once supervised, encrypted, and stripped of private identifiers, the data can then be used to refine Smart City analysis—including the monitoring of logistics and service flows, mobility of people, financial transactions, and spatial planning and utilization—without compromising privacy. This architecture is engineered for adaptability, with reflexive feedback loops that facilitate ongoing learning and iterative policy enhancement, hence assuring the system's accountability to the population it serves.

The shift from concept to reality requires actively confronting a number of significant implementation problems. Conflicts of interest in public-private partnerships must be addressed by restructuring the strategic framework of data governance through enforced open standards and impartial data management, thus harmonizing corporate interests with the public benefit. The significant disparities in capacity among stakeholder groups must be addressed by a sustained capacity-building initiative, guaranteeing that all voices, especially those from the community, can engage meaningfully in government.

Finally, by confronting these challenges with targeted, integrated technical and governance strategies, smart cities can navigate the digital threat and build an urban future that is not only more efficient and innovative but also more equitable, trustworthy, and secure. Furthermore, the proposed concept of integrating Pentahelix collaboration with AI-driven data security highlights the need for future research supported by measurable statistical analysis and technical validation. This includes systematically mapping the interconnections between stakeholders, weighing up their roles in ensuring data security, and conducting in-depth technical evaluations of AI applications in urban governance. Such efforts will not only strengthen resilience against digital threats but at the end of the day protect the population and also ensure that smart city development remains inclusive, secure, and sustainable.

Reference:

Achmad, K. A., Nugroho, L. E., Djunaedi, A., & Widyawan, W. (2018). Smart City Readiness based on Smart City Council's. *International Journal of Electrical and Computer Engineering, 8*, 271-279.

Agarwal, A., Kumar, S., Chilakapati, P., & Abichandani, S. (2023). Artificial Intelligence in Data Governance Enhancing Security and Compliance in Enterprise Environments. *Nanotechnology Perceptions, 19*(S1), 235-252.

Agung, M. F. (2025). Strengthening Governance Through Pentahelix Collaboration: A Qualitative Study in The Era Of Digital Disruptions. *Journal Publicuho, 8*(3), 1619-1626. doi:10.35817/publicuho.v8i3.873

Ahmed, S., Hossain, M. F., Kaiser, M. S., Noor, M. B., Mahmud, M., & Chakraborty, C. (2021). Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. In C. Chakraborty, J. C.-W. Lin, & M. Alazab (Eds.), *Data-Driven Mining, Learning and Analytics for Secured Smart Cities. Advanced Sciences and Technologies for Security Applications.* (pp. 23-47). Cham: Springer. doi:10.1007/978-3-030-72139-8_2

Ali, J., Singh, S. K., Jiang, W., Alenezi, A. M., Islam, M., Daradkeh, Y. I., & Mehmood, A. (2025). A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Computer Communications, 2025*(10800), 1-27. doi:10.1016/j.comcom.2024.108000

Ariyanto, D., Dewi, A. A., Hasibuan, H. T., & Paramadani, R. B. (2022). The Success of Information Systems and Sustainable Information Society: Measuring the Implementation of a Village Financial System. *Sustainability, 14*, 3851.

Bokhari, S. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. *IEEE Access, 11*, 69783-69797. doi:10.1109/ACCESS.2023.3293480

Braun, T., Fung, B. C., Iqbal, F., & Babar, S. (2018). Security and Privacy Challenges in Smart Cities. *Sustainable Cities and Society, 39*, 499-507.

Calzada, I. (2016). (Un)Plugging smart cities with urban transformations: Towards multistakeholder city-regional complex urbanity? *URBS Rev. Estud. Urbanos Cienc. Soc, 6*, 25-45.

Calzada, I. (2020). Democratising Smart Cities? Penta-Helix Multistakeholder Social Innovation Framework. *Smart Cities, 3*, 1145-1173.

Choudhary, S. K. (2025). AI-Driven Data Governance and Security in Real-time Cloud Integration. *International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 8*(1), 3139-3156.

Edwards, L. (2016). Privacy, security and data protection in smart cities: a critical EU law perspective. *European Data Protection Law Review (Lexxion)*, 1-37.

Fernandez-Anez, V., Fernandez-Guell, J. M., & Giffinger, R. (2018). Smart City Implementation and Discourse: An integrated. *Cities, 78*, 4-16.

Founon, A., Hayar, A., & Haqiq, A. (2021). Regulation and Local Initiative of the Development of Smart Cities-Sustainable Penta-Helix Approach. *International Journal on "Technical and Pyhsical Problems of Engineering", 13*(48), 55-61.

Hall, D. (2015). *Why Public-Private partnership Don't Work: The May Advantages of the Public Alternative.* London: University of Greenwich.

Haque, A. K., Bhushan, B., & Dhiman, G. (2021). Conceptualizing smart city applications: Requirements, Architecture. *Expert System, 38*, 1-23.

Hayouni, H., & Nasraoui, L. (2025). NAIDS4IoT: A Novel Artificial Intelligence-Based Intrusion Detection Architecture for the Internet of Things. *Intelligencia Artificial, 28*(76), 253-282. doi:10.4114/intartif.vol28iss76pp253-282

Jyothi, D., Sreelatha, D. T., Thiyagu, D., Sowndharya, R., & Arvinth, N. (2024). A Data Management System for Smart Cities Leveraging Artificial Intelligence Modeling Techniques to Enhance Privacy and

Security. *Journal of Internet Services and Information Security, 14*(1), 37-51. doi:10.58346/JISIS.2024.I1.003

Kukkadapu, G. (2025). AI-Driven Security Architecture in Smart Cities: Balancing Safety and Privacy. *European Journal of Computer Science and Information Technology, 13*(47), 86-94. doi:10.37745/ejcsit.2013/vol13n478694

Kumpf, K., Cajic, M., Zeljkovic, V., Mravik, M., Zivkovic, M., Mani, J., . . . Bacanin, N. (2025). Tackling smart city security: deep learning approach utilizing feature selection and two-level cooperative framework optimized by adapted metaheuristics algorithm. *International Journal of Information Security, 24*(221), 1-35. doi:10.1007/s10207-025-01137-6

Lahby, M., Kose, U., & Bhoi, A. K. (2021). *Explainable Artificial Intelligence for Smart Cities.* Boca Raton: CRC Press.

Lyu, Q., Liu, S., & Shang, Z. (2025). Securing Urban Landscape: Cybersecurity Mechanisms for Resilient Smart Cities. *IEEE Access, 13*, 10966-10977. doi:10.1109/ACCESS.2024.3522078

Majumdar, S., & Awasthi, A. (2025). From Vulnerability to Resilience: Securing Public Safety GPS and Location Services with Smart Radio, Blockchain, and AI-Driven Adaptability. *Electronics, 14*(1207), 1-19. doi:10.3390/electronics14061207

McKendrick, J. (2025, April 10). *Reimagining Data Governance and Security in the Era of AI and Fast-Moving Data*. Retrieved September 14, 2025, from Database Trends and Applications: https://www.dbta.com/Editorial/Trends-andApplications/Reimagining-Data-Governance-and-Security-in-the-Era-of-AI-and-Fast-Moving-Data169127.aspx?PageNum=1

Nakasihima, E. (2011, November 18). *Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says*. Retrieved September 10, 2025, from Thw Washington Post: ttps://www.washingtonpost.com/blogs/checkpointwashington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expertsays/2011/11/18/gIQAgmTZYN_blog.html

Oliha, J. S., Biu, P. W., & Obi, O. C. (2024). Securing the smart city: A review of cybersecurity challenges and strategies . *Journal of Multidisciplinary Studies*, 94-101.

Rosenberg, E., & Salam, M. (2017, April 8). *Hacking Attack Woke Up Dallas With Emergency Sirens, Officials Say*. Retrieved September 10, 2025, from New York Times: https://www.nytimes.com/2017/04/08/us/dallas-emergency-sirenshacking.html

Sefati, S. S., Arasteh, B., Halunga, S., & Fratu, O. (2025). A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT). *Cluster Computing, 28*(792), 1-42. doi:10.1007/s10586-025-05449-z

Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., & Paul, A. (2022). A Decade Review on Smart Cities: Paradigms, Challenges. *IEEE Access, 10*, 68319-68364.

Sucitawathi, I. D., Joniarta, W., & Dewi, Y. (2018). Konsep “Smart City” Dan Tata Kelola Pemerintahan Di Kota Denpasar. *Jurnal Administrasi Publik, 3*(1), 9-15.

Sudiana, K., Sule, E. T., Soemaryani, I., & Yunizar, Y. (2020). The Development and Validation of the Pentahelix Construct. *Verslas: Teorija ir praktika / Business: Theory and Practice, 21*(1), 136-145.

Tao, X., & Zhang, H. (2021). Research on Data Security Governance based on Artificial Intelligence Technology. *2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR)* (pp. 102-105). Shanghai, China: IEEE.

Zoonen, L. v., Rijsohuwer, E., Leclercq, E., & Hirzalla, F. (2022). Privacy Behavior in Smart Cities. *International Journal of Urban Planning and Smart Cities, 3*(1), 1-17.