Robust Security Key Algorithm for Scalable Broker Framework in Internet of Things (IoT) - Enabled Smart Cities.

Mohamad Khairi Ishak, PhD
Universiti Sains Malaysia (USM)

(email: khairiishak@usm.my)

ASEAN IVO
ICT Virtual Organization of ASEAN Institutes and NICT

Executive summary

The Internet of Things (IoT) is one of the most exciting technologies that promises to lead us to the future vision of connected world.

Securing these billions of IoT devices is amongst the top concern for researchers around the world. Several security techniques have been proposed to secure these IoT devices and associated networks.

However, due to the resource-constrained nature of these devices, and the sheer volume of network traffic limits the integration of a fully-fledged security solution like conventional networks.

In order to address these shortcomings a lightweight security solution is required for these devices that addresses these problems as well as provides adaptive security for IoT networks.

Therefore, to address these challenges, a novel lightweight security algorithm is proposed in this project that is scalable, platform independent and can be extended as an independent layer on currently available middleware platforms.

OBJECTIVE

FORMULATION	Initially a **model framework is formulated to identify** the attributes mentioned above. Then, an algorithm will be designed to establish the security framework that will generate Secure Private Identification Keys (SPID).
SECURITY FRAMEWORK	Next, the security framework of **SPID key management** will be generated to test the secure device provisioning and transactions between the devices on test network.
EVALUATION	Finally, the performance in terms of accuracy, efficient resource management and secure communication will be tested through IoT network and smart cities environment.

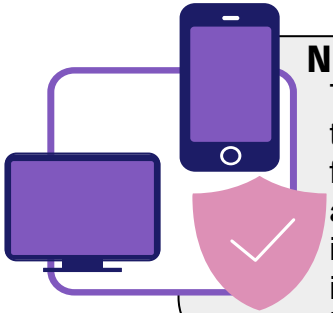
Background of Study

CHALLENGES

Conventionally, many independent schemes and policies were presented to address most of the challenges independently.

POWER

Huge computational overhead which consumes both energy and network bandwidth in real-world data intensive IoT applications.



NEW SCHEME

This project aims to address these challenges specifically for IoT networks, by providing a novel security scheme which is scalable, platform independent and homogenous in nature.

SCALABLE

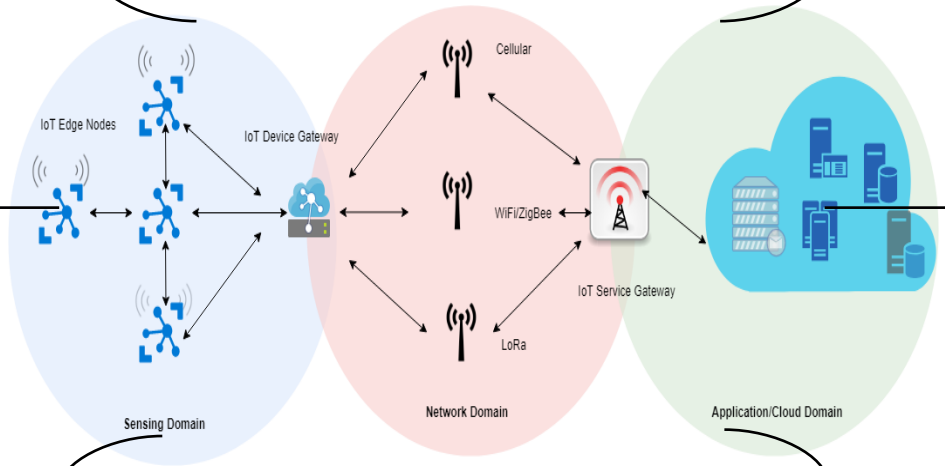
The proposed research presents a secure framework that is scalable and can be applied stand-alone or integrated with middleware frameworks as an added layer of security.

Security Framework

FOCUS
Focuses on network segmentation

SPID
Using secure Personal Identification (SPID) keys

INTERFACE
Uniquely identify the devices, networks, services, application interface



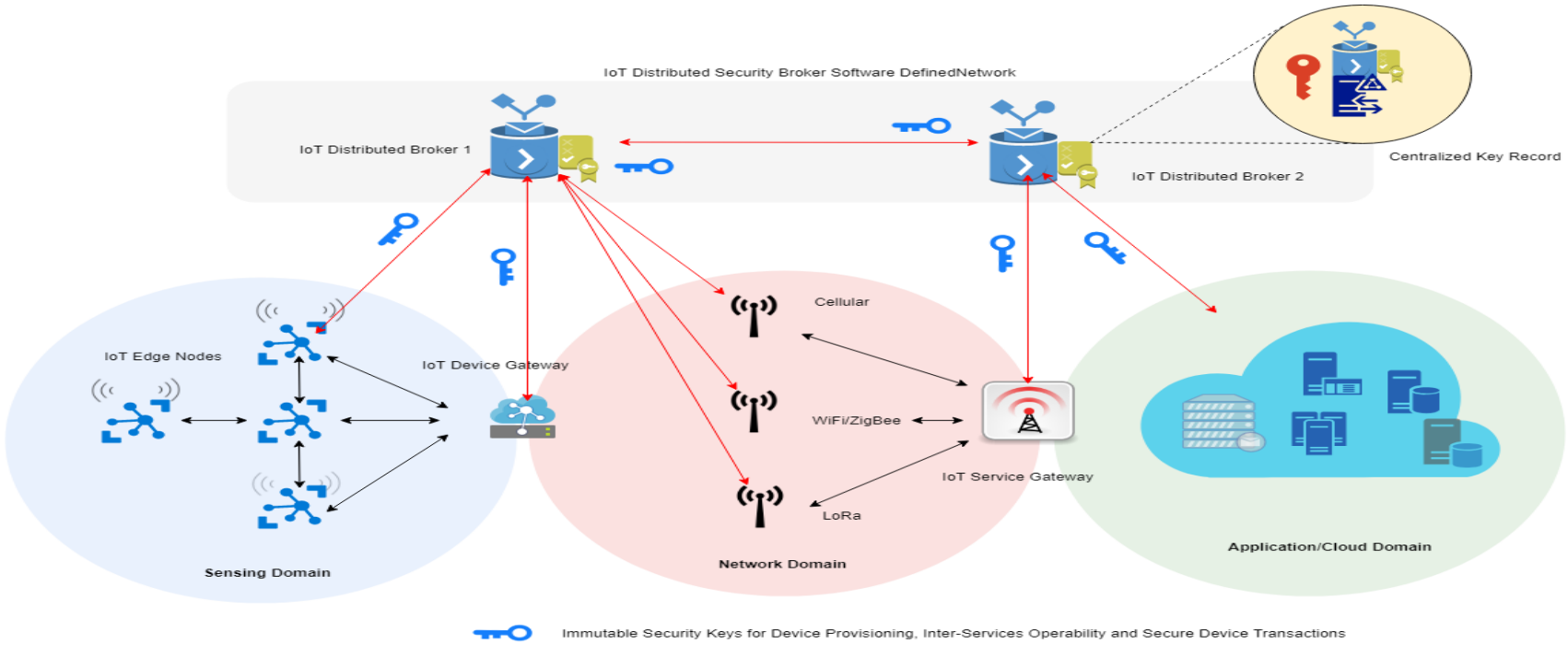
MIDDLE-WARE
security scheme proposes a middle-ware broker solution

DISTRIBUTION
parallel to the distributed deployment.

APPLICATION
three-layer model Sensing domain, Network Domain and Application Domain

Figure 1: Security Framework Requirements at different layers of IoT architecture

Middleware Security Broker Gateways



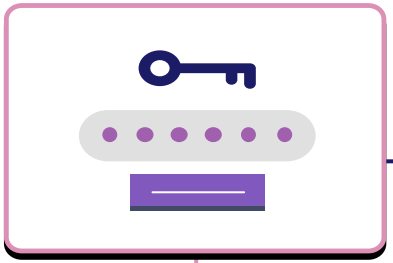
Broker Gateways for enhanced security and device/network isolation

BROKER

SECURITY KEY

Device provisoning inter service operatability

METHODOLOGY



STAGE 1

The mathematical formulation and algorithm design of the SPID algorithm

STAGE 2

Design of the embedded gateway platform to integrate the SPID broker gateway.

STAGE 3

IoT devices can be deployed in many topologies including centralized as well as distributed topologies.

STAGE 4

Implementation of the proposed method to existing as well emulated smart cities environment and performance analysis of the proposed scheme.

Significance of the Project

1. Enhanced security and trust factor for IoT devices to be deployed in multiple domains.

2. Enhanced trust factor by enabling secure transactions between IoT devices.

3. Ability for consumers to utilize IoT devices with advanced and cost-effective security in smart cities