INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

Electronic Driving License-based for Secure Sharing Vehicles in Wireless IoT Networks

Received:
11 August 2023
Accepted:
20 January 2024
Published:
1 February 2024

[1]Aad Hariyadi, [2]Amalia, [3]Rieke Adriati Wijayanti,
[4*]Amalia Eka Rakhmania, [5]Nurul Hidayati, [6]Hudiono
[1-6]Electrical Engineering, Politeknik Negeri Malang
E-mail: [1]aad.hariyadi@polinema.ac.id, [2]amaliahwang@gmail.com,
[3]riekeaw@polinema.ac.id, [4]amaliaeka.rakhmania@polinema.ac.id,
[5]nurulhid8@polinema.ac.id, [6]hudiono@polinema.ac.id
*Corresponding Author

Abstract—In this paper we study electronic driving license (EDL) for secure sharing of vehicles in wireless IoT networks. The process of authentication and data transmission to the server is a very challenging problem to solve. To solve this problem, we propose the use of a wireless IoT network to overcome the transmission speed from the vehicle to the server, and the use of EDL for the driver authentication process. Two devices are installed on the vehicle side and on the server side while the wireless IoT network is used to make data transmission efficient. EDL is used to authenticate drivers who rent vehicles. When the device authentication process on the vehicle will send geographic information obtained through the global positioning system (GPS) to the server. The server will verify the user, if it matches then the server will send a command to the vehicle to be used. To run the considered system, we proposed Algorithm 1 and 2 to run the vehicle device and server, respectively. Experiment result shows the proposed system has maximum accuracy in 95.5%, packet delivery ratio 90%, delay propagation less than 60 seconds. Thus, the security of the shared vehicle will be increases.

Keywords— Authentication; Electronic Driving License; Internet of Things (IoT); Security; Vehicle

Corresponding Author:

Amalia Eka Rakhmania,
Electrical Engineering,
Politeknik Negeri Malang,
Email: amaliaeka.rakhmania@polinema.ac.id
ID Orcid: http://orcid.org/0000-0002-6996-8496

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

I. INTRODUCTION

The growth of sharing vehicles at this time has increased the mobility of people who will travel. However, monitoring registered or unregistered users who drive these vehicles is not easy. Currently, the security of sharing vehicles only uses keys and sensors on the car body. The author in [1] studied the security issue to reduce the occurrence of car theft by using the Internet of Things (IoT) to detect if the lights on the car have not been turned off and the car windows have not been closed; this system is in the form of a mobile application. Meanwhile, at a car rental place, the security system only provides identity as a guarantee, which still causes cases of car theft. In addition, the author in [2] worked on the electronic identification (e-ID) card that can be used as RFID-based car security. The electronic driving license (EDL), which has the same components and characteristics as the e-ID card, can be innovated by replacing e-ID[3].

The Internet of Things (IoT) is a concept that aims to expand the benefits of continuously connected internet connectivity [4]–[7]. Several authors implemented IoT in vehicle security systems. Authors in [8] introduced an innovative automobile security system centered on government-issued driving licenses and biometric verification. While it enhances vehicle safety and prevents unauthorized usage through advanced technology, potential concerns include privacy issues and technological vulnerabilities. [9] examined the shift from vehicular ad hoc networks to the Internet of Vehicles (IoV) and its impending evolution into the Internet of Autonomous Vehicles (IoAV). The IoAV aims for secure communication between vehicles and roadside units for autonomous driving. The article offers insights into autonomous vehicle communication, associated properties, security, and outlines future research directions. Authors in [10]–[14] collectively underscore the thematic resonance of leveraging technology for fortifying vehicular security, manifesting as anti-theft modalities, remote surveillance, and incident anticipation, all while cognizant of prospective exigencies and complexities inherent to the actualization of such systems. noted

The vehicle security system in this IoT-based sharing vehicle has two variables that increase car security. EDL is an identity card that all vehicle users own as proof that the person is fit to drive [15]. The EDL used is the driving license that was just released in 2019 (Indonesia case). This EDL is used in the car security system as a condition for sharing vehicles. Besides that, to ensure the customer's driving eligibility, the EDL must be registered with the EDL-detecting device to start the car. This EDL has a chip that can be read in the Near Field Communication (NFC) Reader to read the ID number [16]. The NFC is a short-range wireless connectivity technology that allows two-way interaction between electronic devices that is safer and simpler [17]. Moreover, the authors in [18] studied the clustering protocol to improve stability in the IoT

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

devices. The speed and cosine similarity were proposed to guarantee vehicle safety provides intelligent traffic management for high-speed data communication and vehicle entertainment. Furthermore, the Leach algorithm was proposed to improve energy efficiency in the wireless sensor network devices to support high mobility IoT networks [19]. While the authors in [20] worked in scanning method to detect jig for the smart learning factory in IoT networks. The EDL will be tapped on the NFC Reader located in the toolbox, where the NFC Reader will send EDL data to the microcontroller and transfer data using a transceiver which will be sent to the server [21]. The web server is used for the registration of rental owners as admins and rental tenants as users. The data on the web server will be stored in the database. However, the aforementioned did not consider the EDL to driver authentication.

The main contribution of the paper lies in the proposal of an electronic driving license-based system aimed at optimizing the monitoring and enhancement of vehicle-sharing protection. Specifically, the approach suggests the utilization of an electronic driving license for authentication within vehicle-sharing scenarios. Through this authentication mechanism, vehicles can be efficiently initiated, automatically recognized, and their last known location transmitted to the server. The experimental findings underscore the efficacy of the proposed system, showcasing notable accuracy levels and minimal delays, thus effectively bolstering security measures within the realm of shared vehicle usage.

II. RESEARCH METHOD

We consider a shared vehicle security system based on the Internet of things (IoT) with an electronic driving license (EDL), where each vehicle will be installed with a device connected to a server via the Internet, as shown in Figure 1. As we can see in Figure 1, there are two main blocks in the proposed system model. The first block is in the car side including NFC tag used to user identification, NFC reader used to read the NFC tag, microcontroller used as brain in the car side, relay and car status as output of the microcontroller, also microcontroller can communicate with server by using transceiver which can connect with internet. For server side consists of authentication, it is used to prove user ID and the databased, databased used for storing the user data and the last is web display to show all information about this system.

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

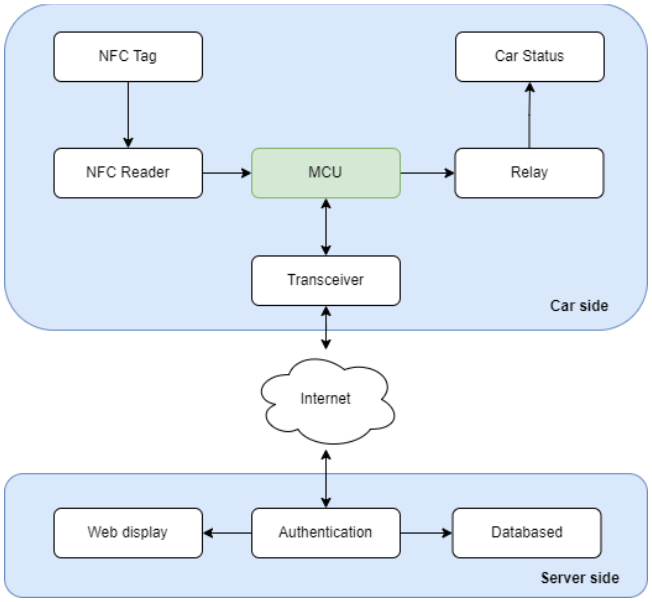


Fig 1. Proposed System Model of EDL for Secure Sharing Vehicle.

We also consider using EDL as a driver authentication, NFC reader functions as an EDL detector, and microcontroller functions as an information processing unit that is read from the EDL and controlled on the vehicle. In addition, there is a global positioning system (GPS) that functions as a vehicle's location detector. At the same time, the server functions as a database and vehicle status information system. We consider internet network connection by utilizing cellular network connection. The schematic diagram proposed to protect the sharing vehicle is illustrated in Figure 2.

As we can see in Figure 2, the hardware design's main goal is to send the readings from the EDL and the latest location to the server and control whether the car can be turned on or not. With input readings from GPS as a source of geographic location information and NFC reader as a source of information from reading EDL. As we can see in Figure 2, the first device connected to Arduino is the PN532 NFC Module. In the NFC Reader PN532, the pins used are for I2C serial communication. In I2C communication, the pins used are serial clock (SCL) and serial data (SDA). SCL is connected to pin 21 on the Arduino, which has the function of providing clock pulses for data transmission intervals, while the SDA pin is connected to pin 20 on the Arduino, which has the function of loading data to be sent between the two devices. Each time the clock pulse changes from low to high, some information containing the device address and a data request is sent from the Arduino via the SDA line I2C. When the clock pin changes from high to low, the previously requested data reply will be sent via the same Arduino I2C line. NFC Reader has an operating frequency of 13.56 MHz. On oled also use SCL, which is connected to pin 21 and SDA, which is connected to pin 20 [22].

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

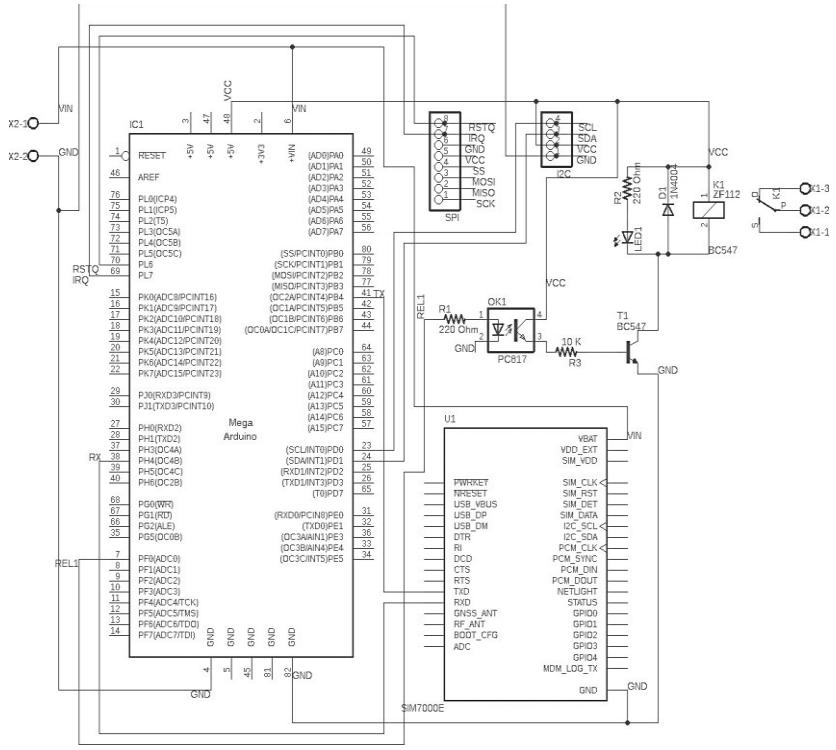


Fig 2. The Proposed Schematic Diagram for Vehicle Device.

The next component is the SIM7000E transceiver is a module that functions for data communication with the server. The program can control the TX and RX operation, TX is connected to pin 10 Arduino Mega, and Rx is connected to pin 7 Arduino Mega. The transceiver is equipped with a GPS module and has a socket for an internet card. The operating voltage for the transceiver is 7-12V, so it also gets input voltage from the accumulator. While the function of the relay is to disconnect and connect the electrical lines regulated by Arduino, which means the vehicle can be used or not. The relay input pin is connected to pin A0 on the Arduino. All devices on this vehicle require a power supply; thus, the device must be connected to the vehicle battery.

To run the proposed system model, we propose Algorithm 1 for the vehicle device and Algorithm 2 for the server.

Algorithm 1 The proposed EDL-based secure sharing vehicle (vehicle device)

Output: relay
Initialization
    Device on
1: While EDL = 1 do
2: Vehicle device read GPS
3: Send data from GPS and EDL to server
4: If received data from server
5: Data = 1 → vehicle ON
6: Data = 0 → vehicle OFF
7: end if
8: end while

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

Algorithm 2 The proposed EDL-based secure sharing vehicle (server)

Output: display
Initialization
    Server on
1: While received data from vehicle do
2: Verification data from vehicle
3: Send verification data to vehicle devices
4: Record verification results in databased and show into display
5: end while

The proposed electronic-driving license-based system's performance in enhancing secure vehicle sharing within wireless IoT networks is assessed through specific performance metrics. These metrics encompass the packet delivery ratio (PDR), which gauges the proportion of received data packets at the server compared to those transmitted; the delay, which quantifies the average latency experienced from data packet transmission by a vehicle to its receipt by the server; and the packet loss ratio (PLR), a measure of lost data packets relative to the total dispatched by the vehicle.

III. RESULT AND DISCUSSION

The experimental results show the system's performance in improving the security of sharing vehicles. We consider using a vehicle with an SUV type with the equipment used, as shown in Table 1.

Table 1 The Type of Devices

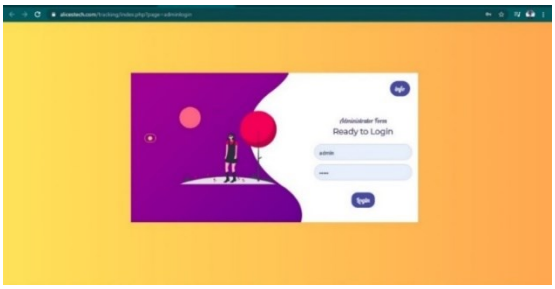
Devices	Type
Microcontroller	Arduino Mega 2560
Transceiver	SIM7000E
NFC Reader	PN532
NFC tag	Electronic driving license
Display	OLED

We tested the proposed system in the province of East Java, Indonesia. The device on the vehicle that has been implemented is shown in Figure 3.

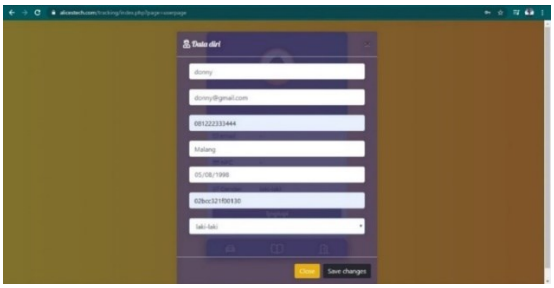
INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

Fig 3. Vehicle Device Implementation

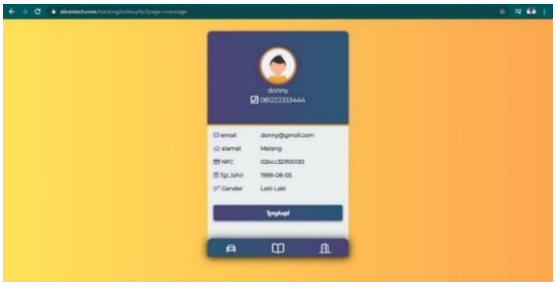
As we can see in Figure 3, user must tap the EDL in the smart sim card part in the left-hand side. After that, in the right-hand side will show the information about the EDL and prove to rent or not. While the server-side implementation can be shown in Figure 4(a). (b) and (c). In Figure 4(a) shows the implementation of the home page. Whereas Figure 4(b) shows implementation of the register page. And for implementation of profile page can be shown in Figure 4(c).



(a) Home page



(b) Register page



(c) Profile page

Fig 4. Implementation of The Home, Register and Profile Page

Besides that, the location of the vehicle in real-time will be displayed on the information system on the server side. An information system displays the vehicle's location, as shown in Figure 5.

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

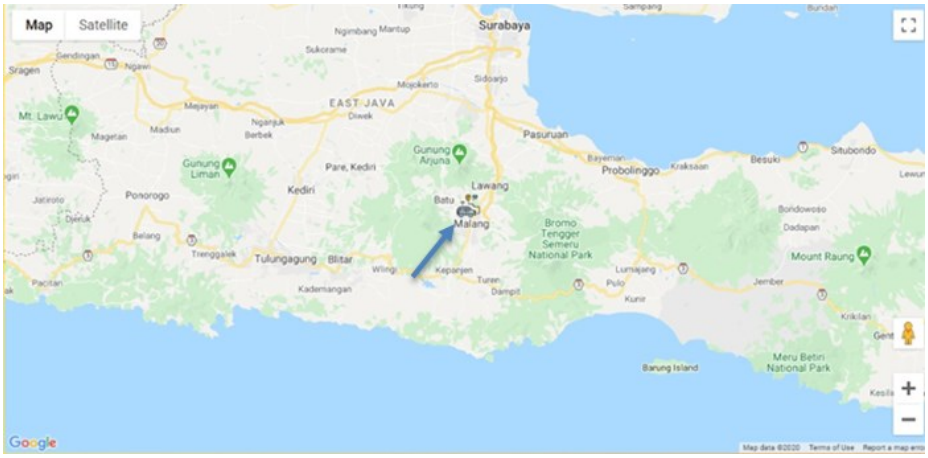


Fig 5. Location Vehicle on Information System

We tested the location accuracy on the device that had been made by comparing it with a GPS tracker as a reference. The device deviation value with the GPS tracker can be [23] expressed as

$$dev = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{1}$$

where x_1, y_1, x_2 and y_2 are denoted as reference latitude, reference longitude, Latitude GPS tracker, and longitude GPS tracker, respectively. The results of the device location accuracy test are shown in Table 2.

Table 2. Location Measurement

No	GPS Tracker		Device		Deviation (m)
	Latitude	Longitude	Latitude	Longitude	
1	-7.946	112.619	-7.946	112.619	2,9
2	-7.946	112.619	-7.946	112.619	3
3	-7,946	112,619	-7,946	112,619	8
4	-7,945	112,616	-7,945	112,616	3
5	-7,945	112,616	-7,945	112,616	8

As we can see in Table 2, the accuracy of the device's maximum deviation value obtained is 8 meters, it means the accuracy of the location measurement has 95.2% of accuracy. The reason is that the difference in sensitivity in capturing signals from satellites between the GPS tracker and the proposed device. Figure 6, 7, 8 and 9, we test performance is average from 100 samples from the system considered. In Figure 6, we analyze the delay as the function of speed.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

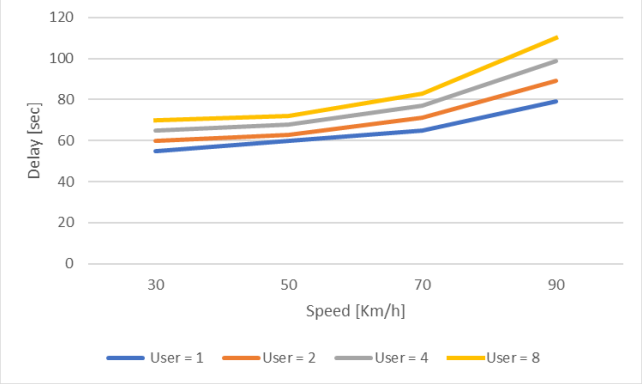


Fig 6. Delay as a Function of Speed

As we can see in figure 6, when the speed increases from 30 to 90, the delay will increase. The reason is that when the speed increases, the transmission from the mobile node to the base station changes the channel characteristic, so the signal quality will be changed [24]. Besides, when the number of vehicles increases from 1 to 8, the delay increases. One of the reasons is when the number of vehicles is larger, the server complexity increases [24]–[27].

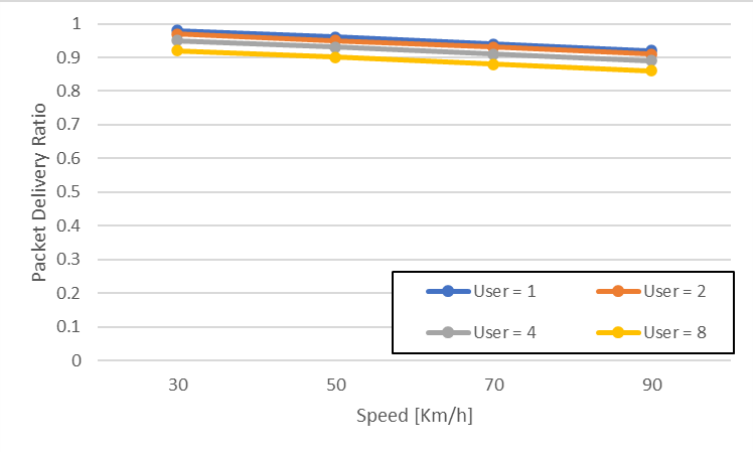


Fig 7. PDR as a Function of Speed

Figure 7 reveals the average packet delivery ratio on the variation of speed. As can be observed when the speed increases, the packet delivery ratio is decreased. The reason is when the vehicle mode faster, the networks become more unstable [28], [29]. Moreover, when the number of vehicles increases, the packet delivery ratio decreases. One of the reasons is when the number of vehicles is larger, the bandwidth in each vehicle decreases.

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

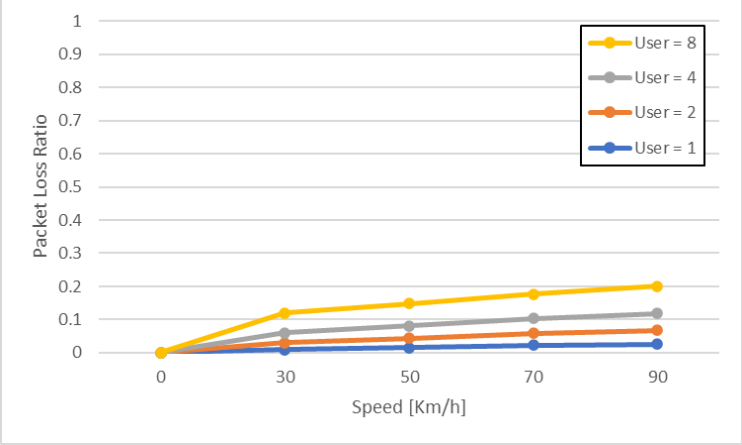


Figure 8. PLR as a Function of Speed

Figure 8 shows the effect of speed on the packet loss ratio. As can be seen in Figure 8, when the speed increases, the packet loss ratio increases. The reason is when the vehicle speed increases, the networks become unstable, and it make server did not received the data. Again, when the number of vehicles increases, the packet loss ratio increases due to the bandwidth in each vehicle decreases [30]. Figure 9 represents the effect of speed on the number of packet loss. As can be observed, when the speed increases, the total number of packet loss increases. Again, one of the reasons is when the speed increases, it makes the networks become unstable. Also when the number of vehicle increases, the total number of packet loss increases due to the bandwidth of each user decreases.

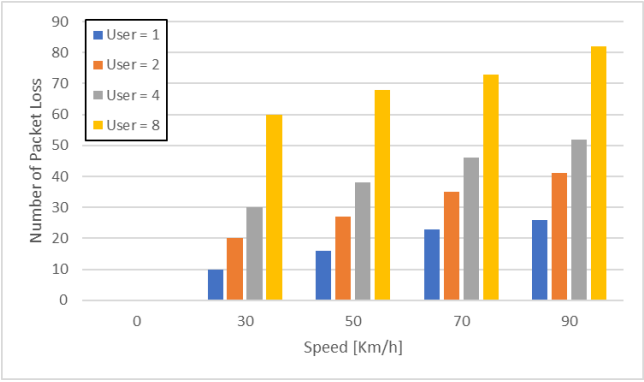


Fig 9. PDR as a Function of Speed

INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

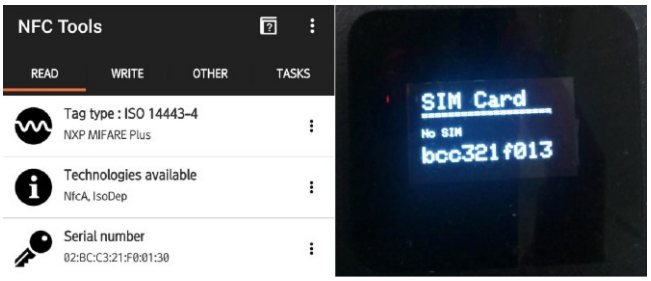


Fig 10. Verification of Electric Driving License.

Figure 10 illustrates the verification of an electric driving license in the system. As we can see in figure 10, the EDL serial number is the same as the serial number driver registered in the system. When the system is verified, the vehicle can be turned on. The vehicle cannot be turned on if the system is not verified. When the system is verified with the EDL, the device in the car will show as Figure 11.

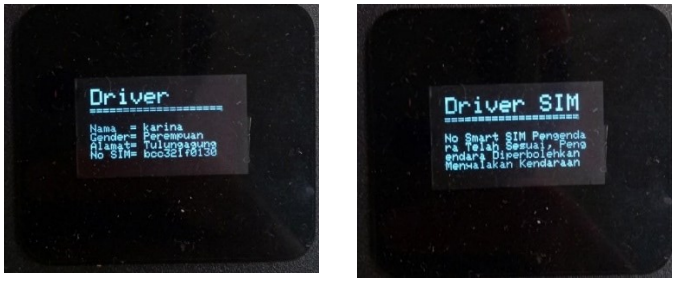


Fig 11. Approval of Electric Driving License

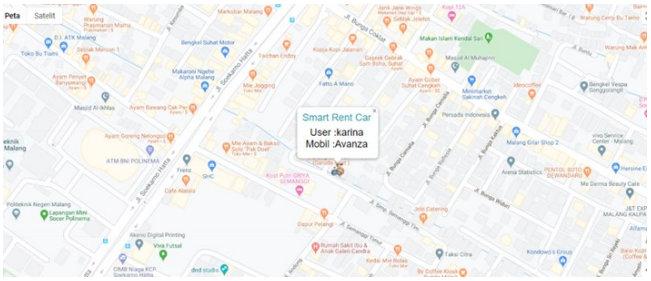


Fig 12. Location of Car Sharing

Figure 12 shows the location of car sharing in the website. As we can see in Figure 12, the location of the car and the user who is renting the car show on the map. Thus, the officer can monitor the location of the car in real-time.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

IV. CONCLUSION

We studied the electronic driving license-based for secure sharing vehicles in wireless IoT networks. The authentication and data transmission problem were considered. To tackle this problem, we proposed the use of a wireless IoT network to enhance transmission speed from vehicle to the server, coupled with EDL for driver authentication. Two devices were installed on both the vehicles and servers' side, employing the wireless IoT network for efficient data transmission. By using the node device, the sharing vehicle parameter was measured. The server side will record all parameters transmitted from the node device. By using an electronic driving license, the system can verify the driver, consequently improving the security of sharing vehicles. The experiment results verified that the suggested system had high accuracy with maximum 95.2 % accuracy, high packet delivery ratio 90% and lower delay propagation less than 60 seconds.

Author Contributions: *Aad Hariyadi*: Conceptualization, Methodology, Writing - Original Draft, Writing - Review & Editing, Supervision. *Amalia*: Software, Investigation, Data Curation, Writing - Original Draft. *Rieke Adriati Wijayanti*: Investigation, Data Curation. *Amalia Eka Rakhmania*: Investigation, Data Curation. *Nurul Hidayati*: Investigation, Data Curation. *Hudiono*: Software, Investigation.

All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Applied Research 2022 Program grant founded by State Polytechnic of Malang (SP DIPA-023.18.2.677606/2022). Aad Hariyadi is the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Data Availability: The data cannot be openly shared for the protection of study participant privacy.

Informed Consent: There were no human subjects.

Animal Subjects: There were no animal subjects.

ORCID:
Aad Hariyadi: http://orcid.org/0009-0000-8770-266X
Amalia: http://orcid.org/0009-0005-9828-5431
Rieke Adriati Wijayanti: http://orcid.org/0009-0007-9400-1432
Amalia Eka Rakhmania: http://orcid.org/0000-0002-6996-8496
Nurul Hidayati: http://orcid.org/0000-0002-6190-5722
Hudiono: http://orcid.org/0009-0001-1448-2501

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

REFERENCES

[1] S. Gnanapriya, M. Sowmiya, S. Priyadarshini, R. R. Priya, and R. Saranya, "An IoT based Anti Theft Detection and Notification System for Two Wheelers," SSRN Electron. J., 2022, doi: 10.2139/ssrn.4109161.

[2] E. P. C., A. P.N., J. L., and A. T. A., "Anti-Theft System for Car Security using RFID," Int. J. Sci. Manag. Stud., no. September, pp. 14–21, 2018, doi: 10.51386/25815946/ijsms-v1i4p103.

[3] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, K. Jambi, and M. Alrasheedi, "A novel and secure smart parking management system (SPMS) based on integration of WSN, RFID, and IoT," in 2018 15th Learning and Technology Conference, L and T 2018, 2018, pp. 102–106, doi: 10.1109/LT.2018.8368492.

[4] W. Puspitasari and H. Y. R. Perdana, "Real-time monitoring and automated control of greenhouse using wireless sensor network: Design and implementation," 2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018, pp. 362–366, 2018, doi: 10.1109/ISRITI.2018.8864377.

[5] M. Taufik, H. Hudiono, A. E. Rakhmania, R. H. Y. Perdana, and A. S. Sari, "An Internet of Things Based Intercity Bus Management System for Smart City," Int. J. Comput. Digit. Syst., vol. 10, no. 1, pp. 1219–1226, Nov. 2021, doi: 10.12785/ijcds/1001109.

[6] M. Z. Chowdhury, S. Ahmed, and Y. M. I. N. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," IEEE Netw., vol. 1, no. July, pp. 957–975, 2020.

[7] R. H. Y. Perdana, Hudiono, M. Taufik, A. E. Rakhmania, R. M. Akbar, and Z. Arifin, "Hospital queue control system using Quick Response Code (QR Code) as verification of patient's arrival," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 8, 2019, doi: 10.14569/IJACSA.2019.0100847.

[8] S. Agrawal, S. Bhardwaj, R. Tyagi, and V. Rastogi, "Vehicle Safety System Using Fingerprint Scanner and Driving License Data," in ICRAME 2020: Recent Advances in Mechanical Engineering, 2021, pp. 591–606.

[9] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," IEEE Wirel. Commun., vol. 26, no. 4, pp. 60–65, Aug. 2019, doi: 10.1109/MWC.2019.1800503.

[10] K. Thamoethata, B. Isong, N. Dladlu, and A. M. Abu-Mahfouz, "Analysis of IoT-based Vehicle Anti-Theft Security," in 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Nov. 2021, pp. 1–6, doi: 10.1109/IMITEC52926.2021.9714660.

[11] A. Aranganathan, G. T, S. P. R, V. Vedanarayanan, S. Sivasundarapandian, and R. E, "Centralized control system employing Node MCU and IoT for finding the vehicle in the event of an accident, theft, or alcohol overdose," in 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Apr. 2023, pp. 1–7, doi: 10.1109/ICONSTEM56934.2023.10142916.

[12] T. Thamaraimanalan, M. Mohankumar, S. Dhanasekaran, and H. Anandakumar, "Experimental analysis of intelligent vehicle monitoring system using Internet of Things (IoT)," EAI Endorsed Trans. Energy Web, p. 169336, Jul. 2018, doi: 10.4108/eai.16-4-2021.169336.

[13] M. M. Rana, "IoT-Based Electric Vehicle State Estimation and Control Algorithms Under Cyber Attacks," IEEE Internet Things J., vol. 7, no. 2, pp. 874–881, Feb. 2020, doi: 10.1109/JIOT.2019.2946093.

[14] I. Indrianto, M. N. I. Susanti, R. R. A. Siregar, P. P. J., and Y. Purwanto, "Smart taxi security system design with internet of things (IoT)," TELKOMNIKA

(Telecommunication Comput. Electron. Control., vol. 17, no. 3, p. 1250, Jun. 2019, doi: 10.12928/telkomnika.v17i3.10167.

[15] Hudiono, M. Taufik, R. H. Y. Perdana, and A. E. Rakhmania, "Digital centralized water meter using 433 mhz lora," Bull. Electr. Eng. Informatics, vol. 10, no. 4, pp. 2062–2071, 2021, doi: 10.11591/eei.v10i4.2950.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[17] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Trans. Ind. Informatics, vol. 10, no. 4, pp. 2233–2243, 2014, doi: 10.1109/TII.2014.2300753.

[18] Y. Pramitarini, T. Tran, K. Shim, A. W. Yulianto, and B. An, "A Speed and Cosine Similarity-based Clustering for QoS Routing Protocol in Distributed Vehicular Ad-hoc Networks," in The 10th International Conference on Green and Human Information Technology, 2022, pp. 109–113.

[19] A. Hariyadi, M. Taufik, H. Hudiono, N. Hidayati, A. E. Rakhmania, and R. H. Y. Perdana, "Efisiensi Daya Perangkat Wireless Sensor Network Pada Penerangan Jalan Umum (PJU) Berbasis Algoritma Leach," Techné J. Ilm. Elektrotek., vol. 20, no. 2, pp. 101–112, 2021, [Online]. Available: http://ojs.jurnaltechne.org/index.php/techne/article/view/264, doi: 10.31358/techne.v20i2.264.

[20] R. H. Y. Perdana, N. Hidayati, A. W. Yulianto, V. Al Hadid Firdaus, N. N. Sari, and D. Suprianto, "Jig Detection Using Scanning Method Base On Internet Of Things For Smart Learning Factory," in 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2020, pp. 1–5, doi: 10.1109/IEMTRONICS51293.2020.9216392.

[21] R. H. Y. Perdana, H. Hudiono, and A. F. N. Luqmani, "Water Leak Detection and Shut-Off System on Water Distribution Pipe Network Using Wireless Sensor Network," in 2019 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation, ICAMIMIA 2019 - Proceeding, 2019, pp. 297–301, doi: 10.1109/ICAMIMIA47173.2019.9223386.

[22] P. Gandotra, R. K. Jha, and S. Jain, "Green Communication in Next Generation Cellular Networks: A Survey," IEEE Access, vol. 5, pp. 11727–11758, 2017, doi: 10.1109/ACCESS.2017.2711784.

[23] Y. Pramitarini, R. Hendra, Y. Perdana, K. Shim, and B. An, "Particle Swarm Optimization-based Clustering Algorithm to Support QoS Routing Protocol in Flying Ad-hoc Networks with CF-mMIMO," in The 11th International Conference on Green and Human Information Technology, 2023, pp. 214–219, doi: 10.3390/s23187960.

[24] R. H. Y. Perdana, T.-V. Nguyen, and B. An, "Adaptive User Pairing in Multi-IRS-aided Massive MIMO-NOMA Networks: Spectral Efficiency Maximization and Deep Learning Design," IEEE Trans. Commun., vol. 71, no. 7, pp. 4377–4390, 2023, doi: 10.1109/TCOMM.2023.3277533.

[25] R. H. Y. Perdana, T. Van Nguyen, Y. Pramitarini, K. Shim, and B. An, "Deep Learning-based Spectral Efficiency Maximization in Massive MIMO-NOMA Systems with STAR-RIS," in 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2023, pp. 644–649, doi: 10.1109/ICUFN57995.2023.10199634 .

[26] R. H. Y. Perdana, T.-V. Nguyen, and B. An, "A Deep Learning-Based Spectral Efficiency Maximization in Multiple Users Multiple STAR-RISs Massive MIMO-NOMA Networks," in 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), 2023, pp. 675–680, doi: 10.1109/ICUFN57995.2023.10199634.

[27] R. H. Y. Perdana, T.-V. Nguyen, and B. An, "Deep Learning-based Power Allocation in Massive MIMO Systems with SLNR and SINR Criterions," in 2021 Twelfth International

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.20957

Conference on Ubiquitous and Future Networks (ICUFN), 2021, pp. 87–92, doi: 10.1109/ICUFN49451.2021.9528565.

[28] Y. Pramitarini, R. H. Y. Perdana, T. Tran, K. Shim, and B. An, "A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering against Sinkhole Attack in VANETs," Sensors, vol. 22, no. 15, pp. 1–22, 2022, doi: 10.3390/s22155811 .

[29] Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "DLSMR : Deep Learning-Based Secure Multicast Routing Protocol against Wormhole Attack in Flying Ad Hoc Networks with Cell-Free Massive Multiple-Input Multiple-Output," Sensors, vol. 23, no. 18, p. 23, 2023, doi: 10.3390/s23187960.

[30] A. Amalia, Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "A Deep-Learning-Based Secure Routing Protocol to Avoid Blackhole Attacks in VANETs," Sensors, vol. 23, no. 19, pp. 1–28, Oct. 2023, doi: 10.3390/s23198224.