CASE STUDY

Securing Smart Cities Using emSecure

eMudhra provides Smart Cities with a high standard of security and protects its network communication and devices from Cyber Threats

Overview

A Smart City is an urbanized area which makes use of technology such as the Internet of Things (IoT) in order to create smart outcomes for its citizens. A typical Smart City solution has the following components, namely, Smart Parking, Smart Water, Smart Waste, Smart Environment, and Smart Energy. These Smart City solution components are largely reliant on the cloud for data storage and interconnected web of IoT sensors for data exchange. This complex web of devices in an uncontrolled and complex environment poses security concerns such as remote exploitation, Denial of Service (DoS), malicious insider threat, eavesdropping etc. Thus a solution is required that could detect & manage vulnerabilities, ensure data privacy & integrity, secure constrained devices, authorize & authenticate devices.
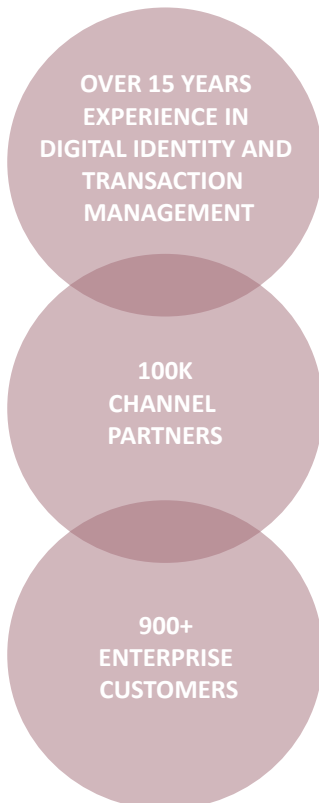
Business Matters

Businesses all over the world have started paying attention to Smart City Security. Cyber Attacks such as Mirai botnet and Dyn DDoS attacks have raised a lot of concern about IoT security and Cloud security which enable technology and platform for centralized data storage respectively for Smart City components. Thus a Smart City security solution is required that could detect, resist and recover from such malicious attacks.

Approach

Smart City security will be enhanced by establishing device identities before they can access gateways and upstream services & apps and by securing communication by encrypting the messages shared between interconnected devices. Furthermore monitoring network communication and activity logs for anomalies will help detect and manage vulnerabilities.

PKI Technology

Public Key Infrastructure framework uses a Cryptographic Key Pair – Private and Public Key for secure access and transmission of Information. It makes use of efficient and unbreakable encryption algorithms that can handle voluminous data and mitigate the risk of unauthorized access to sensitive data

OVER 15 YEARS EXPERIENCE IN DIGITAL IDENTITY AND TRANSACTION MANAGEMENT

100K CHANNEL PARTNERS

900+ ENTERPRISE CUSTOMERS

eMudhra Solution

emSecure is a solution provided by eMudhra which is capable of tracking cybersecurity threats to Smart City components in an effective and scalable manner. emSecure uses Public Key Cryptography to digitally sign and encrypt all communication in the IoT network by issuing Device Certificate and User Certificates. It ensures that all data transmitted is secure and un-hackable.

Digital Signature Authentication is required and used in emSecure to protect and confirm sensor data and enforce any specific automated actions based on the data. Key provisioning, deployment, and management are also a part of the solution.

Hardware and Supports Scalability

eMudhra is working with leading manufacturers of chips, TPM and LoRA devices globally to really go the extra mile and ensure that our offering is complete and capable regardless of the scale of our customer requirements.

emSecure uses trusted platform module for PKI and LoRA (WiFi/ 4G also supported) for connectivity of devices.

Benefits

- Better preemptive security measures

- Prevents data leakages and provides user/device identifiable data

- Provides end-to-end encryption of data thus eliminating the risk of MITM attacks

- User/Device identity is established using Digital Signature Certificates

- Isolation of trusted resources from public resources

- Ensures that only authorized personnel have access to sensitive data

- Strengthens and unifies data protection