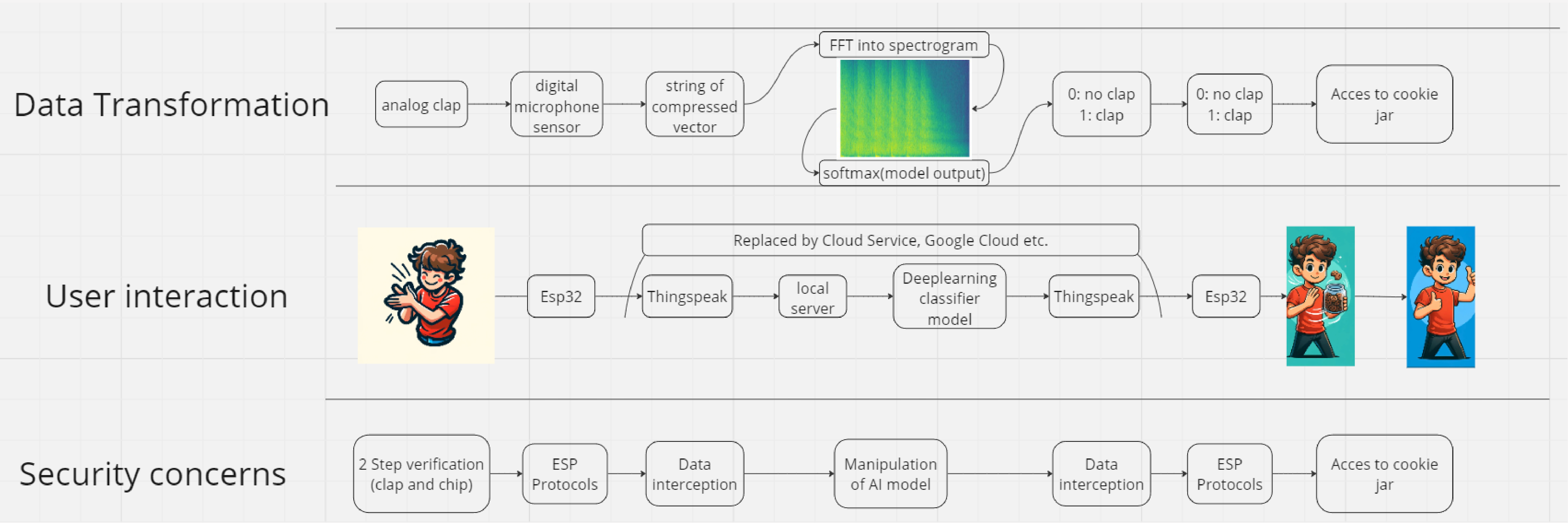
DTU Electrical Engineering
Department of Electrical Engineering

The 2FA Cookie Jar

Bruun, Andreas; Christoffersen, Martin; Grøngård, Mikkel Romvig; Sørensen, Rasmus Saugmann; Standke, Augustin Hellmut


Data Transformation
analog clap
digital microphone sensor
string of compressed vector
FFT into spectrogram
softmax(model output)
0: no clap 1: clap
0: no clap 1: clap
Acces to cookie jar

User interaction
Esp32
Replaced by Cloud Service, Google Cloud etc.
Thingspeak
local server
Deeplearning classifier model
Thingspeak
Esp32

Security concerns
2 Step verification (clap and chip)
ESP Protocols
Data interception
Manipulation of AI model
Data interception
ESP Protocols
Acces to cookie jar

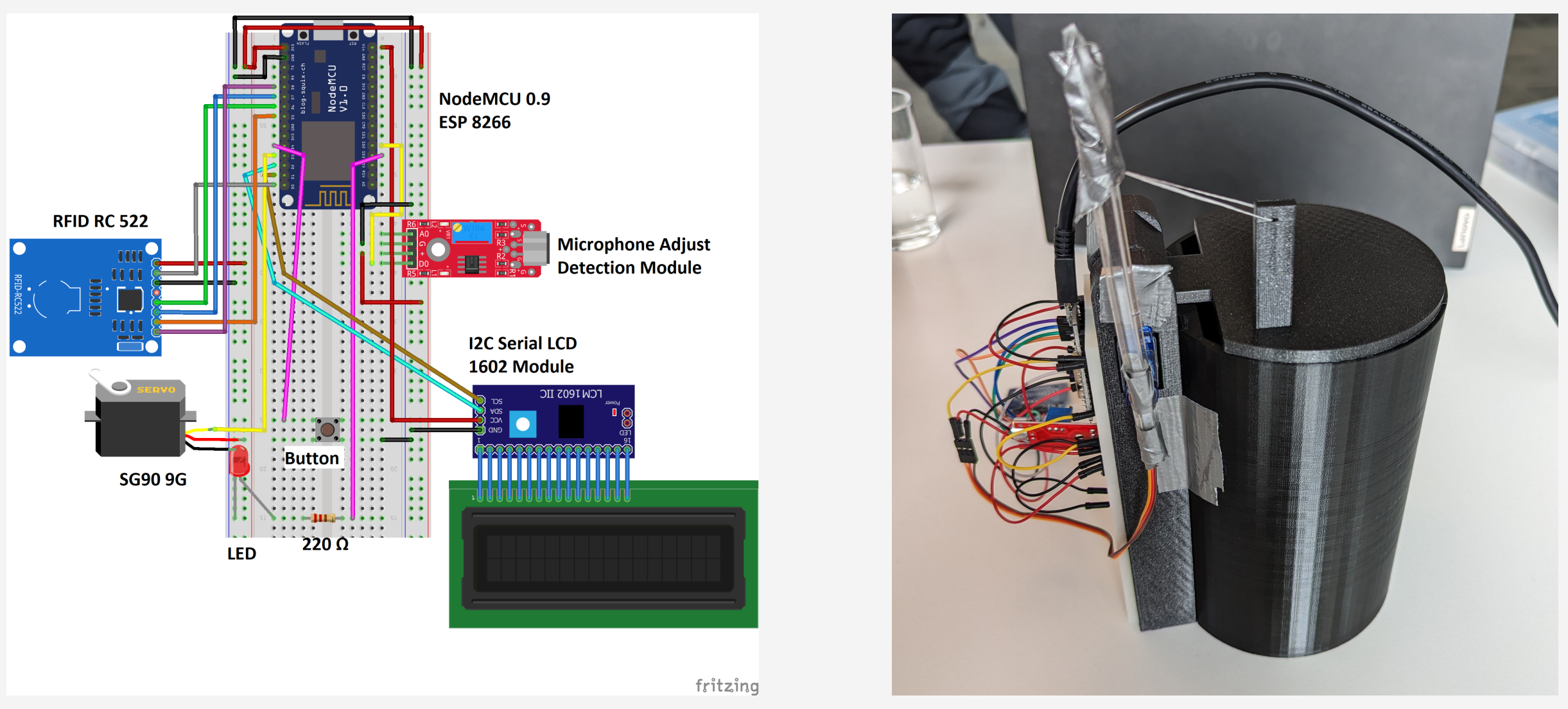
Figure 1: An overview of our project

1 Introduction

This project aims to enhance security in Radio Frequency Identification (RFID) technology, specifically within Internet of Things (IoT) applications. It highlights the increasing use of Radio Frequency (RF) tools like Flipper Zero and the need for improved authentication mechanisms. The proposal suggests integrating an RFID-based unlocking system with a physical input, such as a clap detected by a microphone, to ensure the user's physical presence and add an extra security layer. Furthermore, the text outlines plans for a logging mechanism via a Wi-Fi-connected web server to monitor access attempts, providing valuable data for the security aspect and potential machine learning analysis. The overarching goal is to fortify IoT systems' security by ensuring all system components' robustness and reliability

2 Hardware Design

2.1 Circuit and 3D-Design


NodeMCU 0.9
ESP 8266
RFID RC 522
Microphone Adjust Detection Module
I2C Serial LCD 1602 Module
SG90 9G
Button
LED
220 Ω
fritzing

(a) A Fritzing diagram for our project

(b) The 3D-printed prototype of the cookie jar

3 Code

3.1 Embedded code Arduino IDE, was used to create our code to our esp8266. Then to structure our code we made a document over what functions that we wanted to have for each part of the components used in our project. By only calling the functions at a given time, we ensured that our main loop was only blocked in a correct way, and able to react in real-time.

3.2 Backend/Thingspeak The backend is a mixture of Thingspeak for data storage and local server using Python for data inference.

Why We Use ThingSpeak:

- Cross-Platform Compatibility: Seamless integration across various platforms and support for multiple programming languages.
- User-Friendly: Easy to use with a straightforward API, suitable for both novices and experts.
- Built-in Analytics: Features integrated MATLAB tools for direct data analysis and visualization.

Limitations of ThingSpeak:

- Data Transfer Rate: Limited to one entry every 15 seconds, which may be restrictive for high-frequency data updates.
- Storage Capacity: Limited data storage, unsuitable for large-scale or long-term data collection.
- Scalability: Not ideal for large commercial or industrial projects due to scalability constraints. Other services such as Azure or Google Cloud offer more streamlined end-to-end tools for data-management- and AI-integration.

4 Data Transmission and Security

4.1 Two-Factor Authentication The idea of our project is a proof of concept of two-factor authentication. Our implementation is a simple case, showing the general value of the idea, though leaves room for improvements.

4.2 Data Transmission

Protocols used in the ESP 8266:

- Application: HTTP (Used for communication to Thingspeak)
- Transport: TCP (Used due to guarantee of retransmission)
- Internet: IP
- Link: Wi-Fi (Wi-Fi ensures flexibility)

This protocol comes with a set of security risks illustrated in the figure below:

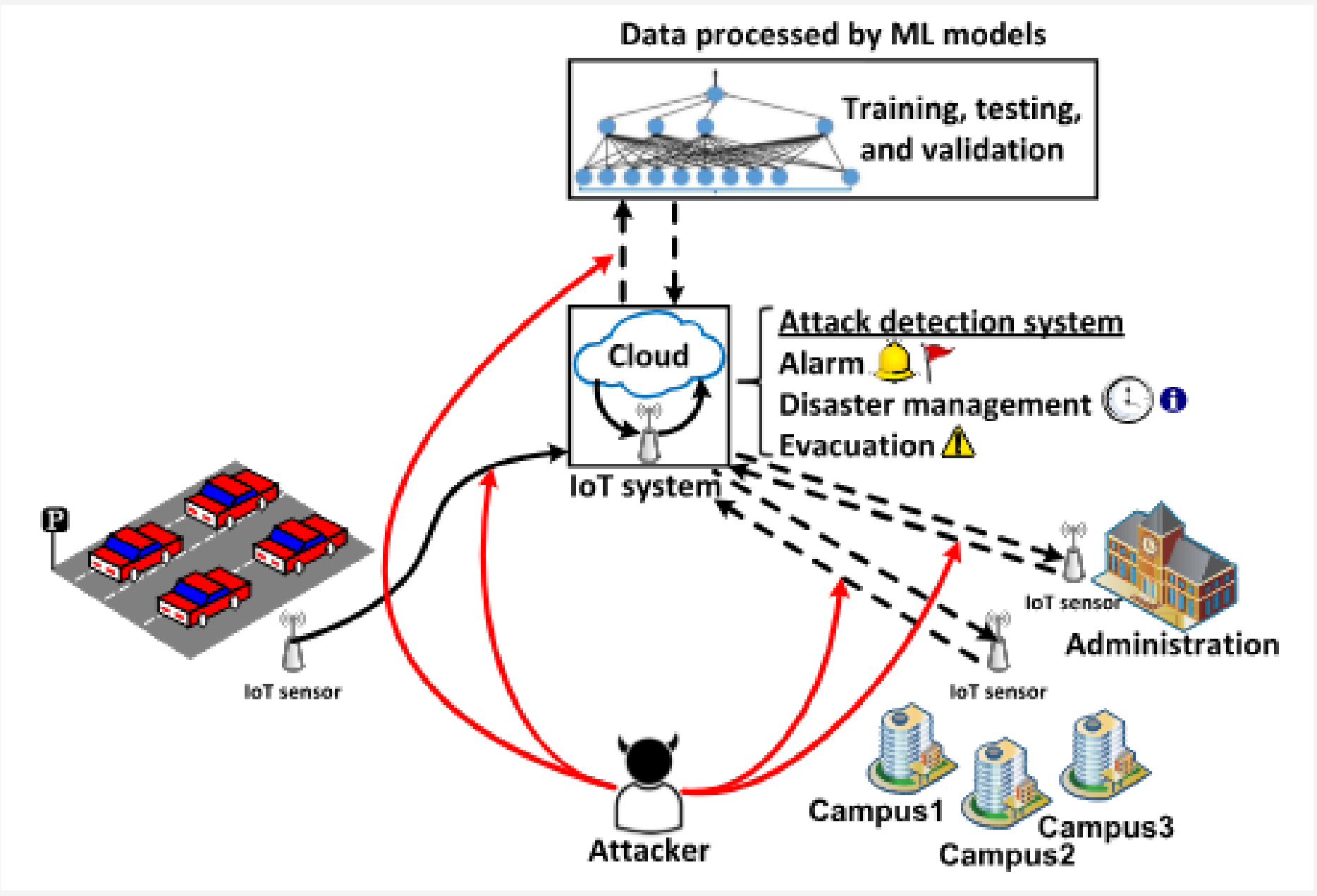


Figure 2: Overview of security risks. (1)

Some of the security risks include source code, HTTP, API, manipulation, and to some extent unethical use of data. A few examples of Counter-measurements are passwords and API keys in separate files locked away etc. Further work would include: using the more secure, HTTPS and AI to find abnormalities in data and to find misuse of our system. To include AI we would like to implement Random Forest in the first issue, and Duenna from "Anomalous behavior detection-based approach for authenticating smart home system users" or look into whether Thingspeak has something equally useful.

5 Conclusion

Although the prototype is working as intended, every aspect of it needs improvements or a change in technology looking forward.

1: By M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed and M. M. Salim, "Toward Secured IoT-Based Smart Systems Using Machine Learning," in IEEE Access, vol. 11, pp. 20827-20841, 2023, doi: 10.1109/ACCESS.2023.3250235. link: https://ieeexplore.ieee.org/abstract/document/10056119