International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 11 | Nov 2025 www.irjet.net p-ISSN: 2395-0072

Security and Privacy in NEOM Smart City: A Systematic Review on Agents Based Systems and Location Based Systems

Rayan Dalaki[1]

[1.] *College of Computing, Fahad Bin Sultan University, Saudi Arabia
(Corresponding Author)

Abstract – *NEOM is considered one of the most promising smart cities all over the world. Addressing security and privacy issues in such smart cites is critical as it leads to make future cities not only smarter but also more secure. Agent based system as well as location based systems form an integral part of smart cities. This work explores both the security and privacy issues in smart cities, where different approaches were reviewed in terms of protection against attacks and sensitive data protection. This work concludes that ensuring both security and privacy is essential for trust of users. Challenges and future trends are also presented to enable researchers to direct their works towards more secure and smart cities, which leads to more sustainability.*

***Key Words*: NEOM, Security, Privacy, Agents, Big Data, Medical Systems.**

1. INTRODUCTION

A smart city is an urban area that leverages digital technologies, data analytics, and interconnected systems to enhance infrastructure, improve public services, and optimize resource management. The goal is to increase efficiency, sustainability, and quality of life for citizens [1].

Internet of Things (IoT) refers to a network of physical devices (sensors, actuators, cameras) embedded with connectivity features that enable them to collect, and process data over the internet. These devices facilitate real-time monitoring and automation in various applications [2].

Cloud computing is the delivery of computing services (storage, processing, networking, analytics, etc.) over the internet ("the cloud"). It provides scalable, on-demand resources without requiring direct physical infrastructure management [3]

1.1 Relationship Among Smart Cities, IoT, and Cloud Computing

In the context of smart cities, IoT and cloud computing are interdependent technologies that enable intelligent urban management:

1. **IoT as the Data Source:**
   - IoT devices (e.g., traffic sensors, smart meters, surveillance cameras) collect real-time data from the city environment.
   - Example: Smart traffic lights adjust signals based on real-time vehicle flow data.
2. **Cloud Computing as the Processing Hub:**
   - The massive volume of data generated by IoT devices is stored, processed, and analysed in the cloud.
   - Cloud platforms provide scalability, AI/ML analytics, and centralized management for smart city applications.
   - Example: Cloud-based AI analyzes traffic patterns to optimize city-wide transportation routes.
3. **Smart City as the Application Layer:**
   - The integration of IoT + Cloud enables smart city solutions like:
     - Smart Energy Management (IoT sensors + cloud-based demand forecasting).
     - Waste Management (IoT-enabled bins + cloud analytics for optimized collection routes).
     - Public Safety (Surveillance cameras + cloud-based facial recognition).

1.2 NEOM (Modern Smart City in Saudi Arabia)

NEOM is a futuristic, $500 billion mega-project in Saudi Arabia, designed to be a model smart city powered by cutting-edge technologies like IoT, AI, cloud computing, and renewable energy. It aims to be a zero-carbon, hyper-connected, and AI-driven urban ecosystem [4].

Key Smart City Features of NEOM

1. **AI & IoT-Driven Infrastructure**
   - Smart Sensors & Automation: IoT-enabled devices monitor energy use, traffic, air quality, and waste management in real time. Example: Autonomous drones for logistics and AI-powered surveillance for security.
   - Smart Mobility: Autonomous vehicles (EVs, flying taxis) connected via 5G/6G and IoT networks. Predictive traffic management using AI + cloud analytics.

2. **Cloud & Edge Computing Backbone**
   - Centralized Cloud AI: NEOM's operations rely on cloud-based AI for decision-making (e.g., optimizing energy grids, water usage).
   - Edge Computing for Low Latency: Critical systems (e.g., autonomous transport) use edge computing for real-time responses.
3. **100% Renewable Energy and Sustainability**
   - Powered by wind, solar, and green hydrogen. IoT-enabled smart grids balance energy demand dynamically.
4. **Hyper-Connectivity (5G/6G & Free Wi-Fi)**
   - Ultra-fast internet enables seamless IoT, AR/VR, and smart services.

Table 1 summarizes how IoT, Cloud, and AI work together in NEOM.

Table -1: IoT, Cloud, and AI in NEOM

Technology	Role in NEOM
IoT	Data collection from sensors (traffic, energy, environment)
Cloud Computing	Stores & processes massive data; runs AI models
AI\ML	Analyzes data for automation & predictions
5G\6G	Enables real-time IoT communication

2. Privacy VS. Security

Smart cities like NEOM rely on IoT, AI, and cloud computing to optimize urban life, but this raises critical concerns about security (protecting systems from attacks) and privacy (protecting citizens' personal data).

In terms of definitions, security is protecting systems, data, and infrastructure from cyber threats, breaches, and attacks, while privacy is ensuring individuals' personal data is collected, stored, and used ethically and with consent. Table 2 summarizes the key differences between privacy and security.

Table -2: IoT, Cloud, and AI in NEOM

Aspect	Security	Privacy
Focus	Prevent unauthorized access, attacks, and system failures.	Protect personal data from misuse or exploitation.
Threats	System integrity, resilience, and threat prevention.	Data leaks, surveillance overreach, profiling.
Technologies Used	Hackers, malware, DDoS attacks, insider threats.	Anonymization, GDPR-like policies, user consent tools.

2.1 Security in Smart Cities

Agent's software technology is used to create smart agents to perform specific tasks, such as collecting data about prices of air trips, or monitoring malicious movements and then issuing alarms to take corresponding actions. Authors of [5] present a comprehensive survey about security of agents and their related issues. Another work [6] presented a robust security approaches based on dummies to protect agents, where the key idea is to select the task based on the probabilities with an aim to confuse host machine (attacker) from determining the real task among dummies. This way ensures security of tasks performed by moving agents against malicious servers. A self-protection mechanism is proposed in work [7]. The key idea is to select a seed that is uncovered by attackers to be used as a primary key for generating encryption key to be used for protecting exchanged messages. In terms of web security, the work [8] aims at enhancing web application security through cross-team collaboration. In other words, to mitigate risks in web applications, organizations must foster collaboration among diverse IT teams, each bringing unique security perspectives. To sum up, the security requirements in smart cities when employing agent based software technology, Figure 1 illustrates them.

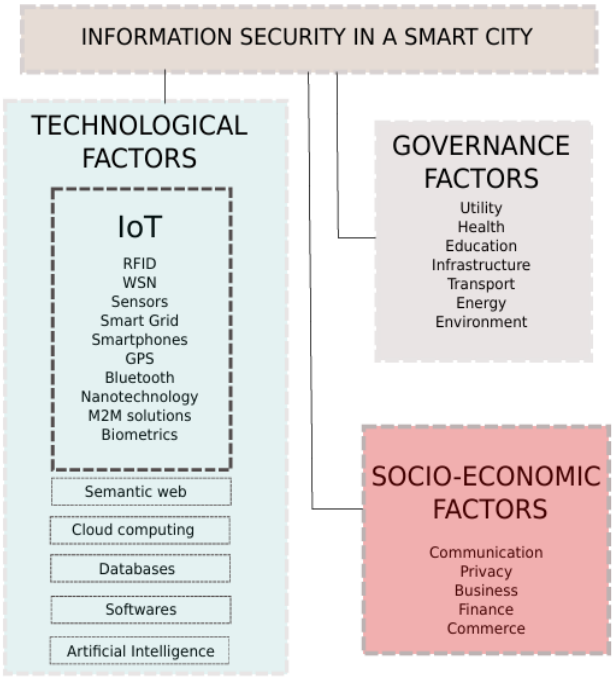

Fig -1: Security aspects in smart cities [9].

2.2 Privacy in Smart Cities

The most common applications used in smart cities is location based services. Location-Based Services (LBS): are digital services that use real-time geographic data (e.g., GPS, Wi-Fi, IoT sensors) to provide personalized information,

navigation, or functionality based on a user's or device's location. The key technologies enabling LBS are:

1- GPS & GNSS (Global Navigation Satellite Systems)

2- IoT & Smart Sensors (e.g., beacons, RFID tags)

3- Cellular/Wi-Fi Triangulation

4- Geofencing & GIS (Geographic Information Systems)

Importance of LBS in smart cities can be listed as follows:

1. **Efficient Urban Mobility**
   - Real-Time Navigation: Apps like Google Maps optimize routes using traffic data.
   - Autonomous Vehicles: Self-driving cars rely on LBS for pathfinding and collision avoidance.
2. **Public Safety & Emergency Response**
   - Faster Dispatch: Precise location tracking reduces emergency response times.
   - Disaster Management: Evacuation routes are dynamically updated based on real-time hazards.
   - **Smart Resource Management**
   - Waste Collection: Sensors detect fill levels in trash bins, optimizing pickup routes.
   - Energy Efficiency: Streetlights dim when no pedestrians are detected (via geofencing).
3. **Personalized Citizen Services**
   - Retail & Tourism: Push notifications for discounts when near a store (beacon technology).
   - Public Transport: Apps show bus/train arrivals based on the user's nearest stop.
4. **Data-Driven Urban Planning**
   - Heatmaps: Analyze foot traffic to design better pedestrian zones.
   - Crowd Control: Monitor dense areas (e.g., stadiums) to prevent accidents.

There are various approaches proposed previously to protect privacy in smart cities. As described below.

Authors of work [10] proposed an AES rout model for privacy protection for road network. The key idea is to issue multiple dummies stored in the access point to be used as a third party between clients and servers. This approach protects privacy against man in the middle attacks. Authors of [11] provided a comprehensive literature review about privacy protection methods used in LBS. The taxonomy provided in the work determines the protection goals and the corresponding methods used for privacy protection. In addition, a wide spectrum of attacks, such as map matching attack, semantic location attack, and heterogeneous attacks are explained in details. Authors of work [12] provided a leader approach for privacy protection, where the key idea is to change the ID of the LBS user when moving from one region to another as well as changing both paths and real names. Authors of work [13] provided deep learning based approach to ensure privacy protection, where the tracks of the users are captures in image formats, and convolutional neural network is employed to protect privacy protection. In addition, to protect privacy of moving objects based on Knn queries, the work [14] provided effective way for ensuring privacy using dummies integrated with fragmentation technique. One important aspect of this work is related to deal with big data to ensure retrieving accurate locations of points of interests [15]. Some works related to addressing power consumption on IoT devices with achieving balancing of high privacy protection were proposed, such as [16].

In medical sector, privacy of patients is critical for people located in smart cities. In this aspect, many approaches were proposed. Authors of work [17] proposed a diagnostic system used to detect breast cancer using convolutional neural network. The system is supported by an augmentation technique based on rotation method to enable extraction effective features. Privacy of medical images are ensured by removing sensitive data from the medical files. Based on fusion of features, authors of work [18] proposed an intelligent medical system to detect lung cancer. The aspect of ensuring privacy of patients is achieved by using k-anonymity based technique. To detect COVID-19 viruses, authors of work [19] proposed an augmented deep learning system, where in regards to privacy protection of CT-scan images is ensured by masking personal information based on generalization method. Particularly, the age, name and ID of patients are masked within a range of values. To highlight the importance of privacy protection during COVID-19 epidemic, authors of work [20] mentioned to the importance of privacy protection when employing deep learning based system to develop diagnostic systems.

3. Challenges and Future Trends

Smart cities leverage IoT, AI, and big data to enhance urban living, but they also introduce significant privacy and security risks. Below is an analysis of key challenges and emerging trends to address them.

3.1. Data Privacy Risks

- Mass Surveillance: AI-powered cameras, facial recognition, and location tracking raise concerns about government overreach and loss of anonymity.
- Data Misuse: Personal data collected by IoT devices (e.g., smart meters, wearables) can be sold to third parties without consent.

- Lack of Transparency: Citizens often don't know how their data is stored, processed, or shared.

3.2 Cybersecurity Threats

- Agent based systems may be attacked by various attacks, where converting the host machine of the mobile agent into an attacker is the most important aspect as it leads to higher dangerous level.
- IoT Vulnerabilities: Many smart devices have weak encryption and default passwords, making them easy targets for hackers.
- Ransomware Attacks: Hackers can shut down critical infrastructure (e.g., traffic lights, power grids).
- AI-Powered Cyberattacks: Attackers use machine learning to bypass security systems.

3.3 Legal and Ethical Issues

- Inconsistent Regulations: Different countries have varying data protection laws (e.g., GDPR vs. weaker policies in some regions).
- Algorithmic Bias: AI-driven policing or resource allocation may discriminate against certain groups.

3.4 Future Trends to Enhance Privacy and Security

1. Federated Learning: AI trains on decentralized data without central storage. Homomorphic Encryption: Allows data processing without decrypting it.
2. Differential Privacy: Adds "noise" to datasets to prevent re-identification.
3. Smart City-Specific GDPR Laws: Stricter regulations for IoT and AI data usage. Citizen-Centric Data Ownership – Users control who accesses their data via self-sovereign identity (SSI).
4. Ethical AI Audits: Independent reviews to detect bias in automated decision-making.
5. Post-Quantum Cryptography: Protects against quantum computing attacks.
6. Digital Twins with Security Layers: Simulates cyber threats before they happen.
7. Decentralized Identity Systems: Blockchain-based IDs reduce reliance on centralized databases.

CONCLUSION

Smart cities represent the future of urban living, leveraging IoT, AI, and big data to enhance efficiency, sustainability, and quality of life. However, this rapid digitization introduces significant privacy and security challenges, from mass surveillance risks to cyberattacks on critical infrastructure. To build trustworthy and resilient smart cities, a multi-layered approach is essential:

- Technologically, through privacy-preserving AI, zero-trust security, and blockchain for transparency.
- Legally, via stronger regulations (like GDPR for smart cities) and ethical AI governance.
- Socially, by empowering citizens with data ownership and consent mechanisms.

The future of smart cities depends on striking the right balance harnessing innovation while safeguarding fundamental rights. By adopting decentralized systems, quantum-resistant encryption, and human-centric design, cities can become not just smarter, but safer and fairer for all.

REFERENCES

[1] Hämäläinen, Mervi. "A framework for a smart city design: digital transformation in the Helsinki smart city." Entrepreneurship and the community: a multidisciplinary perspective on creativity, social challenges, and business. Cham: Springer International Publishing, 2019. 63-86.

[2] Schoder, Detlef. "Introduction to the Internet of Things." Internet of things A to Z: technologies and applications (2025): 1-40.

[3] Kaur, Tajinder. "Cloud computing: A study of the cloud computing services." international Journal for Research in Applied Science & Engineering Technology (IJRASET) 7.VI (2019): 1933-1938.

[4] Touri, Mahboubeh. Crafting the Future: Pioneering Urban Branding and Development in Neom's Visionary Line City Project, Saudi Arabia. Diss. Politecnico di Torino, 2024.

[5] 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 (IJACSA) 10.8 (2019). http://dx.doi.org/10.14569/IJACSA.2019.0100828

[6] Alluhaybi, Bandar, et al. "Dummy-based approach for protecting mobile agents against malicious destination machines." IEEE Access 8 (2020): 129320-129337.

[7] Alluhaybi, Bandar, et al. "Achieving self-protection and self-communication features for security of agentbased systems." (2020).

[8] Albarrk, Majed Abdullah, and Mohamad Shady Alrahhal. "Web Applications Security: More Collaboration." (2020).

[9] Ijaz, Sidra, et al. "Smart cities: A survey on security concerns." International Journal of Advanced Computer Science and Applications 7.2 (2016).

[10] 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 (IJACSA) 8.8 (2017). http://dx.doi.org/10.14569/IJACSA.2017.080847

[11] Alrahhal, Mohamad Shady, Maher Khemakhem, and Kamal Jambi. "A SURVEY ON PRIVACY OF LOCATION-BASED SERVICES: CLASSIFICATION, INFERENCE ATTACKS, AND CHALLENGES." Journal of Theoretical & Applied Information Technology 95.24 (2017).

[12] Alrahhal, Hosam, et al. "A symbiotic relationship based leader approach for privacy protection in location based services." ISPRS International Journal of Geo-Information 9.6 (2020): 408.

[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 (IJACSA)13.1(2022). http://dx.doi.org/10.14569/IJACSA.2022.0130152

[14] 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 (IJACSA) 9.1 (2018). http://dx.doi.org/10.14569/IJACSA.2018.090108

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

[16] Alrahhal, Mohamad Shady, 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 5.3 (2018): 619-625.

[17] 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 (IJACSA)11.7(2020). http://dx.doi.org/10.14569/IJACSA.2020.0110763

[18] Alrahhal, Mohamad Shady, and Eftkhar Alqhtani. "Deep learning-based system for detection of lung cancer using fusion of features." International Journal of Computer Science & Mobile Computing 10.2 (2021): 57-67.

[19] Mohamad Shady Alrahhal, Mohammad A. Mezher, Osamah A.M. Ghaleb, Mohammad Al-Hjouj, Raghad Sehly and Samir Bataineh. "An Augmentation-Based System for Diagnosing COVID-19 Using Deep Learning". International Journal of Advanced Computer Science and Applications(IJACSA)16.8 (2025). http://dx.doi.org/10.14569/IJACSA.2025.0160819.

[20] Alrahhal, Mohamad Shady, 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).

I am a student at FBSU, Cybersecurity specialization