International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

A Survey on Technologies Used in Smart Cities: Cybersecurity, Privacy Protection, Software Agents, and Deep Learning

Fahad Saif Alharbi

College of Computing, Fahad Bin Sultan University, AIMD Lab, KSA, Tabuk

---

Abstract-*Smart cities increasingly depend on interconnected digital technologies, including Internet of Things devices, smart sensors, surveillance systems, cloud computing platforms, artificial intelligence, deep learning, location-based services, and agent-based systems to enhance urban management and improve citizens' quality of life. Although these technologies provide significant benefits in terms of efficiency, automation, and service optimization, they also introduce serious cybersecurity and privacy challenges due to the high level of connectivity among critical urban infrastructures. This paper discusses the major cybersecurity threats facing smart cities, including Advanced Persistent Threats, ransomware attacks, IoT botnets, AI-driven cyberattacks, and attacks targeting industrial control systems. It also highlights privacy risks associated with the collection, processing, and sharing of sensitive citizen data, particularly location information, movement patterns, and service-usage records. Furthermore, the paper emphasizes the importance of securing software agents, as these agents may operate autonomously, exchange information, access distributed resources, and support decision-making across different smart-city environments. Several protection mechanisms are considered, including authentication, access control, encryption, secure communication, network monitoring, data minimization, anonymization, obfuscation, incident response planning, and human supervision. The paper concludes that the development of secure and reliable smart cities requires an integrated security framework that combines cybersecurity, privacy preservation, secure agent-based computing, and responsible use of artificial intelligence and deep learning to ensure service continuity, citizen safety, and public trust.*

Key Words: Privacy, Security, Smart Cities, Agents, Threats, Controls, Healthcare.

1. INTRODUCTION TO CYBERSECURITY IN SMART CITIES

A smart city uses digital technologies such as sensors, connected cameras, smart traffic systems, online services, and smart energy networks to improve city life. These technologies help cities become faster, more efficient, and more organized [1]. However, once many systems are connected, they also become more vulnerable to cyberattacks. CISA (Cybersecurity and Infrastructure Security Agency) explains that smart cities face risk because they create larger and more interconnected attack surfaces, while NIST (National Institute of Standards and Technology) says cybersecurity must be built into smart-city planning from the beginning. Figure 1 shows that cybersecurity in a smart city is not limited to one system only, but affects multiple connected sectors including mobility, energy, water, buildings, homes, education, waste management, and working environments.

Figure-1: Cybersecurity issues around Smart City

2. WHY CYBER SECURITY IS IMPORTANT

Systems, transport, emergency communication, or public services. This means a cyber-problem in a smart city is not only a computer issue; it can become a public safety issue. NIST recommends a risk-managed approach so that cities can identify threats early and apply suitable protections.

3. MAIN CYBER THREATS

One major problem is the large number of connected devices. Smart cities depend on IoT devices, cloud systems, communication networks, and software from different vendors. If one device is weak, attackers may use it as an entry point. Another problem is poor coordination between departments or suppliers. CISA highlights that connected communities need strong cyber practices, and NIST stresses that cities should choose security processes that fit their own environment.

The most advanced cyber threats in smart cities include Advanced Persistent Threats [2], ransomware [3], IoT botnets [4], AI-powered cyberattacks [5], and attacks on

industrial control systems [6]. Advanced Persistent Threats are highly organized and long-term attacks in which hackers secretly enter smart-city networks to steal sensitive information or disrupt important services. Ransomware attacks are also very dangerous because they can lock critical systems such as hospitals, traffic lights, water networks, electricity grids, and municipal databases until a payment is demanded. Another serious threat is IoT botnets, where attackers hijack weakly protected smart devices such as cameras, sensors, meters, and traffic devices, then use them to spy, spread malware, or launch large-scale attacks. In addition, AI-powered cyberattacks are becoming more advanced because attackers can use artificial intelligence to create realistic phishing messages, discover system weaknesses, imitate normal user behavior, or produce deepfake content. Finally, attacks on industrial control systems are among the most critical threats because they can directly affect physical infrastructure such as transportation systems, smart grids, and water treatment plants, which may lead to service disruption, public safety risks, and loss of trust in smart-city technologies.

4. HOW CITIES CAN PROTECT THEMSELVES

To improve cyber security, smart cities need strong passwords, regular updates, network monitoring, controlled access, and clear incident response plans. Staff training is also important because human mistakes often create security gaps. Cyber security should not be added at the end of a project. It should be included from the design stage.

Protection against advanced cyber threats (mentioned above) in smart cities requires a combination of technical, organizational, and monitoring-based methods [7, 8]. To protect against Advanced Persistent Threats, smart cities should use continuous network monitoring, threat intelligence, zero-trust security, multi-factor authentication, endpoint detection and response, and regular security audits to detect hidden attackers early. To reduce the impact of ransomware, cities should apply frequent data backups, disaster recovery plans, email filtering, employee awareness training, access control, patch management, and network segmentation so that malware cannot easily spread across critical systems. For IoT botnets and device hijacking, protection methods include strong device authentication, changing default passwords, secure firmware updates, encryption, device inventory management, and isolating IoT devices from sensitive city networks. Against AI-powered cyberattacks, smart cities should use AI-based threat detection, deepfake detection tools, secure identity verification, phishing detection systems, human review of sensitive decisions, and continuous training of employees and citizens. Finally, to protect industrial control systems and operational technology, cities should separate IT and OT networks, use firewalls and intrusion detection systems, apply strict access control, monitor unusual system behavior, update systems carefully, and prepare incident response plans to ensure that essential services such as electricity, water, transport, and emergency systems remain safe and available.

5. INTRODUCTION TO PRIVACY IN SMART CITIES

Smart cities use cameras, sensors, mobile apps, smart transport, and online services to improve daily life. These systems depend on collecting and using data, which makes privacy protection very important. The smart-city data can affect different forms of privacy.

6. WHY PRIVACY PROTECTION MATTERS

Privacy protection matters because smart-city systems can collect information about where people go, how they travel, and how they use public services. If this data is not handled carefully, it can reduce public trust and expose people to unnecessary monitoring. NIST's smart-city guidebook recommends a risk-managed approach to privacy and cybersecurity from the design stage.

7. MAIN PRIVACY RISKS IN SMART CITIES

The main privacy risks include excessive data collection, location tracking, public surveillance, data breaches, data sharing without clear consent, weak transparency, and profiling through linked datasets. European Commission highlighted privacy concerns in smart-city data use, and the explains that data-protection rules also apply to technologies such as video surveillance and online identifiers.

8. EXAMPLES OF APPLICATIONS AND RISKS

- Smart cameras / CCTV: surveillance in public spaces.
- Transport apps / smart ticketing: tracking location and movement.
- Public Wi-Fi and connected devices: identifying users through device or network data.
- City data platforms: data breaches or unauthorized access.
- Shared city datasets: profiling people by combining information from different systems.

Privacy protection is highlighted when depending on location based services to end daily activities in smart cities by users [9]. All examples mentioned above can be under threat of attacking privacy when integrated with location based services.

9. WAYS TO PROTECT PRIVACY

Smart cities can protect privacy by collecting only necessary data, limiting access, being transparent about data

use, and applying clear governance rules. OECD points to measures such as ethics oversight, opt-out procedures, and stronger data-management practices, while NIST supports privacy-aware risk management as part of smart-city planning.

When it comes to talking about privacy protection in smart cities, taking into account integration with location based services, there are many protection controls that can be explored through [10, 11, 12, 13]. The most common ways are dummies, encryption, transformation of location information, obfuscation, and clocking regions. It is worth mentioning that all of these ways intersect with a common concept, which is achieving k-anonymity level. It is worth mentioning that when location based services use web applications, another ways of protection are required as well as data mining techniques to deal with big data [14, 15].

10. INTRODUCTION TO AGENT-BASED SYSTEMS SECURITY

Agent-based systems are systems made of autonomous software agents that can observe, decide, and act on their own. In many cases, these agents work together as a multi-agent system to solve complex problems. Such systems are useful because they are flexible, distributed, and able to react quickly [16]. However, because agents can make decisions and communicate with each other, security becomes a very important concern. A well-known survey on multi-agent security identifies access control and trust as key issues, while NIST's new AI Agent Standards Initiative highlights the need for secure and interoperable agent systems.

11. WHY SECURITY OF AGENTS IS IMPORTANT

Security is important in agent-based systems because agents may exchange data, access tools, or perform tasks without constant human control. If one agent is compromised, it may spread false information, misuse permissions, or affect the decisions of other agents. NIST notes that AI agents must function securely on behalf of users, especially as they become more capable and autonomous.

The security of software agents is very important in smart cities because these agents may act automatically on behalf of users, systems, or city authorities. In smart cities, software agents can collect data, make decisions, communicate with other systems, manage services, and support applications such as traffic control, healthcare, energy management, transportation, emergency response, and location-based services. If these agents are not secure, attackers may manipulate them, steal the data they carry, change their decisions, or use them as a gateway to attack smart-city infrastructure. This can lead to privacy violations, service disruption, wrong decisions, financial loss, and even risks to public safety.

Moreover, software agents often move between different platforms or interact with many distributed devices, sensors, servers, and cloud systems. This makes them exposed to threats such as identity spoofing, unauthorized access, malicious code injection, data tampering, and communication interception. Therefore, securing software agents helps ensure authentication, confidentiality, integrity, trust, and reliable decision-making. In smart cities, where digital systems are directly connected to real-world services, protecting software agents is essential for maintaining citizen privacy, service continuity, and confidence in smart-city technologies.

12. MAIN SECURITY CHALLENGES

The main security challenges include weak authentication, poor permission control, unsafe communication, and lack of trust between agents. OWASP also warns that agentic applications face new risks and need practical security controls during design and deployment [17]. This means developers must think about threats early, not only after the system is built. In addition, there are a wide spectrum of attacks that can be applied to agents-based systems [18]. Many protection controls are developed in [19, 20], where dummies is considered as one of the most effective controls. It is worth mentioning that power consumption is an important issue linked with agents, where it is addressed in some works such as [21].

13. PROTECTION METHODS

Agent-based systems can be protected through identity verification, access control, secure communication, monitoring, logging, and human oversight for sensitive actions. OWASP recommends treating outside data as untrusted and using validation and clear boundaries before agents act on that data. These controls reduce the chance of manipulation or unauthorized actions.

14. INTRODUCTION TO AI and DL IN SMART CITIES (HEALTHCARE SECTOR AS AN EXAMPLE)

Artificial intelligence and deep learning are becoming very important in healthcare. They are used to support diagnosis, medical imaging, patient monitoring, drug development, and health-system management. WHO (world health organisation) explains that AI can help countries build more people-centered, equitable, and sustainable health systems [22]. This shows that AI is no longer just a future idea; it is already part of modern healthcare development.

15. ROLE OF DEEP LEARNING

Deep learning is a part of AI that learns patterns from large and complex datasets. A Nature Medicine guide describes deep learning in healthcare across computer vision, natural language processing, reinforcement learning, and other general methods. This is why deep learning is especially useful for reading medical images, processing clinical records, and finding hidden patterns in health data.

16. BENEFITS IN HEALTHCARE

AI and deep learning can help doctors work faster and support better decisions. FDA (Food and Drug Administration) notes that AI-enabled medical devices are already authorized for marketing in the United States, which shows that AI is already being used in real healthcare products. These tools can improve efficiency, assist diagnosis, and support patient care when they are properly tested and regulated.

There are many researchers conducted in healthcare sector that provide advanced diagnosing systems to predict diseases for the sake of protecting health of people, such as [23, 24, 25].

17. CHALLENGES AND RISKS

Despite these benefits, AI in healthcare also creates challenges. WHO warns that ethics, governance, and human rights must remain central in the use of AI for health. FDA also emphasizes safety, effectiveness, and life-cycle management for AI-enabled medical devices. This means AI systems must be monitored carefully because healthcare decisions directly affect human lives.

18. CONCLUSION

Smart cities depend heavily on connected technologies, IoT devices, cloud platforms, artificial intelligence, deep learning, location-based services, and agent-based systems to improve the quality of life and efficiency of public services. However, this high level of connectivity also increases cybersecurity, privacy, and system-security risks. Advanced cyber threats such as ransomware, IoT botnets, AI-powered attacks, Advanced Persistent Threats, and attacks on industrial control systems can affect not only digital systems but also real-world services such as transportation, healthcare, energy, water, and emergency response. Therefore, cybersecurity must be considered from the design stage through strong authentication, access control, monitoring, encryption, regular updates, network segmentation, and incident response planning. In addition, privacy protection is essential because smart-city applications may collect sensitive information about citizens' locations, movements, activities, and service usage. Techniques such as data minimization, anonymization, obfuscation, encryption, and clear governance policies can help reduce privacy risks. Furthermore, securing software agents is important because agents may act autonomously, exchange data, and make decisions across different smart-city systems. Overall, building a safe and trusted smart city requires an integrated approach that combines cybersecurity, privacy protection, secure agent-based systems, and responsible use of AI and deep learning to ensure service continuity, citizen safety, and public trust.

ACKNOWLEDGEMENT

The author takes help of ChatGPT to present illustrative figures as well as for proof reading. However, the basic scientific content is presented by the author.

REFERENCES

1) Rehan, Hassan. "Internet of Things (IoT) in smart cities: Enhancing urban living through technology." Journal of engineering and technology 5.1 (2023): 1-16.

2) Hummelholm, Aarne. "Cyber threat analysis in Smart City environments." European Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2018.

3) Farid, Farnaz. "A threat analysis framework for cyberattacks in smart cities: Ransomware in focus." Advances in the Internet of Things. CRC Press, 2026. 101-124.

4) Kim, Donghyun, et al. "Design the IoT Botnet Defense Process for Cybersecurity in Smart City." Intelligent Automation & Soft Computing 37.3 (2023).

5) Khan, Irfan, and Asif Ali. "Cybersecurity Challenges in AI-Powered Smart Cities: A Risk Assessment Framework." (2024).

6) Drias, Zakarya, Ahmed Serhrouchni, and Olivier Vogel. "Analysis of cyber security for industrial control systems." 2015 international conference on cyber security of smart cities, industrial control system and communications (ssic). IEEE, 2015.

7) Shawl, Rashed Qayoom, Manmeet Singh, and Malik Mubasher Hassan. "Leveraging Cyber-Physical Security Solutions Blended With Machine Learning for Advanced IoT Botnet Detection." IEEE Communications Standards Magazine (2025).

8) Demertzi, Vasiliki, Stavros Demertzis, and Konstantinos Demertzis. "An overview of cyber threats, attacks and countermeasures on the primary do-

mains of smart cities." Applied Sciences 13.2 (2023): 790.

9) Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "A Survey on Privacy of Location-Based Services: Classification, Inference Attacks, and Challenges," Journal of Theoretical and Applied Information Technology, vol. 95, no. 24, 2017.

10) Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "Agent-Based System for Efficient kNN Query Processing with Comprehensive Privacy Protection," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018.

11) Mohamad Shady Alrahhal, Muhammad Usman Ashraf, Adnan Abesen and Sabah Arif, "AES-Route Server Model for Location Based Services in Road Networks," International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017.

12) Hosam Alrahhal et al., "A symbiotic relationship based leader approach for privacy protection in location based services," ISPRS International Journal of Geo-Information, vol. 9, no. 6, p. 408, 2020.

13) Abdullah S. Alyousef, Karthik Srinivasan, Mohamad Shady Alrahhal, Majdah Alshammari and Mousa Al-Akhras, "Preserving Location Privacy in the IoT against Advanced Attacks using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 13, no. 1, 2022.

14) Majed Abdullah Albarrk and Mohamad Shady Alrahhal, "Web Applications Security: More Collaboration," 2020.

15) Mohamad Shady Alrahhal and Adnan Abi Sen, "Data mining, big data, and artificial intelligence: An overview, challenges, and research questions," 2018.

16) Cardoso, Rafael C., and Angelo Ferrando. "A review of agent-based programming for multi-agent systems." Computers 10.2 (2021): 16.

17) Sinan, Maysa. Support Security Control Management and Implementation in DevSecOps. Diss. RMIT University, 2025.

18) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "A Survey: Agent-based Software Technology Under the Eyes of Cyber Security, Security Controls, Attacks and Challenges," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, 2019.

19) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Dummy-based approach for protecting mobile agents against malicious destination machines," IEEE Access, vol. 8, pp. 129320-129337, 2020.

20) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Achieving self-protection and self-communication features for security of agent-based systems," 2020.

21) Mohamad Shady Alrahhal, Maher Khemekhem and Kamal Jambi, "Achieving load balancing between privacy protection level and power consumption in location based services," International Research Journal of Engineering and Technology, vol. 5, no. 3, pp. 619-625, 2018.

22) World Health Organization. WHO global strategy on people-centred and integrated health services: interim report. No. WHO/HIS/SDS/2015.6. World Health Organization, 2015.

23) Mona Alfifi, Mohamad Shady Alrahhal, Samir Bataineh and Mohammad Mezher, "Enhanced Artificial Intelligence System for Diagnosing and Predicting Breast Cancer using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, 2020.

24) Mohamad Shady Alrahhal and Eftkhar Alqhtani, "Deep learning-based system for detection of lung cancer using fusion of features," International Journal of Computer Science and Mobile Computing, vol. 10, no. 2, pp. 57-67, 2021.

25) Mohamad Shady Alrahhal and Majed Abdullah Albarrk, "A Survey of the COVID-19 Epidemic Through the Eyes of Artificial Intelligence and Deep Learning: Challenges and Research Questions," 2020.