JURNAL EMACS
*[Engineering, MAthematics and Computer Science]* Vol.5 No.1 January 2023: 1-6
e-ISSN: 2686-2573
DOI: 10.21512/emacsjournal.v5i1.9251

# IoT Based Vehicle Safety Controller Using Arduino

**Said Achmad[1*], Raditya Adinugroho[2], Nur Safii Hendrawan[3], Thomas Franklin[4]**

[1,2,3,4] Computer Science Department, School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480
said.achmad@binus.edu; raditya.adinugroho@binus.ac.id;
nur.hendrawan@binus.ac.id; thomas.franklin@binus.ac.id

*Correspondence: said.achmad@binus.edu

***Abstract –*** *Several people try to break into vehicles and steal vehicles left by their owners, sometimes even without the owner's knowledge. There are still various ways that can be done to a turn on the vehicle without the key from the vehicle so that the vehicle can be stolen easily. Due to the ease of break-in from some vehicles, several additional security implementations can be installed. One of these ways is to implement IoT and RFID. There are several implementations of IoT as an extra device for safety and tracking vehicles. RFID can be Implemented as an additional key or access. IoT and RFID can be combined to provide additional safety for vehicles and prevent vehicle theft. This research aims to propose a device that uses IoT technology and RFID to keep the vehicle safe and track the use of the vehicle. This research use severals IoT Components such as Arduino, RFID, and GPS module with a clear schema and architecture of implementation. The proposed device was tested under various conditions of RFID use for ensuring that the additional key is works to improve safety and testing also conducted on the level of accuracy of the GPS module used. The test results show that the proposed tool can work well for security and tracking needs.*

***Keywords:*** *IoT; RFID; GPS; Arduino; Android*

## I. INTRODUCTION

The Internet of Things (IoT) is often implemented in various fields around us. IoT can be seen in its implementation, facilitating daily medical, culinary, fitness, automotive, and even building facility (Widjaja et al., 2022). IoT is often used to provide remote access and control of a device (Kemala et al., 2022). Apart from the convenience it offers, IoT is also implemented for the safety of vehicles that are marketed worldwide, and its existence is vital for the convenience of owners (Desima et al., 2017).

Even though many rapid technological developments exist today, the safety of vehicles running on the highway is only sometimes safe (Maghanoy, 2017). Several people will try to break into vehicles and steal vehicles left by their owners, sometimes even without the owner's knowledge. There are still various ways that can be done to a turn on the vehicle without the key from the vehicle so that the vehicle can be stolen easily.

Due to the ease of break-in from some vehicles, several additional security implementations can be installed during vehicle design to prevent any crime from causing harm to potential owners. One of these ways is to implement IoT on our vehicles. In terms of security, IoT can be used as a tracking device (Datta et al., 2019) and an alternative way to open a vehicle without using the available keys. In addition, IoT can be programmed so that vehicle owners can access control of the vehicle remotely. Unfortunately, such features are not often found in vehicles currently marketed. Many studies have implemented IoT to increase the security of objects and locations (Lv et al., 2021). Research states that IoT already has many implementations in various fields, one of which is security. Several important buildings and companies have implemented IoT to access specific locations. There are also network systems that require IoT to be able to access the information contained in it (Mahmoud et al., 2015).

IoT technology is also widely implemented in CCTV cameras where recording and live view can be accessed via the internet so that the location where the camera is attached can remain safe. In addition, IoT is also available on devices in hospitals to facilitate data collection on essential tools and objects (Ikuesan et al., 2020).

There is also technology, namely RFID (Radio Frequency Identification), which is a technology that uses objects such as cards or tags to store data and can be read by a reader. Even though RFID is said to be commonly applied in various fields, including security, the data on the card can be retrieved without contact with the RFID card if it is not stored with an RFID blocker. Even with these weaknesses, RFID security is guaranteed on condition that the RFID card is stored wisely (Raman et al., 2020).

There are several implementations of IoT as an extra device for safety and tracking vehicle (Kaur et al., 2019). Implementation of RFID as an additional key or access (Nambiar, 2009). The combination of IoT and RFID which have been done in other papers (Costa et al., 2021). For example, one uses Arduino with RFID and Network modules to create an anti-theft system on motorized vehicles (Ikuesan et al., 2020). Another implementation is the use of Arduino Nano as well as the RFID module to assemble prototypes to increase the security of motorized vehicles with a double lock system, making vehicles need two keys to open and start the engine (Wijenayaka & Wedasinghe, 2018).

One of the research on IoT was carried out by (Husni et al., 2021) implementing IoT using Arduino hardware on vehicles to create an anti-theft system that contains alarms, device data logs, and vehicle tracking. The system created has several modes. The first mode is the normal mode, where the motor can operate normally. Then the second mode is the anti-theft mode, where the electric current is cut off and will sound when vibration is felt, or there is movement in the motor. In addition, other research to secure vehicles was also carried out by (Muslem, 2020) by adding an RFID module as a double key or additional key to start the vehicle. Research conducted by (Muslem, 2020) utilizing RFID can be developed with research inspired by (Harish et al., 2021). The use of RFID can be expanded using master and slave keys. Master key, which is the highest authority, can add and remove Slave Keys. Slave Key is valid for starting the vehicle when it has been added as a key to the device. Then an application can be designed that is used to monitor the time when the vehicle starts and stops along with the user's identity based on the data in the RFID key.

This research aims to deal with problems in vehicle security by utilizing the latest technology such as IoT and RFID. This research will implement IoT into the vehicle and make the vehicle accessible using an E-KTP (Andriansyah et al., 2017) card or an RFID card that can be placed in a hidden location. Apart from that, the IoT device can also control and send vehicle locations to Android applications.

## II. METHODS

In this research, the method used is an experimental approach  where the design of the Arduino motor model is carried out based on the identified problems and specified requirements. The developmet stage in this research can be seen in figure 1. The steps is including gathering device component, assemnly and alsotesting to check whether the design results meet the applicable requirements and can work properly. In this research, the tests included testing the RFID sensor system, GPS tracking, and DC vehicle. First, the RFID sensor is tested in the accuracy of reading the E-KTP sensor, which will be used to turn on the motor current. Furthermore, GPS testing is carried out in the form of the accuracy of the coordinate values that are read to determine the distance of the tool's displacement. The next test is testing the DC vehicle to determine whether the E-KTP system is legible.

In the first stage, the thing to do is start looking for ideas, then identify the problems that exist in several sources that have been searched. This identification is in the form of the number of motorbikes stolen, and minors can bring motorbikes. For this reason, this RFID sensor helps prevent theft, and only users who have an E-KTP can use the motorbike.

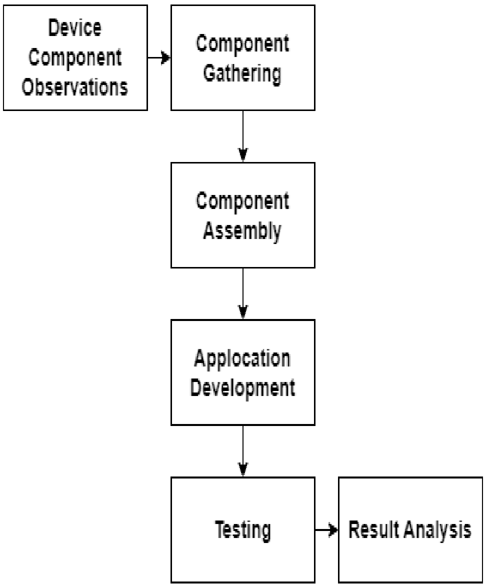

**Figure 1.** Development Phase

Then the second stage is selecting components such as ARDUINO, RFID, GPS, Bluetooth, BUZZER, LED, and CABLE. After the selection/purchase of components is complete, the next stage is the components assembly. The commponents assebly is a stage to assemble all the components into one device. Figure 4 and Figure 5 is the architecture components of proposed device. Table I and Table II is the detail of components that are used in this research.

The next stage is Application Development. At this stage, the apps used are the MIT APPS INVENTOR apps (the platform for making these apps). If you have passed the test phase and the results are functional, continue with the data analysis stage. At this stage, you will test the Bluetooth connection to Android, the accuracy of the GPS, the detection of the E-KTP that has been registered.

For this project use case is used As seen in Figure 2, for Arduino device usage, the user can register the card as the main card, allowing additional cards to be used to start the machine. Besides that, the user can add a card as a key to start the machine and, after that, use it to turn on or turn off the machine. In the Android Application, the user can initiate a connection with the Arduino device via Bluetooth, turn on or turn off the vehicle, and search for the location of the Arduino device. The method we report is an app-based digital motor controller using Arduino. Later on, our device can activate automatic vehicle contacts by scanning using NFC and tracking coordinates using GPS, which can be connected to Android using Bluetooth. Figure 3 is the flow chart of device for the Arduino devices used. This research serves to improve the motor vehicle security system.

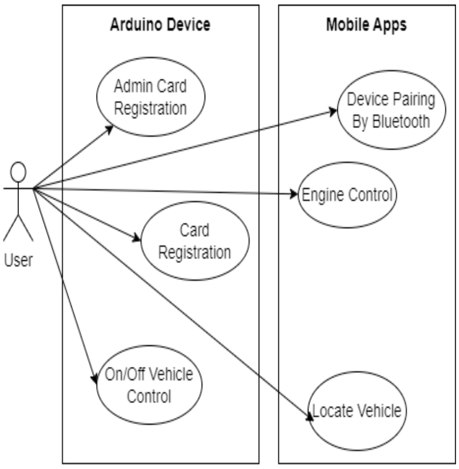

**Figure 2.** Use Case Diagram

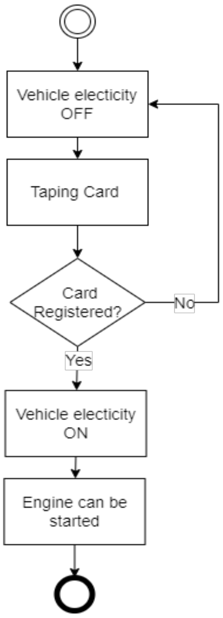

**Figure 3.** Flow Chart Diagram

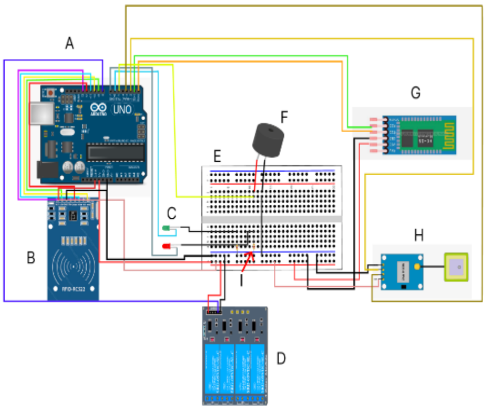

**Figure 4.** Device Architecture

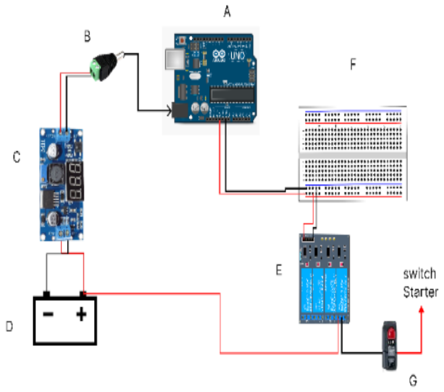

**Figure 5.** Device to Vehicle Architecture

**Table I.** Device Architecture Detail

| Symbol | Component |
|---|---|
| A | Arduino UNO R3 |
| B | RFID RC522 |
| C | Led Green & Red |
| D | Rellay 4 channel 5V DC |
| E | Mini Breadboard 400 titik |
| F | Buzzer 5V |
| G | Bluetooth HC-05 |
| H | GPS NEO 6M ublox NEO-6M -V2 |
| I | Resistor 10k 1/4watt |

**Table II.** Device to Vehicle Architecture Detail

| Symbol | Component |
|---|---|
| A | Arduino UNO R3 |
| B | Power Suplly Connector |
| C | Step Down Arduino |
| D | Vehicle Battery |
| E | Rellay 4 channel 5V DC |
| F | BreadBoard |
| G | Button Start |

This application is made through the MIT App Inventor 2 WEB application, which is designed to create Arduino applications. Here is the application interface developed can be seen in Figure 6. When the device and Android are activated, there will be a pairing mode to connect Bluetooth and Android devices. When it has paired, the Bluetooth status condition will turn green. When the device is paired and connected, the motor status will change to ON for active relay conditions if the user triggers the NFC scanner device using a registered card. Users can activate the motor using a starter and OFF if the user wants to turn off the relay current. The next button is the tracker button using the Neo Blox 6m device, which will send a coordinate link for the device that has been installed on the motor. When the tracker button is triggered, it will send to the link page and open the google maps application as seen on figure 7. After completion, continue testing/testing. If the tool responds well or functions appropriately.

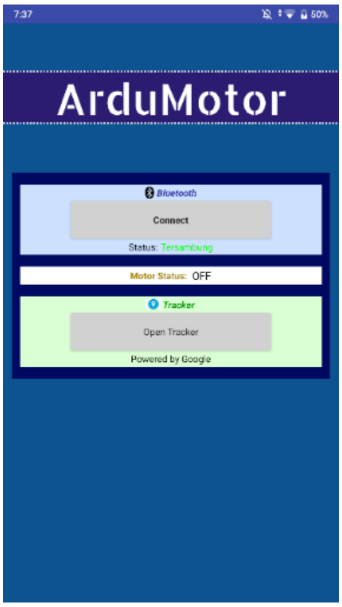

**Figure 6.** Application Interface

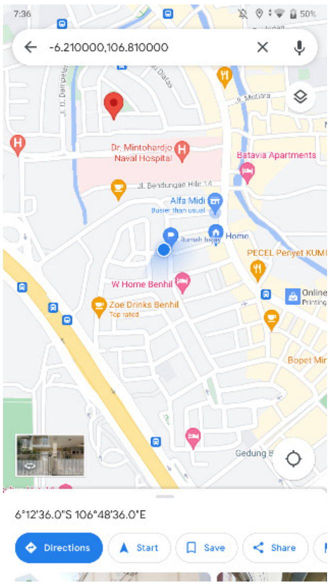

**Figure 7.** Cordinate Interface

## III. RESULTS AND DISCUSSION

Evaluations have been carried out to see if the results of the tool's performance are as expected. Tests were carried out in several places to bring up the results of different responses, which could then be analyzed and concluded through the average results obtained. Test results are divided into two: the results for testing tools as safety control and the results of application connection and GPS testing.

Evaluation for testing tools as safety control has been conducted to evaluate is the tools works correctly on every state when users access the vehicle. Table III shows the card access registration state. Based on Table III, it can be seen that the device can work according to the expected target. First, users can use the admin card as a key to enter GetID mode, and then users can register other cards that are used as access. Lastly, users can use the admin card again to exit GetID mode. When GetID mode is active, GetID Mode is the Mode for registering Card IDs to be registered to Arduino memory. Table III shows that a card that has not been registered can be registered in GetID mode, and the registration can also be withdrawn. Table IV shows the card access used and the result as response of device. Table 4 is the default mode where the device validates access to provide voltage current to the relay.

**Table III.** Card Registration State

| Card Access | Relay State | Buzzer | Result |
|---|---|---|---|
| Admin card (Registered) | Off | On repetitif | Enter GetID Mode |
| E-KTP (Unregistered) | Off | 3 times rapidly | Card Registered |
| Other NFC Card (Unregistered) | Off | 3 times rapidly | Card Registered |
| E-KTP (Registered) | Off | 3 times long | Card Registration Withdrawal |
| Admin card (Registered) | Off | Off | Exit from GetID Mode |

From the access card evaluation, it can be seen that the access security validation is working correctly. Registration for a new card requires an already registered admin card, which will provide exit access into GetID Mode. After that, the card that has been registered can activate the relay or provide voltage to start the vehicle.

**Table IV.** Vehicle Access State

| Card Access | Relay State | Buzzer | **Result** |
|---|---|---|---|
| E-KTP (Registered) | Off | 2 times rapidly | Recognize access and turn relay on |
| NFC Card (Registered) | Off | 2 times rapidly | Recognize access and turn relay on |
| NFC (Unregistered) | Off | 1 times long | Access denied and relay stay off |
| E-KTP (Registered) | On | 2 times rapidly | Recognize access and turn relay off |
| NFC Card (Registered) | On | 2 times rapidly | Recognize access and turn relay off |
| NFC (Unregistered) | On | 1 times long | Access denied and turn relay off |

The next test tests device connectivity with the Android application via Bluetooth. The evaluation was conducted to test the ease with which the device can be connected to our mobile device via Bluetooth. The results of the evaluation of Bluetooth connectivity can be seen in Table V. From the result on Table V it can be seen that the bluetooth has a limitation in range out of 15 m.

**Table V.** Bluetooth Connectivity Result

| Schenario | Distance | Result |
|---|---|---|
| Indoor without barrier | 10 cm | Bluetooth Connected |
| Indoor without barrier | 1 m | Bluetooth Connected |
| Indoor without barrier | 5 m | Bluetooth Connected |
| Indoor with barrier | 10 m | Bluetooth Connected |
| Outdoor with barrier | 15 m | Failed to Connect |

Lastly, testing the GPS coordinate points is conducted to test the accuracy of the coordinates generated by the sensor device compared to the coordinates generated by the mobile device using Google Maps. Testing is carried out by activating the device and mobile device at the same location point and comparing the coordinates generated by the two devices. The coordinate point of the mobile device is used as the primary reference, then the distance is calculated between the mobile device coordinate point and the proposed device coordinate point. The test results can be seen in Table VI. The testing result shows a difference in the distance between the points produced by the two tools and the proposed device has accuracy in range of 15m.

**Table VI.** GPS Test Result

| Proposed Device | Mobile Device | Result |
|---|---|---|
| -6.212631, 106.811203 | -6.212703, 106.811203 | 9m |
| -6.212631, 106.811210 | -6.212703, 106.811203 | 9m |
| -6.212606, 106.811271 | -6.212703, 106.811203 | 11m |
| -6.212586, 106.811187 | -6.212703, 106.811203 | 14m |
| -6.212576, 106.811195 | -6.212703, 106.811203 | 15m |

## IV. CONCLUSION

Various evaluations have been carried out to test the device proposed in this study and the proposed device can be considered successful in carrying out its functions properly. The experiment was carried out starting from the condition when registering access, the condition for using access, the condition of device connectivity with the mobile device, and the accuracy of the coordinate points generated by the device. The test results found no failures under various conditions. The device can be connected to the mobile application via Bluetooth so that security and tracking of vehicles can be carried out. For future research, it is recommended to implement large vehicles or heavy equipment and conduct trials with a more accurate GPS sensor.

## REFERENCES

Andriansyah, M., Subali, M., Purwanto, I., Irianto, S. A., & Pramono, R. A. (2017). E-KTP as the basis of home security system using arduino UNO. *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 1–5.

Costa, F., Genovesi, S., Borgese, M., Michel, A., Dicandia, F. A., & Manara, G. (2021). A review of RFID sensors, the new frontier of internet of things. *Sensors*, *21*(9), 3138.

Datta, N., Malik, A., Agarwal, M., & Jhunjhunwala, A. (2019). Real time tracking and alert system for laptop through implementation of GPS, GSM, motion sensor and cloud services for antitheft purposes. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1–6.

Desima, M. A., Ramli, P., Ramdani, D. F., & Rahman, S. (2017). Alarm system to detect the location of IOT-based public vehicle accidents. *2017 International Conference on Computing, Engineering, and Design (ICCED)*, 1–5.

Harish, V., Chrisvin, D. S., & Thottungal, R. (2021). Overview of RFID Security and its Applications. *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, 1–5.

Husni, M., Ginardi, R. V. H., Gozali, K., Rahman, R., Indrawanti, A. S., & Senoaji, M. I. (2021). Mobile Security Vehicle's based on Internet of Things. *Journal of Robotics and Control (JRC)*, *2*(6), 546–551.

Ikuesan, R. A., Ganiyu, S. O., Majigi, M. U., Opaluwa, Y. D., & Venter, H. S. (2020). Practical Approach to Urban Crime Prevention in Developing Nations. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1–8.

Kaur, P., Das, A., Borah, M. P., & Dey, S. (2019). Smart vehicle system using arduino. *ADBU Journal of Electrical and Electronics Engineering (AJEEE)*, *3*(1), 20–25.

Kemala, A. P., Syahputra, M. E., Lucky, H., & Achmad, S. (2022). Pengembangan Smart Air Condition Control Menggunakan Platform Blynk Berbasis Mikrokontroler ESP8266 dan Sensor DHT11. *Engineering, MAthematics and Computer Science (EMACS) Journal*, *4*(1), 19–23.

Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT security for smart cities. *ACM Transactions on Internet Technology*, *21*(4), 1–21.

Maghanoy, J. A. W. (2017). Crime mapping report mobile application using GIS. *2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP)*, 247–251.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341.

Muslem, I. (2020). Prototype Kunci RFID (Radio Frequency Identification) dalam Meningkatkan Keamanan Kendaraan Bermotor. *Jurnal TIKA*, *5*(3), 70–76.

Nambiar, A. N. (2009). RFID technology: A review of its applications. *Proceedings of the World Congress on Engineering and Computer Science*, *2*, 20–22.

Raman, D. R., Devi, S. G., & Saravanan, D. (2020). Locality based violation vigilant system using mobile application. *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, 1–6.

Widjaja, D., Octaviandra, M. F. D., Achmad, S., & Sutoyo, R. (2022). Important Security Factors for Implementing Internet of Things in Smart Home Systems. *2022 International Conference on Informatics Electrical and Electronics (ICIEE)*, 1–7.

Wijenayaka, L. C., & Wedasinghe, N. (2018). *Emergency Alert System for Reporting Crime Issues to Nearest Police Station*.