Smart Airkey

We create secure keyless access environment

Secure access for IoT connected devices from a smartphone with Bluetooth.

The problem

It is predicted that by 2020 there will be about 20.4 billion connected devices in the world and such exponential introduction of IoT devices will increase the safety requirements for their use.
Currently the IoT devices rely on common technology and utilize simple security measures, and any violation can cause the serious threats.
The security policies must define how IoT devices are to be used and integrated into security processes, including user identification and access management. The majority of the IoT devices and should be segmented with controlled access within their own network and should be determinated which people can use IoT devices.

Proposed solution

SmartAirkey is a system for managing access to an IoT device using a smartphone equipped with Bluetooth 4.0/BLE running Android version 5.0 or higher or IoS version 9.0 or higher.
The system is designed to provide authorized access via a digital key to IoT devices equipped with a mobile access controller (BT module) integrated with a device control system.
The system incorporates a communication protocol between a smartphone and a BT module, which use digital keys, and a cryptographic signature based on the SHA-256 algorithm similar to authorization systems in banking systems.
The main problem of Bluetooth is the ability to intercept encryption keys at the time of the “handshake” process.
Since, in the SmartAirkey protocol, the keys are not transmitted over the radio channel at the time of the Handshake, it is impossible to fake commands.
The protocol is protected from hacking by "brute force" , “man in the middle” , “repeat play” (replay).

How it works

The access control operator issues a digital key for a specific IoT device to the user (sends to the mobile application via the Internet).
The user of an IoT device receives a digital key in a mobile application adapted for using SmartAirkey technology (receive-transmit, use of digital keys via Bluetooth and the Internet).
When the user approaches the IoT device and selects “Access" option in the mobile application, the application communicates with the mobile

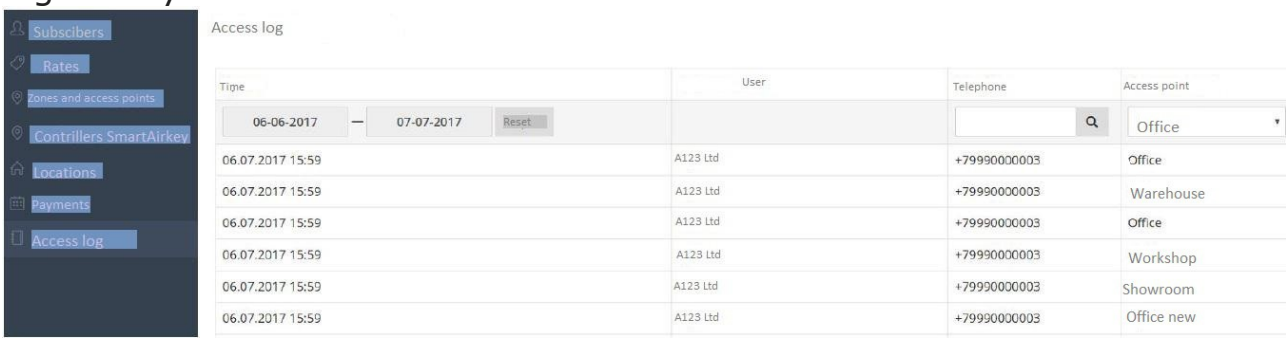
access controller (BT module) integrated with the IoT control system of the device and authenticates with a digital key.
The digital key is valid only for a specified period of time and is only suitable for a specific IoT device.
Digital keys are securely protected by a cryptographic protocol based on the digital signature SHA-256.
The secret information is not transmitted over the air, therefore, it cannot be intercepted and used by an unauthorized person to access the IoT device.

Solution components

The system consists of the following components:

- Cloud service for managing digital keys.
- Mobile App.
- Mobile Access Controller (BL module) integrated into the IoT device.

The cloud service allows the operator to issue, send,modify or revoke digital keys.

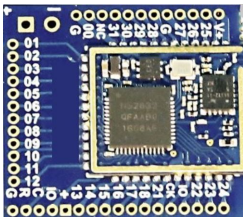


The image is intended for illustrative purposes only.

The mobile application stores digital keys and allows the user to access the IoT device from mobile device with Bluetooth.

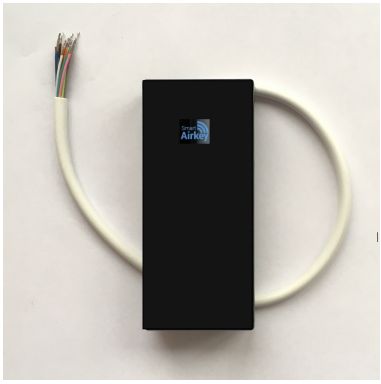
The mobile access controller (BT module) is integrated with IoT device and grants the user access to the device.
The mobile access controller (BT module) can be integrated with the IoT device in 2 ways (A or B):

A. BT module is an electronic assembly on a dedicated PCB for further mounting on the IoT device's board.



The image is intended for illustrative purposes only.

B**.** BT module is assembled as a separate device (assembly), which is enclosed in a case and installed inside/outside the housing of IoT device.



The image is intended for illustrative purposes only.

PoT - proof of technology

You can quickly test the technology with help of COTS components:

1. SmartAirkey controller
2. SmartAirkey mobile application (Android and IoS)
3. Cloud service digital keys SmartAirkey

The SmartAirkey controller requires a power supply of 10-15 V and has a relay for switching up to 3A load, which allows testing of almost any device.

The image is intended for illustrative purposes only.

Steps of integration process

- To integrate the SmartAirkey access control system into the connected IoT device need to make the following steps:
- Integrate access operator's service server with SmartAirkey cloud key management service. The digital key service has an advanced API that supports all the necessary methods for integration into other systems and external management of digital keys.
- Connect the access library that manages a digital keys in the mobile application of access operator's service. The library will perform the function of communication between App with the mobile access controller (BT module) and the implementation of a secure crypto-protocol.
- Integrate the BT module made on the basis of customer requirements with IoT device.
- The BT module can be integrated with IoT device by buses SPI, I2C, UART, CAN and can be supplied as an assembly on a board or stand alone enclosed module in the case connected by a cable to the IoT device.

Our competencies and experience

CybTech LTD bears many years of experience in design local identification systems based on Bluetooth and digital identifiers. The company's competencies cover a full range of digital solutions development - electronics design, mobile application and cloud computing based solution development.

OÜ Xmetra since 2013 is engaged in marketing, products adapting and promoting the modern solutions in the field of telematics,, access control, shared economy, IoT and M2M.

Contact us

E-mail:info@xmetra.com

www.xmetra.com