Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 20, Issue 1 Ser. 1 (Jan. – Feb. 2025), PP 14-22
www.iosrjournals.org

Electronic Lock For A High-End Data Acquisition System

Prof. Dr. Matthias Górka[1], Kurian Cyriac[2]
[1,2](Deggendorf University Of Technology, Germany)

Abstract:
Protecting data acquisition devices in environments vulnerable to unwanted physical access, like academic institutions with nearly public access or in mobile applications, necessitating solutions in the field of security. To create a security framework, this study shows an electronic lock system for the DEWETRON DEWE3-A4 that can be transferred to other grid powered devices. It integrates GPS satellite positioning with an average geofencing break alert of 20 s, GSM communication technologies, access authorization with an average time of 1.2 s and tampering detection with a delay of 0.29 s. The suggested solution improves the protection without compromising the device's operation or warranty, in contrast to conventional mechanical locks that provide restricted security features. The system meets the need for a non-intrusive but effective security measure with its capacity to restrict access to specific locations, its remote-control capabilities, and its real-time alerts for unwanted access attempts or a low battery alert within 0.6 s. According to the research, the implementation of such an electronic lock system greatly reduces the possibility of equipment and data theft, creating a new standard for the safety of expensive (data collection) equipment.

Key Word: *Electronic Lock System, System Design; System Security; RFID; DEWETRON.*

Date of Submission: 03-01-2025 Date of acceptance: 13-01-2025

I. Introduction

Figure 1.1: Front view of the data acquisition device DEWE3-A4 [2]

The security of high-end data acquisition devices has become a key concern, particularly in contexts such as academic institutions, mobile applications and industrial settings where such equipment is widely employed. This study based on [1] presents a novel method for preventing unwanted access to the DEWETRON DEWE3-A4 [2] that is shown in figure 1.1, a data acquisition system, using a customized electronic lock system but can be transferred to other grid applications as well. The DEWE3-A4, that's suitable for high accuracy and versatility in signal analysis and data collection, requires a security solution that is both reliable and non-intrusive. The proposed solution combines the GPRS (general packet radio service) and GPS (global positioning system) satellite locating technology with the use of IR (infrared) and RFID (radio-frequency identification) sensors. Together, these parts form a security mechanism that ensure the integrity and compliance with warranty terms of the DEWE3-A4, while also improving its physical security. The advantage is an easy to add solution without drilling, gluing or opening of the housing and therefore loosing any warranty rights of the manufacturer. The IR sensors are a part of an alert system that monitors and reacts to unwanted access attempts, while RFID technology provides an additional layer of protection by allowing user access control based on verified tags.

II. Material And Methods

System Requirements:

Based on an internal requirement process [1] and [3] several product features are defined, that a finale system should be capable of. The following list shows the most relevant high-level features:

- **Power efficiency** – can work for a time without any external power support and reports in case of low battery
- **Remote monitoring** – get information without being next to the device
- **Intrusion detection** – detect if someone opens the system
- **Geofencing** – detect when the device leaves a given area
- **User control** – distinguish the rights between different roles

Figure 2.1: RFID reader RC522 [6]

Figure 2.2: Infrared sensor TCRT5000 [7]

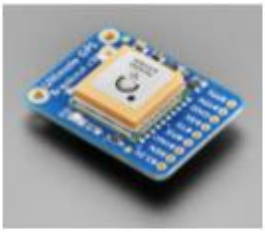

Figure 2.3: Adafruit ultimate GPS breakout module [8]

Figure 2.4: Pinning of the SIM800L GSM module [9]

System Architecture:

To realize the mentioned product features, some core components are defined:

- **Microcontroller:** For the task management and real time communication a Raspberry Pi 4 B 8GB [4] is used due to its GPIO (general purpose input/output) pin support, integrated connectivity choices, computing power and availability in the laboratory.
- **RFID:** A RFID chip with the RC522 reader as shown in figure 2.1 is used to enable a user specific and contactless access control that can be maintained without the need of distributing physical keys e. g. to distinguish between a staff member and a student. [5]
- **Infrared Sensor:** The infrared sensor TCRT5000 (see figure 2.2) is used for intrusion detection.
- **GPS Module:** For efficient geofencing and real-time position tracking, the Adafruit Ultimate GPS breakout [8] (see figure 2.3) module is chosen due to its sensitivity and accuracy.
- **GSM Module:** The SIM800L module shown in figure 2.4 is included because of its wide frequency support and quick network connection speeds, which provide dependable communication even in the absence of an internet connection.
- **Power Management:** To maintain continuous operation, the system draws power from the same source as the DEWE3-A4. To extend the usage, a combination of buck converter and a UPS (uninterruptible power supply) assures a reliable power supply even in case of disconnecting the power supply.

The resulting architecture consists of the RFID chip (for access authorization), IR sensor (for intrusion detection), GPS (for location tracking) and GSM (for remote communication in the event of theft) as critical components that are coordinated via the Raspberry Pi 4. Figure 2.5 shows the system architecture and its interconnections.

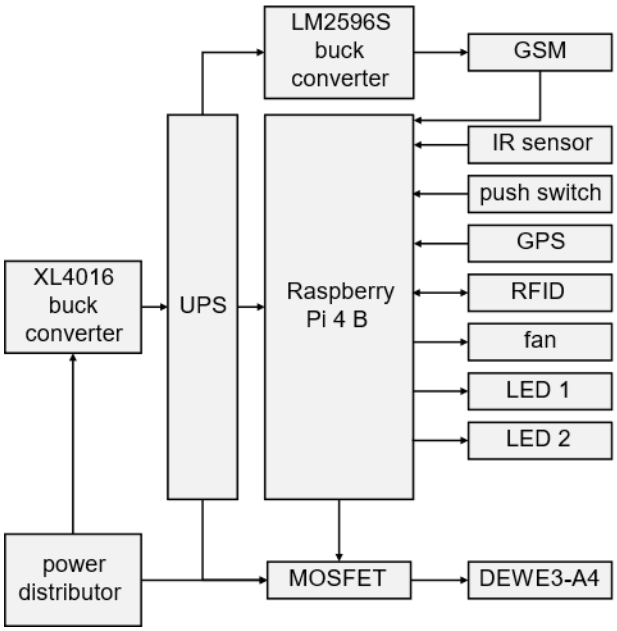

Figure 2.5: System architecture [1]

III. Result

Establishing connections between the Raspberry Pi and various modules, such as RFID for access authorization, an IR sensor for intrusion detection, GPS for location tracking, and GSM for remote communication in theft scenarios, as well as setting up communication via Telegram and E-Mail for alerts, are all part of the integration of the electronic lock system.

Power Supply

The power management system involved the utilization of a buck converter, which is assigned the duty of transforming erratic input voltage into a consistent 5 V output for the UPS system. This configuration is essential to minimize the possibility of power related disturbances by ensuring a steady power supply to the Raspberry Pi 4 and all linked modules.

A LM2596S DC-DC buck converter [10] that is shown in figure 3.1 is used to lower the 5 V output voltage from the UPS's to the necessary 3.7 V to 4.2 V range for the GSM module, guaranteeing effective functioning and connectivity.

Figure 3.1: LM2596S DC-DC buck converter for GSM module [10]

Raspberry Pi Configuration

The Raspberry Pi is configured with software drivers and libraries specific to each module, which made it easier to write custom code for controlling system functions like alerts and access control. Installing the operating system, attaching peripherals, and turning on SSH (secure shell) for remote access all helped to setup the Raspberry Pi. This configuration made it easier to integrate and manage the lock system's component parts in the development environment.

E-Mail Alerts and Telegram Bot

Using the BotFather function of Telegram [11], a bot is developed to enable real time warnings. The Python programmed bot alerts administrators in different cases like unwanted access attempts. Similarly, E-Mail alerts are set up with access token authentication and an E-Mail service provider's API (application programming

interface), allowing the system to automatically send E-Mails under predetermined parameters without the need for human interaction.

Access Authorization Feature

The access authorization is realized by the Raspberry Pi 4's connection with the RFID RC522 [6] module as illustrated in figure 3.2. The SPI (serial peripheral interface) allows the Raspberry Pi to communicate with the RFID RC522, which is essential for secure access control. To get this working, the SPI on the Raspberry Pi – which is by default deactivated – is turned on, allowing the module to communicate with the RFID. [12] The connections for this module are as follows: GND for ground; SDA for serial data signal; SCK for serial clock; MOSI for master out slave in; MISO for master in slave out; and RST for reset. In this arrangement, the IRQ (interrupt request) pin is not used.

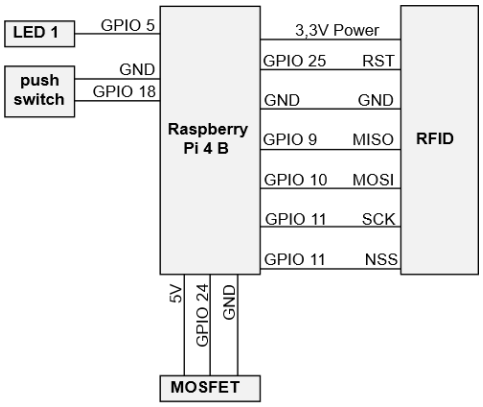

Figure 3.2: Block diagram of access authorization setup [1]

A technique to remove pin floating is required to guarantee dependable operation of the push switch that is used for manual control within the system. By using a Python script to turn on the Raspberry Pi's built-in pull-up/pull-down resistors, the status signal of the switch is stabilized without the need for external resistors.

In addition, the system directly interfaces with the Raspberry Pi using a MOSFET (metal oxide semiconductor field-effect transistors) as a power control mechanism. The GPIO output levels of the Raspberry Pi are compatible with the MOSFET, which is chosen due to its working voltage range of 3.3 V to 10 V.

Figure 3.3 illustrates the RFID access authorization process in our security system. Initially, the system prepares by initializing all devices. Upon RFID tag detection, the reader decrypts its message to check against the system's database. If the data matches, access is granted. In case the access is granted, the MOSFET powers the DEWE3-A4 device, and a Telegram alert notifies the owner. Conversely, if data mismatches or a push button is activated, the system denies access or disengages the MOSFET, maintaining security.

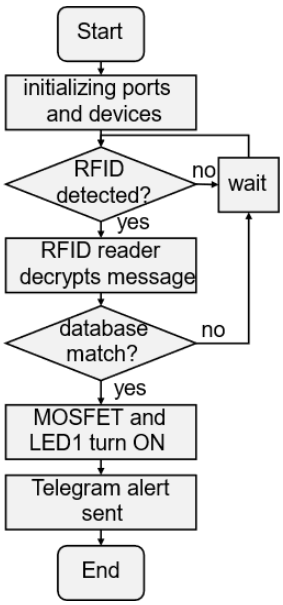

Figure 3.3: Flow chart of RFID authorization [1]

Battery Alert Feature

The UPS's multiple I/O functions contribute to the future development of the electronic lock device. The LO_DT pin switches HIGH at low values to indicate low battery status. [13] Concurrently, the LO_DT pin is used by the system to continuously check the battery levels. When the charge falls below 20%, an alarm via Telegram and E-Mail on low battery circumstances is send and the LED2 is turned ON. This enables the administrator to take actions, as the protection sooner or later will be stopped.

Intrusion Feature

The intrusion detection system that uses infrared sensors TCRT5000 is vital to the device's physical security since it monitors anything that moves within its detecting range. The system initiates its warning processes upon detecting movement, which may indicate any manipulation for example when someone tries to open the housing to manipulate the circuit. This results in the prompt dispatch of warnings via E-Mail and Telegram to alert users of a security occurrence. The prompt response to any security breaches is ensured by this dual channel notification strategy.

GPS and GSM Configuration

The serial communication between the GPS, GSM modules, and the Raspberry Pi uses the UART (universal asynchronous receiver / transmitter) protocol. GPIO 14 (RX) on the Raspberry Pi is designated for data reception from the GPS while and GPIO 0 (TX) is for the transmission to the GSM module. A buck converter adjusts the power supply to 4 V for the GSM module, accommodating its specific voltage requirements. Due to communication overlaps, reserved GPIOs 0 and 1 facilitate GSM module connectivity, necessitating the activation of UART2.

The purpose of the GPS and GSM combination is the possibility of a geofencing for the system. When the system first boots up, it initializes all required ports and hardware, the GPS for tracking location and the GSM module for communication. The system checks the device’s current geographical coordinates. [14] The next step involves evaluating these coordinates to see if the device is inside a geofenced area that is 20 m radius, which is the predefined geographic limit. The system reverts to monitoring if it finds that the device is inside the geofence’s perimeter. If the device is outside the geofence, the system will transmit commands to the GSM module, indicating a possible breach or unauthorized movement. As a result, the GSM module sends an SMS (short message service) to an administrator or monitoring service with the device’s current coordinates, informing them that the device is outside of the safe zone. The purpose of this automated notice is to protect the device from theft or unauthorized movement.

System Enclosure

The device's enclosure, designed to house the mentioned components, is designed as shown in figure 3.4. Special attention is paid to cable management and the ease of assembly or disassembly, catering to both maintenance and future upgrades.

PETG (polyethylene terephthalate with glycol modification) material is chosen for its durability, thermal resistance and 3D printing compatibility, enhancing the case design. The final prototype is a robust case that safeguards the components while optimizing their functionality through effective ventilation and design features like lid extrusions for precise placement.

Figure 3.4: System enclosure with lid [1]

Test and Verification

The key characteristics of the prototype RFID authentication, power management, geofencing, intrusion detection, and communication effectiveness are used to categorize the results. Figure 3.5 shows the general use case diagram of electronic lock system.

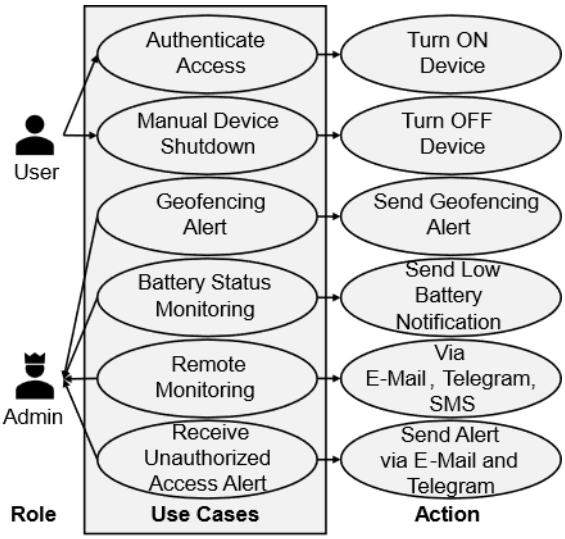

Figure 3.5: Use case diagram [1]

The system is put through several functional, integration and performance tests while the build up to confirm the requirements of the prototype:

- **Performance Testing:** Core of this test is the assessment of the system's responsiveness, power usage and overall stability, especially when it is under load or had a fluctuating power source. An average battery backup time of 2 h is measured. Moreover, the response of RFID reader recorded for 100 access attempts from different distances and the results are shown in the figure 3.6. The RFID system showed excellent user authentication reliability, identifying permitted access attempts 98% of the time. With an average authentication time of 1.2 s, the system accurately refused access for unauthorized tags across 100 trials while guaranteeing prompt and secure admittance for legitimate users.

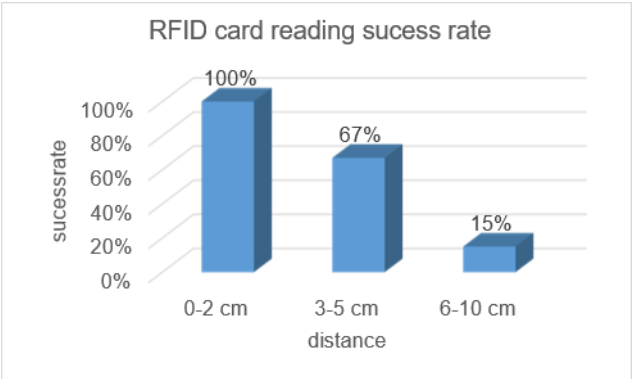

Figure 3.6: RFID card reading success rate [1]

- **Alert or Notification Testing:** Various trigger events, such as unauthorized access and low power status and geofencing are tested to see if the Raspberry Pi and GSM module could send timely alerts and notifications via SMS, E-Mail, and Telegram. [14] To reduce the number of alerts, the E-Mail notifications are sent only when there is an unauthorized access or low battery status. SMS sent when there is a geofencing break. All general notifications are sent to telegram. Table 3.1 shows the time delays between an event is taken place and until when the corresponding role will be informed.

test	access notification delay [s]	intrusion alert delay [s]	geofencing break alert delay [s]	low battery alert delay [s]
1	0.50	0.25	20	0.50
2	0.50	0.30	19	0.70
3	0.50	0.30	24	0.60
4	0.52	0.28	20	0.52
5	0.52	0.30	21	0.52
6	0.51	0.30	20	0.70
7	0.51	0.30	22	0.51

8	0.50	0.28	17	0.80
9	0.50	0.30	18	0.60
10	0.53	0.30	21	0.53
ø	0.50	0.29	20	0.60

Table 3.1: Alert delay test [1]

- **Low Battery Level Alert:** Testing shows that the UPS ensured a stable power supply, allowing uninterrupted system operation through power fluctuations and short outages. The expected low battery alerts are effectively communicated via Telegram as shown in figure 3.7 and by E-Mail. The average system response delay for this type of notification is 0.6 s. E-Mail alerts complemented the notification system, enhancing reliability in critical conditions

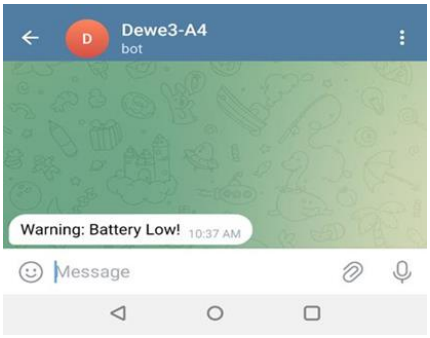

Figure 3.7: Low battery Telegram notification [1]

- **User action notification:** The system's ability to respond to the successful authorization demonstrated by the MOSFET's fast ON-OFF switching efficiency in controlling power supply to the data acquisition device following successful RFID identification. Figure 3.8 displays the Telegram notification in case a user accesses the system.

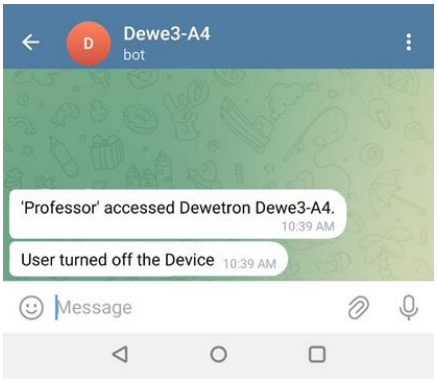

Figure 3.8: User access notification on Telegram [1]

- **Intrusion Detection:** In all simulated intrusion situations, the IR sensor detected unauthorized access attempts. When the sensor encountered a movement by the device box lid the IR sensor "alerts" the Raspberry Pi. Subsequently the alert message will be sent via Telegram as shown in the figure 3.9 and additional an E-Mail.

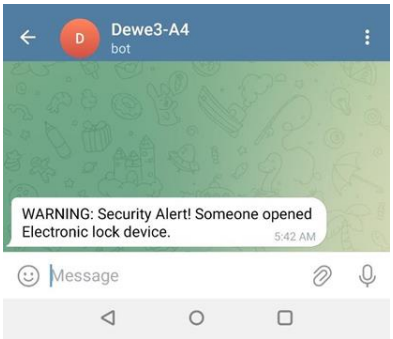

Figure 3.9: Intrusion alert on Telegram [1]

- **Geofencing:** The DEWETRON DEWE3-A4's location is recorded by the GPS module, which also enforced the geofencing rules that are established for the experiment. When the device is moved outside of the predetermined geographic border, e. g. outside of the laboratory, the system sent an alert. Figure 3.10 shows an example of the implemented location tracking.

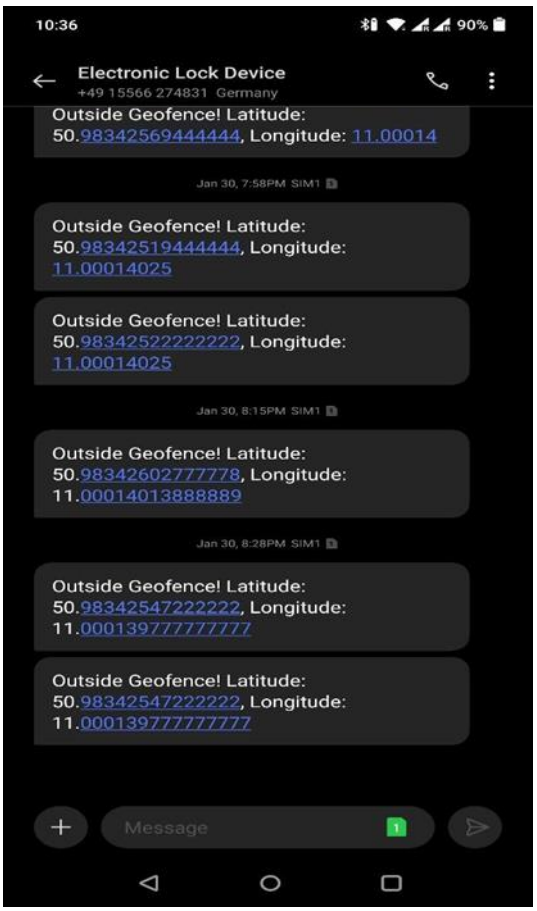

Figure 3.10: Location alert by SMS [1]

Once the geofence is breached the GSM module will send coordinates every 30 s. [15] The reliance on GSM networks may impair operation in locations with poor coverage. Environmental factors like heavy rain or physical barriers affecting the GPS reliability due to signal reception. In future application this can be mitigated by attaching an additional antenna or adding additional location tracking mechanisms via WIFI, positioning via GSM signal intensity or technologies like AirTags. [16]

In general, the concentration on a single prototype restricts broader tests, but for an early stage the tests show the effectiveness of the electronic lock system.

IV. Conclusion

This investigation on creating and implementing an electronic lock system for the DEWETRON DEWE3-A4, resulting in the necessary understanding of the components and procedures needed to improve security for high end data collection devices. A Raspberry Pi 4 is determined as the microcontroller for this application because of its processing powers, wide range of networking options and possibility for future development improvements.

The process of choosing and incorporating extra parts, such GPS and GSM modules and power management options, like UPS systems and buck converters, is based on the given requirements. Diverse tests of the manufactured prototype showing the capability of this technology like an average geofencing alert of 20 s, intrusion alerts 0.29 s but also the weaknesses like the availability of GPS and GSM signals. Further notifications like a low battery alert with an average delay of 0.6 s or an access notification with an average delay 0.5 s showed the functionality of the system. With an average battery backup time of 2 h and an average authentication time of 1.2 s all requirements are fulfilled.

Future directions could be including advanced encryption algorithms, deeper integration and therefore physical downsizing, improved user management and new energy-efficient power management strategies.

Additionally, this application can used for other or older grid applications that need a protection and dedicated user access by small modifications to use it generally. This would include a change in the power distribution socket to the individual target device, a different input power socket and change of the internal power supply. All other hardware and software can be taken over.

References

[1]. K. Cyriac, Electronic Lock For High-End Data Acquisition Device. Master Thesis, Faculty Of Applied Natural Sciences And Industrial Engineering, Deggendorf Institute Of Technology, Deggendorf, Feb. 2024.

[2]. Dewetron. (Accessed: 2024, Jul.) Highspeed Dewe3-A4 Für Mobile Datenerfassung. Dewetron.Com. [Online]. Available: Https://Www.Dewetron.Com/De/Messtechnik-Produkte/Hardware-Zur-Datenerfassung/All-In-One-Mit-Display/Dewe3-A4/

[3]. A. Churi, A. Bhat, R. Mohite, And P. P. Churi, "E-Zip: An Electronic Lock For Secured System," In 2016 Ieee International Conference On Advances In Electronics, Communication And Computer Technology (Icaecct). Ieee, Dec. 2016.

[4]. Raspberry Pi. (Accessed: 2024, Jul.) Raspberry Pi 4. Raspberrypi.Com. [Online]. Available: Https://Www.Raspberrypi.Com/Products/Raspberry-Pi-4-Model-B/

[5]. U. Farooq, M. Ul Hasan, M. Amar, A. Hanif, And M. Usman Asad, "Rfid Based Security And Access Control System," International Journal Of Engineering And Technology, Pp. 309–314, 2014.

[6]. Az-Delivery. (Accessed: 2024, Jul.) Rfid Kit Rc522 Mit Reader, Chip Und Card Für Raspberry Pi Und Co. (13,56mhz). Az-Delivery.De. [Online]. Available: Https://Www.Az-Delivery.De/Products/Rfid-Set

[7]. Makershop.De. (Accessed: 2024, Jul.) Tcrt5000 Reflektierende Ir Lichtschranke. Makershop.De. [Online]. Available: Https://Www.Makershop.De/Sensoren/Lichtsensor/Tcrt5000-Modul/

[8]. Adafruit. (Accessed: 2024, Jul.) Adafruit Ultimate Gps Breakout - 66 Channel W/10 Hz Updates - Pa1616s. Adafruit.Com. [Online]. Available: Https://Www.Adafruit.Com/Product/746

[9]. W. Ewald. (Accessed: 2024, Jul.) Sim800l Modul. Wolles-Elektronikkiste.De. [Online]. Available: Https://Wolles-Elektronikkiste.De/Sim800l-Modul

[10]. Eckstein Komponenten. (Accessed: 2024, Jul.) Lm2596s Dc-Dc Einstellbarer Step-Down Spannungsregler Mit Led-Voltmeter Adjustable Power Modul. Eckstein-Shop.De. [Online]. Available: Https://Eckstein-Shop.De/Lm2596sdc-Dceinstellbarerstep-Downspannungsreglermitled-Voltmeteradjustablepowermodul

[11]. Telegram. (Accessed: 2024, Jul.) Telegram. Telegram.Org. [Online]. Available: Https://Telegram.Org/

[12]. S. Kaya, E. Aşkar Ayyildiz, And M. Ayyildiz, "Smart Door Lock Design With Internet Of Things," International Journal Of 3d Printing Technologies And Digital Industry, Vol. 6, No. 2, Pp. 201–206, Aug. 2022.

[13]. Sunfounder. (Accessed: 2023, Nov.) Pipower - Raspberry Pi Ups With Battery. Sunfounder.Com. [Online]. Available: Https://Docs.Sunfounder.Com/Pro-Jects/Pipower-V2/En/Latest/Features.Html#About-Io-Pins

[14]. R. Shukla, D. K, And N. M, "Vehicle Theft Detection And Driver Identification System Using Iot," In 2022 International Conference On Power, Energy, Control And Transmission Systems (Icpects). Ieee, Dec. 2022.

[15]. F. Arat And S. Akleylek, "A Systematic Survey On Mobile Internet Of Things Security," In 2021 International Conference On Information Security And Cryptology (Iscturkey). Ieee, Dec. 2021.

[16]. Apple. (Accessed: 2024, Jul.) Airtag. Apple.Com. [Online]. Available: Https://Www.Apple.Com/De/Airtag/