SECURE SMART SYSTEM OFFICE (SSSO)

Xiao Lin Chen,
Heesang Kim,
Mdzafar Sadak
Aparicio Carranza, PhD

2019 ECC CONFERENCE, June 9 – 11 at Marist College

AGENDA

INTRODUCTION

FLOW CHART

Hardware Components

Google FireBase Overview

Key Features of FireBase

ENCRYPTION & DECRYPTION

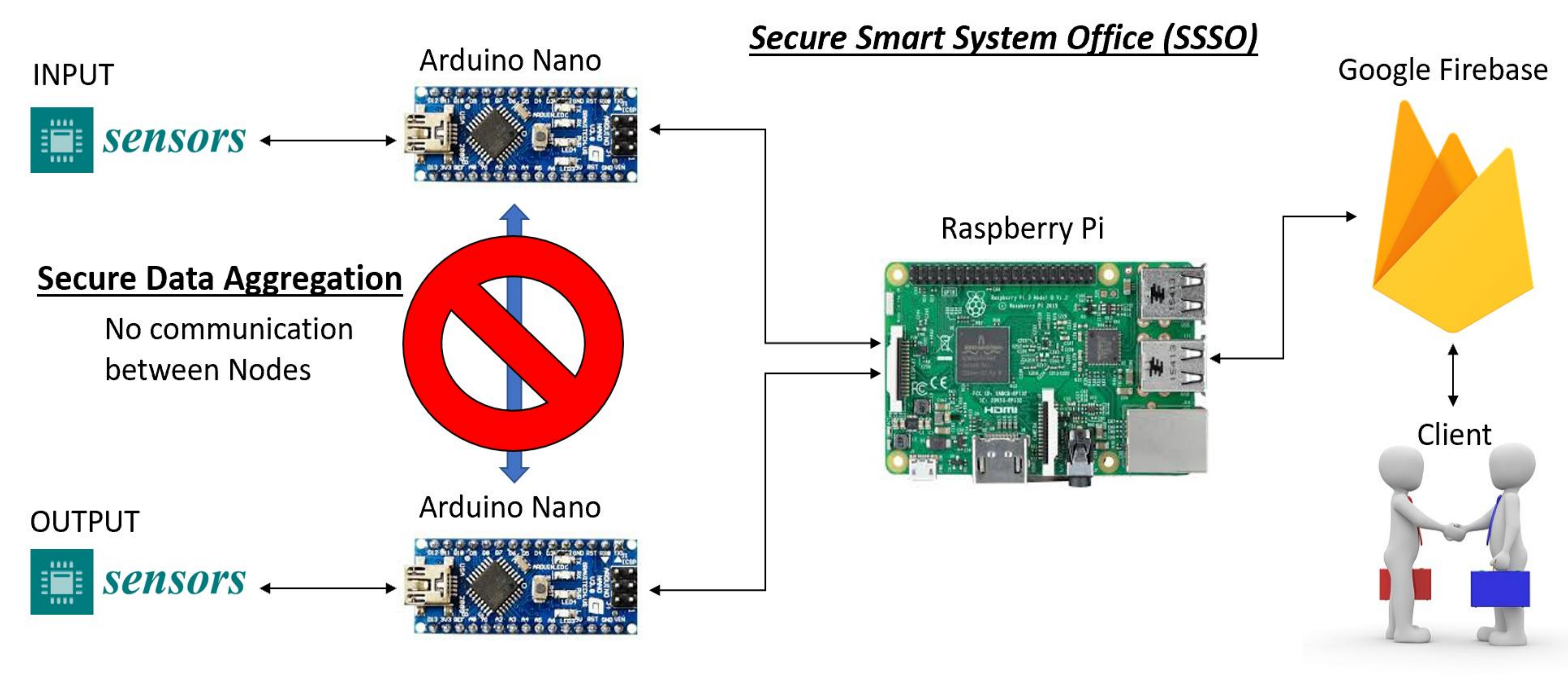
DATA AGREGATION

CONCLUSIONS

INTRODUCTION

- Secure Smart System Office represents a special feature that allows employees to comfortably manage their working environment In and Out of the office
- Eco-friendly smart system which relies on a number of connected devices that can monitor, control, and manage various operations and equipment
- Security mechanisms such as firewall, data aggregation, encryption, decryption, will be implemented to prevent from a passive and active security attack

FLOW CHART


Secure Smart System Office (SSSO)
INPUT
sensors
Arduino Nano
Secure Data Aggregation
No communication
between Nodes
OUTPUT
sensors
Arduino Nano
Raspberry Pi
Google Firebase
Client

HARDWARE COMPONENTS

- Raspberry pi
- Arduino board
- RGB LED
- Temp/humidity sensor
- A buzzer
- Fan
- Ultrasonic sensor
- 3D printed parts

GOOGLE FIREBASE OVERVIEW

- Firebase is a Backend as a Service (BaaS) that is powered by google cloud platform
- Data will be stored in JSON and synchronized to every connected client
- It supports cross-platform such as Android, iOS, windows

KEY FEATURES OF FIREBASE

- Storage
- Hosting
- Analytics
- Authentication
- Notifications

ENCRYPTION & DECRYPTION

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it
- Encryption is a risky procedure since we are modifying system files - then it might cause some errors such as boot failure
- Some Examples: data being transferred via network, mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines
- Decryption is the reverse process of encryption so that a client is able to access

DATA AGGREGATION

- The secure Data Aggregation is about adding a secure aspect during data aggregation. Many nodes of sensor connected to the individual central controller
- Each controller analyzes and processes the raw data. For hackers who try to hijack the data transferred through the network, it is easy of gaining control of one controller and sending false data to the main controller
- For other controllers that attach to sensors directly, they can only send data to the central controller and have no privilege to store data and communicate to other nodes
- Using Data Aggregation in WSN system reduces energy consumption

CONCLUSION

- *We have implemented a Raspberry Pi encryption*
  - *The first stage of encryption was completed including a Raspberry Pi configuration, installing packages, and implementing some key encryption commands*

- *Google Firebase cloud was successfully deployed, and firebase has been connected to a Raspberry Pi*

- *The 3D printed SSSO demo has been printed and hardware components were placed*

Questions?