FLASH networks

Smart City Security

Smart cities and security threats

Smart cities stimulate economic growth and sustainable living, all while enhancing their citizens' quality of life through intelligent technologies and data analysis. The true value lies in how effectively technologies are employed. The smartness of a city is evaluated based on a range of characteristics, including the presence of technology-driven infrastructure, dedication to environmental initiatives, efficient and reliable public transportation systems, forward-thinking urban planning, and more. It is important to safeguard smart cities against cyber-attacks and data theft, while also ensuring the accuracy of reported data. The number of potential vulnerabilities and attack methodologies remains unknown.

Data and identity theft pose significant risks. Unprotected smart city infrastructure, such as smart parking garages, EV charging stations, and surveillance feeds, can provide cyber attackers with a wealth of targeted personal information that can be exploited for fraudulent transactions and identity theft. Another vulnerability is the **man-in-the-middle attack**, where an intruder breaches, disrupts or impersonates communications between two systems. For instance, a man-in-the-middle attack on a smart valve in a wastewater system could have catastrophic consequences, leading to a biohazard spill.

Distributed Denial of Service (DDoS) attacks aim to render a machine or network resource unavailable by disrupting services through a flood of requests. In the case of a distributed denial-of-service attack, multiple sources generate incoming traffic, making it difficult to thwart the cyber offensive by blocking a single source. Within smart cities, parking meters can be breached and coerced into joining a botnet, programmed to overwhelm a system by simultaneously requesting services. Popular cyber security concern for smart cities is **device hijacking** in which attackers gain control of a device without altering its basic functionality. These attacks can be challenging to detect, particularly within the context of a smart city. For instance, a cyber-criminal could exploit hijacked smart meters to launch ransomware attacks on Energy Management Systems (EMS) or secretly siphon energy from a municipality.

Protecting smart cities from these threats is crucial to ensure the seamless integration of technology and secure data management. Citizens of a smart city could be encouraged to report any suspicious activity or potential vulnerabilities to authorities or to take steps to protect their own personal information when using smart city services. Including this perspective could help foster a sense of shared responsibility for protecting smart cities against cyber threats. Protecting smart cities from these threats is crucial to ensure the seamless integration of technology and secure data management.

Harmony Cyber Security by Flash Networks can safeguard networks and devices from hacker infiltration and botnets. It works on any SIM card device, with no limitations on OS or CPU, and is compatible with all types of networks and transport technologies. Flash Networks has been the leader in network optimization and security solutions for over 25 years. Flash Networks` Harmony platform has been deployed in leading telecom companies globally. Flash Networks is well-equipped to handle the future demands of the mobile data world. Our expertise in handling high-throughput traffic enables Flash Networks to easily keep up and address technology changes. Check out more for us here.

FLASH networks