



Paper Type: Original Article

AI-Assisted Network Security in Smart City IoT Frameworks

Priyansh Sahu* 

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22054071@kiit.ac.in.

Citation:

Received: 25 January 2025

Revised: 28 March 2025

Accepted: 01 May 2025

Sahu, P. (2025). AI-assisted network security in smart city IoT frameworks. *Metaversalize*, 2(2), 60-68.

Abstract

As cities transform into smart cities, they are increasingly filled with Internet of Things (IoT) devices that bring new challenges to keeping networks secure. This paper explores how Artificial Intelligence (AI) can be a game changer for network security in these smart city environments. It discusses how AI can improve traditional security by providing real-time threat detection, automated reactions, and forward-looking threat analysis. We particularly look at how machine learning can power Intrusion Detection Systems (IDS) to spot unusual patterns in network traffic, helping to predict and mitigate potential threats more accurately. We also explore how reinforcement learning can dynamically tweak network settings to enhance security while efficiently using resources. These AI-driven techniques speed up response times compared to manual methods and boost the precision of detecting real threats while minimizing false alarms. This study highlights AI's vital role in safeguarding critical urban infrastructure like energy grids, transport systems, and healthcare networks. It also considers the complexities AI introduces, such as issues with privacy, potential biases, and the need for clear system transparency, pointing out that these issues require thoughtful consideration as we apply AI in smart city security.


Keywords: Artificial intelligence, Security, Smart cities, Predictive threat analysis, Intrusion detection systems.

1 | Introduction

Smart cities are changing how we live, connecting everything from traffic lights to power grids with Internet of Things (IoT) devices [1], [2]. But as our urban spaces become smarter, they face new security challenges. Traditional security methods can't keep up with the scale and complexity of these interconnected systems. This is where Artificial Intelligence (AI) steps in, offering a new layer of protection with its ability to detect threats in real-time, automate responses, and predict future risks [3–5].

Recent developments in AI are proving to be a game changer. For instance, AI-powered systems can now analyze vast amounts of data from traffic patterns and spot anomalies that could signify a threat, all without

 Corresponding Author: 22054071@kiit.ac.in

 <https://doi.org/10.22105/metaverse.v2i2.76>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

a human having to lift a finger. This kind of automation is making our cities smarter and safer. Wolniak and Stecula [6] highlights the broad applications of AI in improving city operations across various sectors, including public safety.



Fig. 1. The broad applications of AI.

In terms of public safety, AI's impact has been particularly noteworthy. It's been instrumental in enhancing how emergency services respond to disasters and manage crises, effectively saving lives and resources. For example, AI helps emergency managers deal with everything from floods to wildfires by predicting these events before they happen and strategizing effective responses. Koormala et al. [7] discusses how these AI systems assist in real-time decision-making during critical public safety scenarios, a testament to AI's growing role in our urban environments.

However, with all these technological advances, there are legitimate concerns about privacy, transparency, and the potential biases within AI systems. These are not just technical challenges but ethical ones, too, and they require us to think carefully about how we deploy AI in our smart cities. This paper dives into how AI can fortify the security frameworks of IoT networks in smart cities, balancing the technological benefits against the ethical considerations to help build urban environments that are smart, secure, and respectful of our rights and freedoms [8].

Still, implementing AI-based security raises important concerns, such as privacy risks, system transparency, and algorithm biases. This study explores how AI can strengthen IoT networks in smart cities while addressing these challenges, ultimately building safer and more adaptive urban environments.

2 | AI-Powered Security Framework

At the heart of every smart city, there's a central system—think of it as the brain of the operation. Often based in the cloud, this hub tirelessly collects and analyzes data from countless IoT devices scattered throughout the city. It keeps an eye out for anything unusual, like unexpected data flows or odd behavior from devices, ensuring everything runs smoothly and securely. Here's a closer look at how it all works [9].

Anomaly detection: Imagine having a highly intuitive detective that never sleeps. That's what our machine learning algorithms are like. They're constantly learning and improving, making them great at spotting security threats that might slip past more traditional systems. This early detection is key to stopping potential breaches before they can do any harm.

Predictive analytics: Our system doesn't just react to threats; it predicts them. Analyzing patterns and trends from past data can help anticipate where vulnerabilities might occur next. This foresight allows us to be proactive, fortifying weak spots before they're exploited.

Automated responses: When a threat is detected, time is wasted. That's where automated responses come in. The system can make quick decisions, like isolating a compromised device or tweaking settings to shut down an attack pathway, all without needing a human to step in. This swift action helps keep critical city services running without interruption.

2.1| The Role of AI in Enhancing Cybersecurity

AI is stepping up as a game-changer for smart city cybersecurity by providing not just monitoring but real-time, proactive protection. Here's how it's helping to secure our digital spaces [10]:

- I. **Intrusion detection and prevention:** Think of AI-powered Intrusion Detection Systems (IDS) [11] as digital security guards, constantly watching over network traffic to spot unusual or unauthorized access. They scan for any activity that doesn't look right—like someone trying to access data, they shouldn't—and take immediate action to block potential threats. This helps create a secure boundary around critical digital infrastructure, essential as cities get more connected and data-heavy.
- II. **Adaptive learning with reinforcement learning:** AI systems today don't just respond to attacks; they learn from them. Using reinforcement learning, they adapt based on past experiences, like rerouting data or enhancing defenses in real time. This way, if a similar attack occurs, the system has already "learned" from previous events and is equipped to handle it better. It's a bit like the city learning its defense strategies to stay one step ahead of evolving cyber threats.
- III. **Anomaly detection for user and device behavior:** AI also uses behavioral analysis to understand what "normal" activity looks like across city networks. If something doesn't fit—a device accessing restricted files or transferring data in an unusual way—the system quickly flags it. This is particularly useful for spotting insider threats or compromised devices, especially where critical infrastructure is at stake.
- IV. **Secure data encryption:** Data security is essential as it moves across a smart city's network, from sensors on the streets to central control hubs. AI doesn't just apply standard encryption but adjusts and strengthens these protocols dynamically based on the type and sensitivity of the data. This keeps eavesdropping and tampering at bay while safeguarding the privacy of city residents.
- V. **Real-time threat intelligence:** AI systems pull from large datasets of past cyber incidents to recognize patterns in attacks, enabling them to anticipate and prepare for emerging threats. This proactive approach means smart city systems are ready for certain types of attacks before they even happen, issuing alerts to security teams in real-time for quicker response.

Together, these technologies form an adaptable, intelligent cybersecurity framework. They don't just react to issues; they evolve with them, reinforcing the city's defenses in real time. With AI, cities can be smarter and safer, creating an environment where residents' data and public infrastructure are well-protected.

3| Advantages and Disadvantages

While the benefits of AI-assisted network security in smart cities are substantial, some notable challenges accompany its implementation [12].

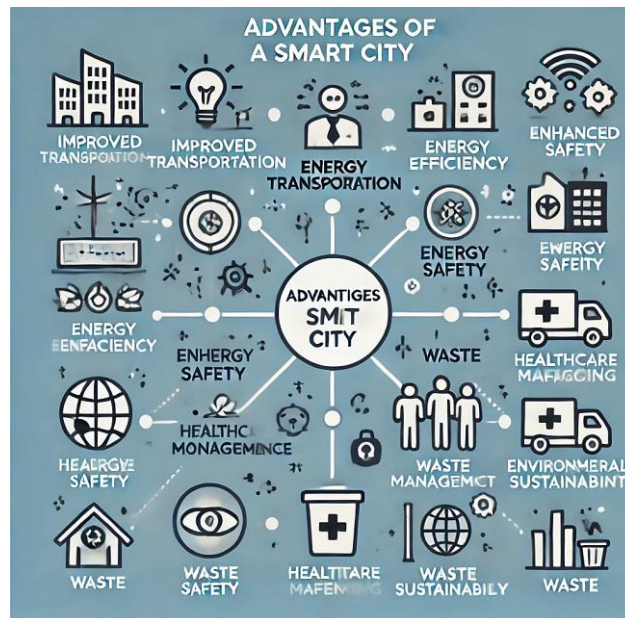


Fig. 2. Advantages of a smart city.

Enhanced threat detection: AI's capability to analyze large datasets in real-time increases the accuracy of detecting potential threats before they escalate.

Automated threat response: AI-driven automation ensures a rapid response, minimizing the impact of cyberattacks on essential city services.

Scalability: AI frameworks can evolve with growing numbers of IoT devices and adapt to emerging attack patterns, making them a future-ready solution for urban environments [13].

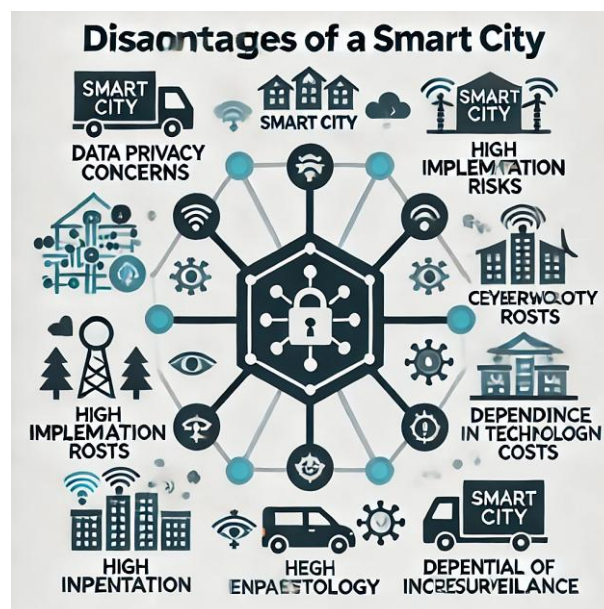


Fig. 3. Disadvantages of a smart city.

Privacy concerns: The extensive data collection for AI raises questions about user privacy and data security.

Algorithmic bias: Without careful monitoring, AI systems can reflect biases in their training data, potentially leading to unfair or less effective security responses.

Complexity: Integrating AI into security frameworks requires specialized expertise and additional resources for smooth implementation.

3.1 | Addressing Challenges in AI Integration

The integration of AI into smart city security frameworks brings specific challenges that need attention for ethical and effective deployment.

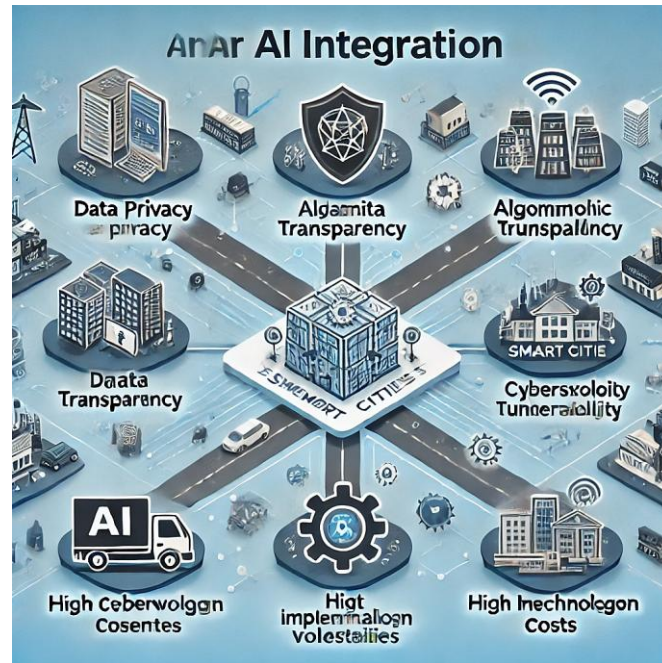


Fig. 4. AI integration.

- I. **Data privacy:** The extensive data required by AI-powered systems raises privacy concerns, as managing personal information securely is crucial to maintaining public trust. Cities can address these challenges by implementing stringent data governance policies that mandate responsible data collection, secure storage, and transparent usage practices. These measures help balance data accessibility with privacy protection, reducing risks associated with AI-powered surveillance and citizen data management [14].
- II. **Algorithmic transparency:** One of the significant concerns with AI in public systems is the "black box" effect, where AI decision-making processes are often difficult to interpret. This can complicate security management and public accountability. To overcome this, developing explainable AI models can ensure city officials, security teams, and citizens understand how decisions are made. Transparent algorithms foster accountability and help detect and correct biases, creating a fairer application of AI in public services.
- III. **Cybersecurity and vulnerability to attacks:** AI systems in interconnected smart city networks become potential targets for cyberattacks, which can compromise critical infrastructure. Protecting these systems requires a proactive approach that includes regular updates to AI models, frequent security audits, and implementing robust defensive mechanisms. Cities can look to examples like Singapore, which employs a layered cybersecurity strategy to secure its AI-driven traffic and energy systems from threats. This combination of preemptive security and vigilant monitoring strengthens the resilience of AI infrastructure [15].
- IV. **Funding and investment constraints:** Securing sustainable funding for smart city projects, especially those requiring AI integration, remains a hurdle, particularly for developing regions. Addressing this challenge involves public-private partnerships and innovative financing mechanisms enabling cities to allocate resources effectively. For example, Copenhagen and Singapore have successfully collaborated with private sectors to support AI initiatives in traffic and energy management areas.

These solutions underscore the need for cities to strategically navigate AI's integration, leveraging its potential while addressing ethical, security, and financial concerns to foster a safer, efficient, and citizen-centered smart city infrastructure [16].

4 | Use Cases and Data Flow

AI-driven security solutions are transforming urban management across multiple sectors. Here's how they're making a real-world impact.



Fig. 5. AI-driven security solutions.

- I. **Smart traffic management:** AI processes real-time data from cameras and sensors to reduce congestion, dynamically adjusting traffic signals based on current traffic patterns. In practice, this can ease urban gridlock and make commuting faster and safer for city dwellers. By reducing traffic jams and improving flow, cities can reduce pollution and enhance road safety.
- II. **Energy grid optimization:** To manage electricity usage more efficiently, AI-integrated smart meters monitor real-time consumption, flagging unusual patterns that may indicate security risks or inefficiencies. This has translated to notable energy savings and reduced carbon emissions in several cities—particularly in large buildings and public sector facilities, where demand is highest. For example, trials in Suwon, South Korea, led to a 30% increase in energy efficiency and a 35% decrease in emissions from public buildings.
- III. **Healthcare monitoring:** AI supports critical health infrastructure by analyzing data from wearable devices to monitor patient vitals and alert medical personnel during emergencies. This system ensures patient privacy through secure data protocols, guarding sensitive health data against breaches and keeping healthcare systems running smoothly in cities where service demand is growing.
- IV. **Threat detection and crowd management:** AI-powered systems enhance public safety in busy urban areas. Real-time analysis from cameras and IoT sensors enables AI to detect suspicious objects, recognize faces from watchlists, or even spot behaviors that could indicate criminal intent. This is especially valuable for crowd management during large events or in busy transit hubs, where AI can instantly alert security teams to potential threats.
- V. **Smart waste and environmental management:** Many cities struggle with waste collection inefficiencies. AI-integrated smart bins can monitor fill levels and optimize collection routes, reducing operational costs and emissions from garbage trucks. Additionally, air quality sensors integrated with AI monitor pollution trends, enabling cities to proactively respond to environmental hazards and making urban areas healthier for residents [6].



Fig. 6. Use case of smart monitoring.

These applications show how AI fortifies urban infrastructure against cyber and physical threats. By securing critical systems and optimizing resources, AI is helping cities become more resilient, efficient, and safe for residents.



Fig. 7. Air quality sensors integrated with AI monitor pollution trends.

5 | Conclusion

In summary, integrating AI into network security frameworks for smart cities represents a transformative approach that enhances real-time threat detection, automates responses, and maintains secure data flow. With a centralized AI-powered monitoring hub, predictive analytics, and adaptive protocols, cities are better equipped to manage the complexities of urban IoT networks. However, addressing privacy, bias, and system transparency challenges will be essential to fully realize AI's potential in securing these environments. As AI-driven security solutions evolve, they will be instrumental in safeguarding vital city services—such as

transportation, healthcare, and energy management—ensuring seamless operation amid the changing landscape of cyber threats [17].

Funding

This research received no external funding.

Data Availability

The data used and analyzed in this study are accessible from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest. Authors must disclose any personal circumstances or interests that may have an undue influence on the presentation or interpretation of the reported study findings. Funders had no part in the study's design, data collection, analysis, interpretation, manuscript preparation, or decision to publish the findings.

References

- [1] Panda, A. K., Lenka, A. A., Mohapatra, A., Rath, B. K., Parida, A. A., & Mohapatra, H. (2025). Integrating cloud computing for intelligent transportation solutions in smart cities: A short review. In *Interdisciplinary approaches to transportation and urban planning* (pp. 121–142). IGI Global. <https://doi.org/10.4018/979-8-3693-6695-0.ch005>
- [2] Pratap, A., Nayan, H., Panda, P., & Mohapatra, H. (2024). Emerging technologies and trends in the future of smart cities and IoT: A review. *Journal of network security computer networks*, 10(2), 28–38. <https://matjournals.net/engineering/index.php/JONSCN/article/view/606>
- [3] Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT Security for smart cities. *ACM transactions on internet technology*, 21(4), 1–21. <https://doi.org/10.1145/3406115>
- [4] Alahi, M. E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay, S. C. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends. *Sensors*, 23(11), 5206. <https://doi.org/10.3390/s23115206>
- [5] Kabir, M. H., Hasan, K. F., Hasan, M. K., & Ansari, K. (2022). Explainable artificial intelligence for smart city application: A secure and trusted platform. In *Explainable artificial intelligence for cyber security: next generation artificial intelligence* (pp. 241–263). Springer. https://doi.org/10.1007/978-3-030-96630-0_11
- [6] Wolniak, R., & Stecula, K. (2024). Artificial intelligence in smart cities—applications, barriers, and future directions: A review. *Smart cities*, 7(3), 1346–1389. <https://doi.org/10.3390/smartcities7030057>
- [7] Koormala, H., Reddy, C. K. K., Balusa, V. S., Jillapalli, N., & Hanafiah, M. M. (2025). Enhancing urban safety: AI-driven security solutions for smart cities. In *Information security governance using artificial intelligence of things in smart environments* (pp. 146–163). CRC Press. <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003606307-7/enhancing-urban-safety-harika-koormala-kishor-kumar-reddy-vasavi-sravanthi-balusa-nikitha-jillapalli-marlia-mohd-hanafiah>
- [8] Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. *Cities*, 89, 80–91. <https://doi.org/10.1016/j.cities.2019.01.032>
- [9] Mohapatra, H., Rath, A. K., Balajee, R. M., & Devi, H. S. (2022). Comparative case study on smart city versus digital city. In *Handbook of research of internet of things and cyber-physical systems* (pp. 51–78). Apple Academic Press. <https://doi.org/10.1201/9781003277323-4>
- [10] Mohapatra, H. (2021). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies, 3ICT 2021* (pp. 57–62). IEEE. <https://doi.org/10.1109/3ICT53449.2021.9581905>
- [11] Prabha, B. V., Yasotha, B., Senthilkumar, C., Pandi, V. S., & others. (2023). Enhancing residential security with ai-powered intrusion detection systems. *2023 international conference on sustainable communication*

- networks and application (ICSCNA)* (pp. 1510–1515). IEEE.
<https://doi.org/10.1109/ICSCNA58489.2023.10370042>
- [12] Hussain, I. (2024). Secure, sustainable smart cities and the Internet of Things: Perspectives, challenges, and future directions. *Sustainability*, 16(4), 1390. <https://doi.org/10.3390/su16041390>
- [13] Priyadarshini, I. (2024). Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning. *Big data and cognitive computing*, 8(3), 21. <https://doi.org/10.3390/bdcc8030021>
- [14] Bee Smart City. (2023). *The use of AI for smart urban services in smart cities*.
<https://www.beesmart.city/en/smart-city-blog/the-use-of-ai-for-smart-urban-services-in-smart-cities>
- [15] Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE access*, 8, 228922–228941.
<https://doi.org/10.1109/ACCESS.2020.3046442>
- [16] KaaIoT. (2024). *AI and IoT for smart city public security: Top 6 use cases*. www.kaaiot.com
- [17] Buttice, C. (2022). *Top 14 AI use cases: Artificial intelligence in smart cities*. Techopedia. <https://www.techopedia.com/top-14-ai-use-cases-artificial~....> www.techopedia.com