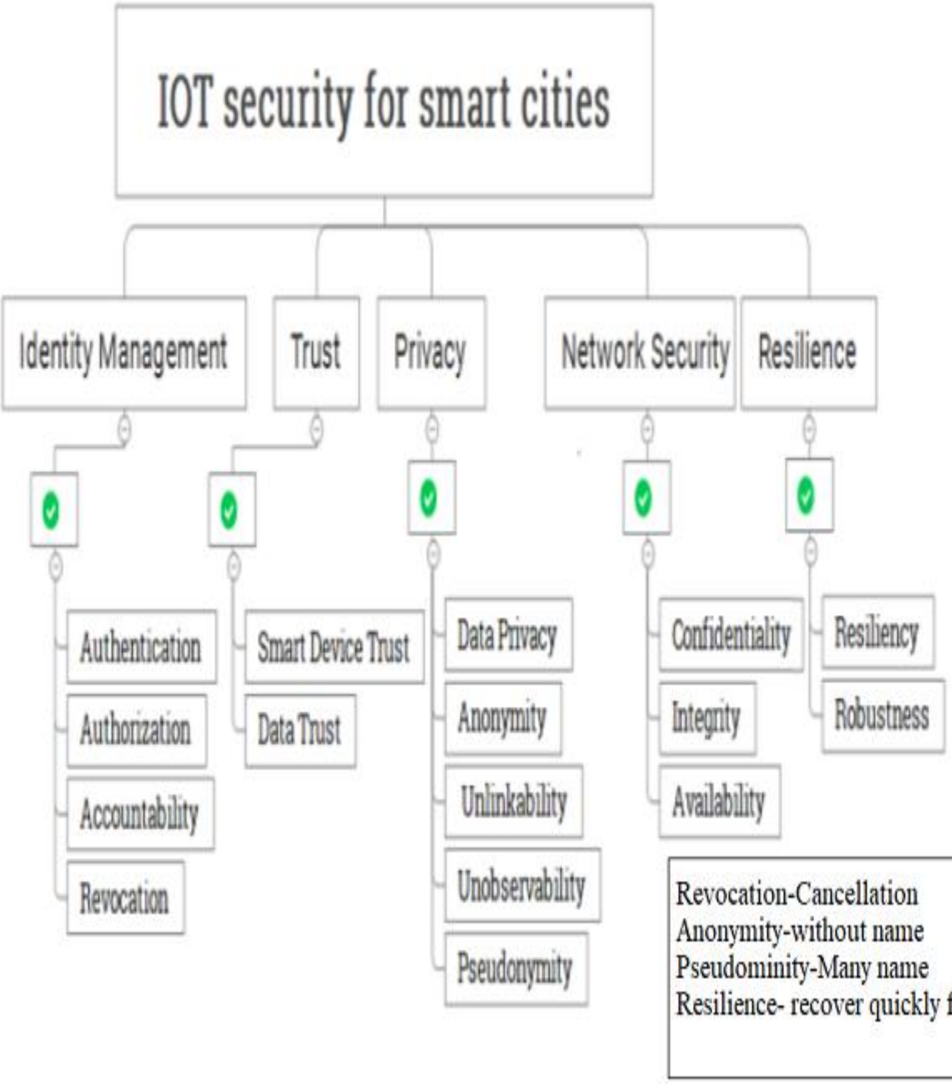
Security, Privacy and Trust in IoT-Data-Platforms for Smart Cities

Smart city technologies can improve the quality of life for citizens, increase efficiency and sustainability, and drive economic growth. Still, these benefits are only possible if the systems are designed with trust, privacy, and security in mind.

Ensuring trust, privacy, and security in future sustainable smart cities is critical for several reasons.

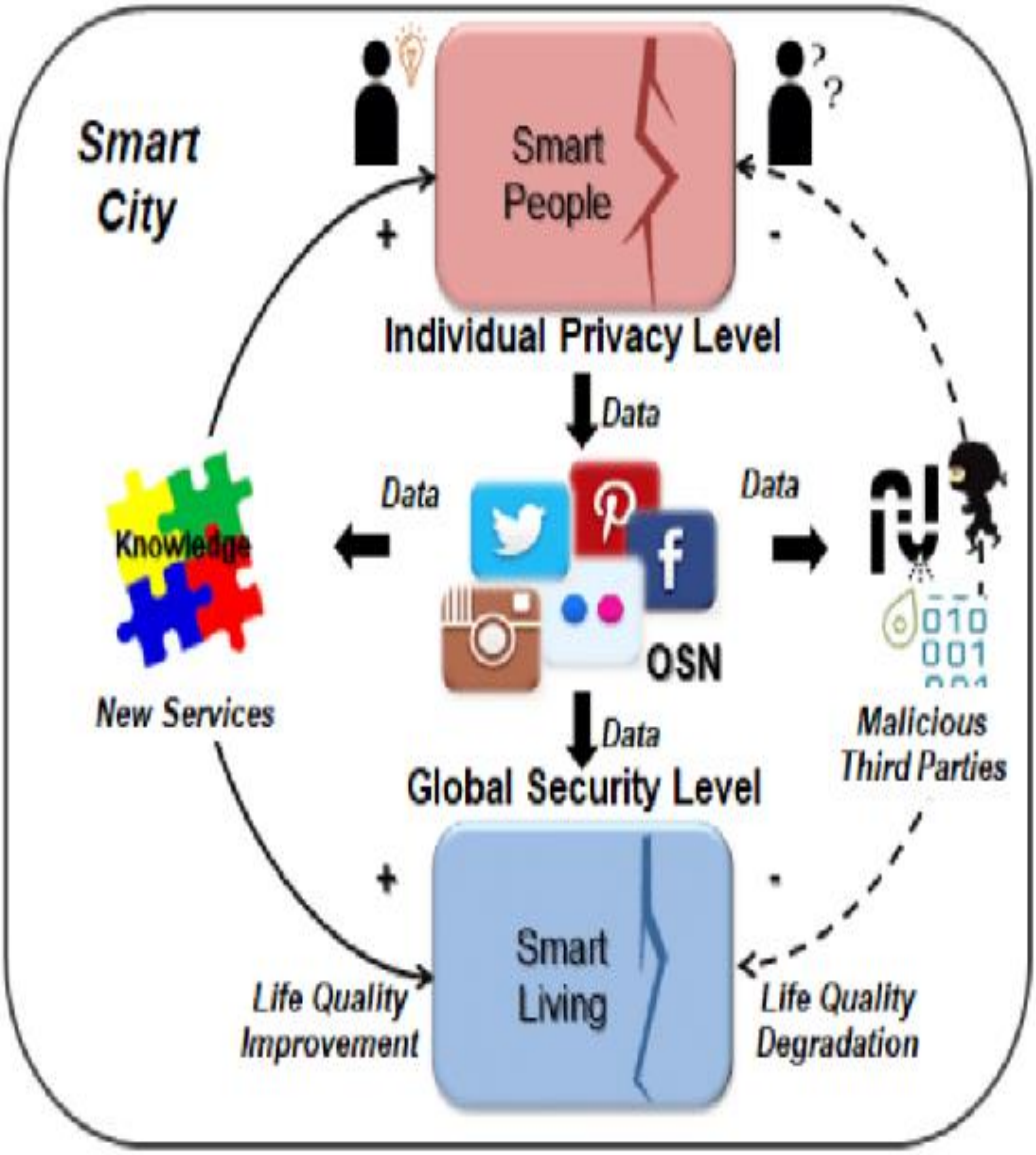
Ultimately, ensuring trust, privacy, and security in future smart cities is essential for creating sustainable and equitable urban environments that benefit all citizens. The successful development of sustainable smart cities depends on implementing robust measures to ensure trust, privacy, and security.



Revocation-Cancellation
Anonymity-without name
Pseudominity-Many name
Resilience- recover quickly from difficulties

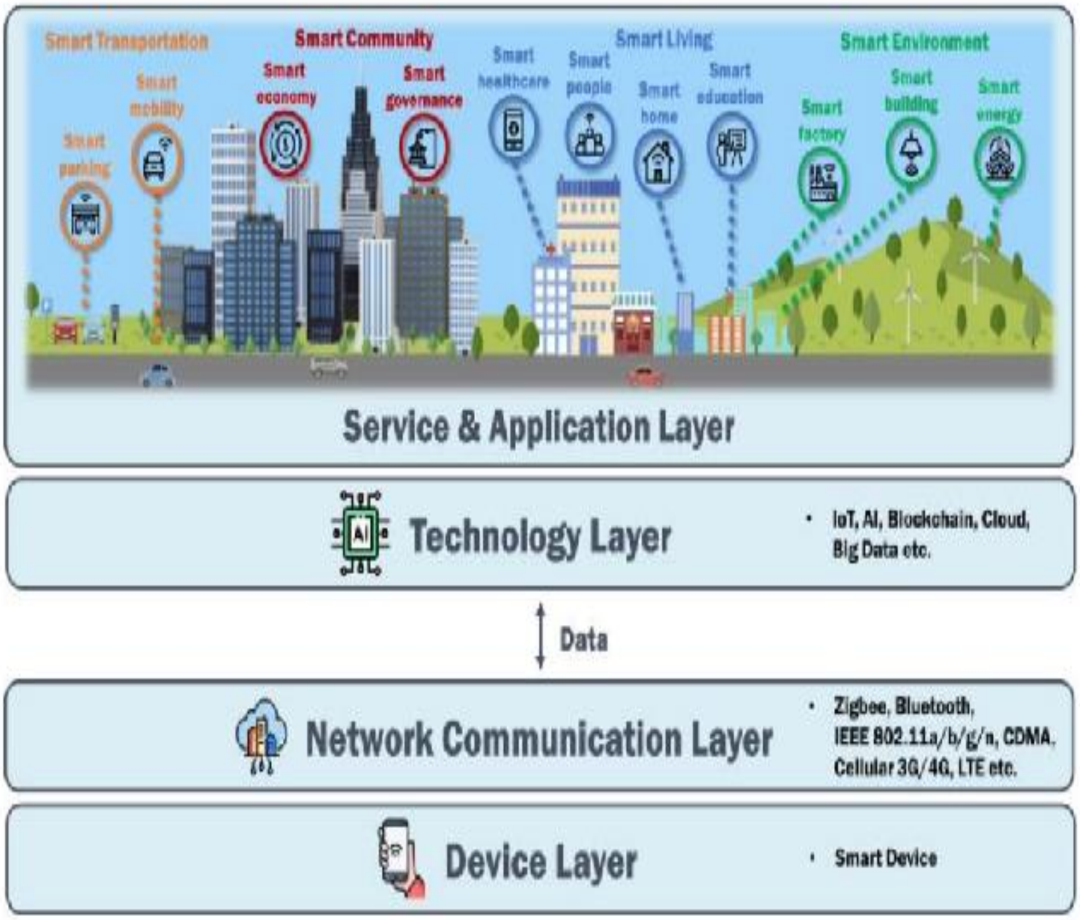
To achieve these objectives, technical solutions such as data encryption, access control, authentication, data minimization, anonymization, blockchain technology, and threat modelling can be employed. Encryption can secure sensitive data, access control mechanisms ensure only authorized access, authentication verifies identities, data minimization limits data collection, anonymization removes personal identifiers, blockchain technology provides tamper-proof and decentralized records, and threat modelling identifies potential security threats.

A holistic approach that considers the entire smart city ecosystem is essential to safeguard citizen privacy and security while delivering the benefits of smart city technologies to enhance urban life.



Key Elements of Smart Cities :

Smart cities can be divided into four layers. In the top layer, there is the provision of services and applications for residents living in the smart cities. Below this, there are the technology, network communication, and device layers.



Smart services can carry out the real-time monitoring and management of smart buildings, smart factories, and smart energy systems, which can enhance energy efficiency and waste management.

Cyberattacks are primarily directed towards smart city services and applications, making cybersecurity countermeasures essential for ensuring the safety of smart cities. The risk of cybercrime also increases with the implementation of these technologies.

AI technology is rapidly evolving to enable the fast and efficient delivery of complex services for small-scale smart city elements, such as smart homes and smart buildings, as well as large-scale elements, such as smart infrastructure and smart transportation.

Big data technology is a key enabler of AI as it can collect and analyse the vast amount of data generated in smart cities, thereby allowing AI to predict or infer future results and make better decisions. Additionally, blockchain and deep learning technologies can be used to provide smarter automation services for smart cities as data can be learned and determined autonomously.

Authentication technology is also being researched for smart cities from a blockchain perspective. However, privacy and security issues arise when data are exchanged across a wide range of areas in smart cities. As a potential solution, blockchain is increasingly being used for some data exchanges.

By enabling smart transactions through smart contracts and decentralized applications, blockchain provides a high degree of autonomy for the operation of smart cities.

The information-centric networking (ICN) routers can be used in smart home networks for more efficient content distribution due to their increased caching capacity and improved cyber security.