LOGI – Scientific Journal on Transport and Logistics
Vol. 14 No. 1 2023 DOI: 10.2478/logi-2023-0003

An Optimal Security Framework Based on Driver Authentication for Intelligent Transportation Systems

Shalini Yadav[1*] and Rahul Rishi[1]

[1]Maharshi Dayanand University, University Institute of Engineering & Technology, Department of Computer Science and Engineering, Rohtak, India; Email: sch.shaliniyadav@gmail.com, rahulrishi@mdu.ac.in

***Corresponding Author:** Shalini Yadav

Received: 2 August 2022; Revised: 2 October 2022; Accepted: 2023; Published: 2023

Abstract: Security and safety have been a critical issue in the field of Intelligent Transportation Systems. Security of both people and vehicles is a matter of concern. In this paper, an authentication-based security framework is designed to serve the purpose. Only authorized users are provided access to the vehicle. The drivers are first registered for driving the vehicle from an authorized and valid source. The next step is the authentication check before one can be given access to the vehicle. There are two alternative methods provided for the authentication check in the solution depending upon the situation the vehicle is in. The solution is an optimally viable solution from the security perspective of the real-time Intelligent Transportation System environment. The results have shown that the security solution fits into the domain very well and performs as per expectations. The solution has been tested on a Vehicle Tracking Device connected to a vehicle. The same solution can be extended to a fleet of vehicles.

Keywords: Intelligent transportation system, vehicle tracking device, authentication, smart city

1. Introduction

The Intelligent Transportation System (ITS) field is a much-researched field with new technology being added every day to it. It has increased both the scope and power of the field. There are vehicles used for all kinds of purposes for travelling, as hospitals, as mobile kitchens, as homes. ITS has not only been restricted to travel or transportation but also to accommodation as well as hospitals. Human creativity has no limits. With the incorporation of VTD (Vehicle Tracking Device) devices and SIM, ITS has been provides enormous communicating power, and with the vehicle communicating with other vehicles or RSU (Road Side Unite) or any other connectable device, it has also raised concern to the security aspect. Security is of paramount importance in a connected world. Vehicles are considered an essential commodity in the developed world and a luxury in the still-developing world.

The ITS field has provided a new dimension or a complete makeover to these vehicles and all connected and communicating devices. Communication technology has integrated ITS very finely into the smart world. Therefore, security is of utmost importance when one ecosystem communicates with the other ecosystem. Thereby it is not just the cost of ITS and infrastructure but the data and information sharing or the communicating faculty that requires the ITS to become a very secure ITS. Security again has many domains and branches varying from cybersecurity attacks like routing, spoofing, man in the middle, denial of service, data poisoning, AI and cloud attacks, etc. [1] to major attacks on confidentiality, integrity, authentication, non-repudiation, availability, privacy [2]. Out of the many security issues, the paper deals with identity privacy, authentication, authorization, and security from theft. In addition to providing security, the paper goes way ahead to track the ecosystem as well as provide an optimized solution for security in ITS.

1.1 Motivation

Security has always been a challenging area in the connected transportation world. So providing an optimized security solution to ITS has been the guiding force for this work. This paper allows only an authenticated driver to access a vehicle. The vehicle access is entirely under secure control. The paper defines one of the strongest authentication security solutions for vehicular access. The driver is first registered into the ecosystem as the valid or authorized driver. Access to the vehicle is only provided by first verifying the driver. This security is provided by using a biometric sensor. The authentication check can be done locally or can be done at the server end. The authentication check done at the server makes the solution more secure but network use may become an issue in this case. The authentication check done locally at the device results in providing an optimal security solution thereby saving time and network bandwidth.

The vital contribution of the paper can be summarized as follows:

- An optimal security framework for the smart transportation system by allowing only authenticated driver access to the vehicle or fleet of vehicles.
- The drivers are first registered physically into the vehicle ecosystem as valid drivers.
- Only these registered drivers can start the vehicle. The authentication check has two options: a remote check at the server or a local check at the vehicle tracking device (VTD)

The paper is divided into five sections. This is the first introduction section. Section 2 studies the existing literature in the ITS field. Section 3 explains the system model. Results and discussion are illustrated in section 4. Section 5 finally concludes the paper. The paper achieves the aim of developing a strong security solution for driver authentication in vehicles.

2. Related Work

In [3] authors provided a lightweight framework for ITS. The framework is based on fog computing. When compared to a current framework, iFogSim, it provided better security, latency and energy consumption. PrivacySignal [4], a traffic signal control system preserves the privacy of users and efficient system performance is shown by a theoretical analysis and simulation experiments. The authors in [5] classified 28 parameters into 5 categories being government, financial constraints, inadequate transport infrastructure, the overdevelopment of urbanization and the readiness and integration of ITS. A systematic understanding of urban mobility is provided for government, planners, agencies and designers. The importance of digital infrastructure is highlighted. The paper [6] developed a process to authenticate vehicles to facilitate security in an ITS cloud network. Authentication redundancy is moved to identify a vehicular unit over many RSUs. Some of the past studies like [7] enumerated the various human biometric authentication systems. Their pros and cons are analyzed in detail with respect to traditional security methods like passwords and PINs. Many previous studies [8] illustrated various biometric technology and their respective application fields. The applicability of the biometric sensor depends entirely on the situation at hand. Authors in [9] modified and used virtual sensors in their work to identify the identity of the driver. Driver identification over the vehicular networks provided additional authentication. Author [10] developed the hardware framework w.r.t. AIS-140 standard for vehicle tracking. The work has shown fruitful results. Authors in [11] designed an architecture to authenticate V2X entities over the vehicular network. Any threat or fault in security in terms of authentication can be easily caught up. The author [12] proposed a reliable system by the efficient distribution of workload and functionality between the various components of ITS. The work in [13] recapitulates the recent developments in 3GPP with respect to radio, network architecture and application areas. The author in [14] identified the semantic gaps between existing security solutions and security privacy issues. Authors in [15] developed time-based authentication to avoid false authentication and identity and location privacy. Cellular-based communication security solutions are given out. In [16] authors applied cellular-based cryptography and trust-based schemes to preserve both identity and location privacy. Cellular-based communication security solutions are given out. The IoT-based ITS framework in [17] is extended to keep check of the fastened package transportation in the connected environment. It is successfully tested in a Wi-Fi enabled environment. The Author in [18] mounted sensors in e-vehicles to detect and prevent road mishaps. Eye-blink, fingerprint and alcohol sensors are retrofitted to carry out the intended work. Abdul Nafrees in [19] enhanced the monitoring solution in ITS to accurately define the bus location for the public buses network in a real-time environment. The driver can be monitored virtually. Study [20] answered the issues of driver identification by employing real driving datasets collected from onboard vehicular sensors. The driving pattern of the driver and the driver features refine the identification performance. Author in [21] designed a framework for driver identification that works on accelerated and brake pedal signals. The framework showed a 95% accuracy rate. Paper [22] outlined a number of sensor technologies for ITS. The incorporation of sensors and vehicles has taken ITS to new heights. It has provided a much more secure, controlled and sustainable solution. Paper [23] used cryptographic techniques to solve the problem of security and privacy. Author [24] designed a code-based authentication technique for integrity scans of intelligent vehicles. Qi Jiang in [25] proposed a model CT-AKA that incorporates 3-factor authentication and a key agreement protocol for a strengthened security solution. The paper in [26] used a biometric device, a temper-proof device and a decentralized authentication privacy protocol to enhance security levels. In [27] the authors review the existing data fusion techniques by which information from multiple sensors are combined to reach a better inference. This work also tries to find a better solution than those existing in the market. Some inspiration is taken in terms of the art and science of collaborative decision-making in [28].

3. System Model

Security has always been a pain area in the communicating transportation world. So providing an optimized security solution to ITS has been the guiding force for this work. The work studies the existing solutions in the field followed by conception then development, testing and validation. This paper allows only authenticated drivers to access the vehicle. The vehicle access is entirely under secure control. The paper defines one of the strongest authentication security solutions for vehicular access. The driver is first registered into the ecosystem as the valid or authorized driver. Access to the vehicle is only provided by first verifying the driver. This security is provided by using a biometric sensor. The authentication check can be done locally or can be done at the server end. The authentication check done at the server makes the solution more secure, but network use may become an issue in this case. The authentication check done locally at the device results in providing an optimal security solution thereby saving time and network bandwidth. As the driver has to be physically present in the vehicle to start it and cannot do so from a mobile app or any other distant process, it makes it the most secure and very different compared to all other methods. The approach successfully answers the security issue in the vehicles related to driver authentication resulting in a strong secure system.

3.1 Registration Process

The registration steps are as follows:

- The authorized user initiates the registration process from the mobile number i.e. pre-programmed in the VTD using the SMS command.

- The vehicle tracking device then triggers the fingerprint scanner to register the user as a valid driver of the vehicle.
- The driver is then prompted to put and take off his finger five to eight times on the scanner to cumulate the fingerprint template for enrolment.
- The scanner then forwards this template data to the VTD for temporary storage.
- The VTD keeps this template data in its memory.
- If the registration is successful, the VTD stores this data permanently in the memory. Else, it rejects its temporary memory.
- The VTD sends the status of the registration process to the pre-programmed mobile number with the help of the SMS command. It may be a success or a failure. Table 1 illustrates the requirement corresponding to various stages of the registration process. Figure 1 explains the process flow in a diagram.

Table 1 Registration process requirements. Source: authors

Stages	**Requirements**
Input	Valid Driver's fingerprint
Output	Driver successfully registered
Components	Fingerprint scanner, VTD, mobile with SIM, required communication channel
Pre-requisites	Authorized mobile number is pre-programmed into VTD
Users	Driver, authorized person to register/a person with all the credentials of the authorized person

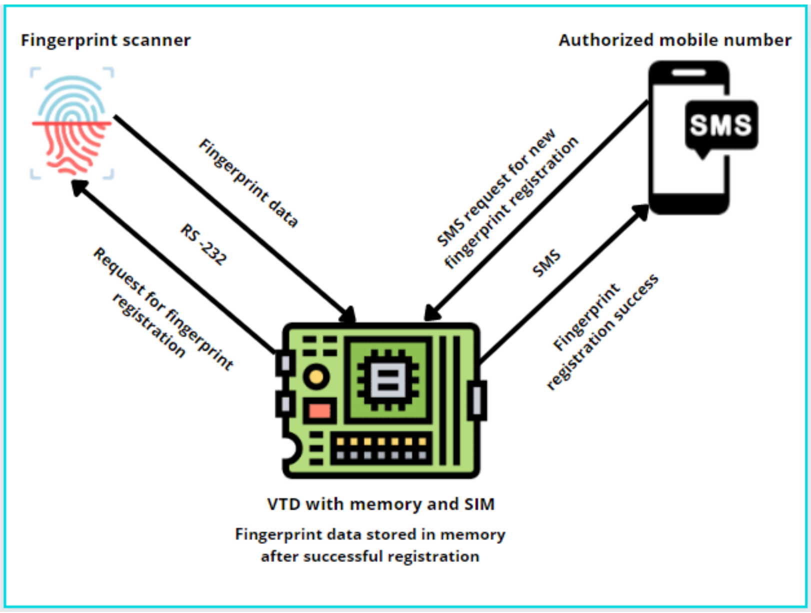
Fingerprint scanner
Authorized mobile number
SMS
Fingerprint data
RS -232
Request for fingerprint registration
SMS request for new fingerprint registration
SMS
Fingerprint registration success
VTD with memory and SIM
Fingerprint data stored in memory after successful registration

Fig. 1 Registration Process. Source: authors

3.2 Authentication Process

The authentication steps are as follows:

- The user/driver puts his finger on the fingerprint scanner.
- The template pictures are sent to the VTD for further processing by the scanner.
- In case 1 i.e. authentication at the server, the VTD forwards this data to the server for an authentication check. If a match is found the server sends ‘T’ to the VTD. If no match is found, it returns ‘F’.
- In case 2 i.e. authentication at the VTD (locally), the incoming data from the fingerprint scanner is compared to the data stored in the memory of the VTD.
- If a match is found, the VTD signals the relay that in turn triggers the start mechanism of the vehicle for a pre-determined period of time and the driver can start the vehicle.
- If a match is not found, the vehicle’s start mechanism is disabled and the user cannot start the vehicle. Table 2 enlists the various stages in the authentication process and their corresponding requirements. Figure 2 is the schematic diagram of the authentication process flow.

Table 2 Authentication process requirements. Source: authors

Stages	Requirements
Input	Driver fingerprint
Output	Vehicle shall/ shall not start
Components	Fingerprint scanner, VTD, server (for remote verification), required communication channel
Pre-requisites	Valid driver to be registered, internet connection (for remote verification)
Users	Driver

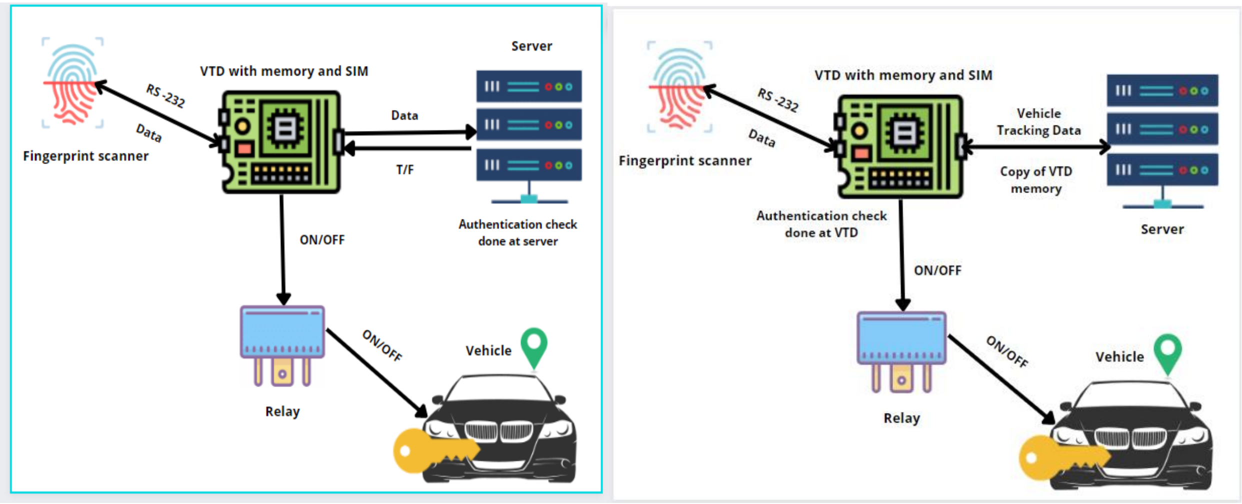

Fig. 2 Authentication at (a) server and at (b) VTD. Source: authors

3.3 Description

The mobile number which sends the SMS command for registration is pre-programmed into the VTD. The VTD is a combination of a Global Navigation Satellite System (GNSS) and a cellular system: General Packet Radio Service (GPRS). This helps in continuous tracking. It is capable of operating at a range of 9 to 90 V DC. It has a Unique Identification Number (UIN) i.e. IMEI. The fingerprint scanner and the VTD are connected by RS-232 TTL wired port at a baud rate of 9600. The fingerprint scanner works on 5V DC and derives its power from the VTD. The VTD operates at 3.3V. The level shifter circuit is used to bridge the voltage difference between the fingerprint scanner and the VTD. Communication between the fingerprint scanner and the VTD is in hexadecimal format. Communication between the VTD and the phone is in ASCII format. A relay has been added and linked to the digital output of the VTD. When signaled by the VTD to start the vehicle, the relay then triggers the start of the vehicle for a pre-defined and fixed time interval. The fingerprint data is stored both at the VTD and the server making it a reliable solution. Local authentication at the device saves the network access time and bandwidth providing an optimal solution. The driver has to be physically present at the vehicle to start the vehicle. So no compromise is made with security.

4. Results and Discussion

After the development and installation of the solution, the solution is tested on a device i.e. well-fitted with the VTD. It is well connected to communicate with the internet-enabled smart city environment. The vehicle is both receiving and sending data via the VTD to the server. The sensors are tested and deployed on the vehicle. Ten drivers were first registered as valid drivers of the vehicle using the fingerprint scanner. The time taken to register a driver into the system is between two and five minutes. The number of users that can be added to the vehicle is limited by the VTD memory size if the verification check is done at the VTD. The VTD memory size in this experiment is 4 MB. Therefore, a limit has been set on the number of users that can be registered. A maximum number of 100 users can be registered into the VTD. If registration is on the server, it can be extended to a very large number of users, but doing so is not required. The framework was tested by 100 users. The VTD allowed only the 10 users that were registered at the VTD to access to the vehicle. It was tested in two scenarios with internet connection and without internet connection. When the vehicle has a network connection and is connected to the server, the authentication check is done at the server. The time taken for verification of the user at the server is 1.38 seconds. There may be a case when the vehicle is in a place where there is no network (for example: a basement where there is no connection to the internet). The latter case becomes a problem and even a valid driver will not be able to start the vehicle. Therefore, an optimal option is provided, wherein the authentication check is done locally at the VTD. The memory of the VTD contains a copy of the valid drivers of the vehicles. As a result, a valid driver can start the vehicle in the absence of the network. The time taken for verification of the user at the VTD is 0.58 seconds. The hardware components required for the ecosystem are: a fingerprint scanner, a vehicle tracking device, RS-232, a relay, a server, a mobile phone with an authorized mobile phone number and a vehicle.

Table 3 Communication method format. Source: authors

Communication between devices	Format
Mobile – VTD	ASCII
VTD – Fingerprint scanner	Hexadecimal
VTD – Server	ASCII, hexadecimal
VTD – relay	Binary

Table 4 Parameters assumed with values and results. Source: authors

Parameters	Value
No. of users registered into system	10 drivers
Testing sample size	100 persons
Average time taken to register driver into the system	2-5 minutes
VTD memory size	4 mb
Server memory size	3 tb
Time taken for verification at server	1.38 sec (depending on internet speed)
Time taken for verification at VTD	0.58 sec
Time duration for which start mechanism is enabled after successful verification	5 seconds

Table 3 enumerates the communication method format and Table 4 illustrates the results and findings.

When the network is up and working, the VTD transfers its memory data copy along with the tracking information to the server. The start mechanism of the user is enabled for 5 seconds after the successful match, so the vehicle is very secure and safe. The experimental results show that in the absence of a network, the verification check at the VTD is a better option than at the server. The option of a verification check at the VTD is optimally more secure and saves time and cost. However, the verification check done at the server is still a strong security solution. The solution performed as intended and fitted well into the real-time ITS area. The framework made was implemented on a single vehicle. It can be easily extended for a fleet of vehicles. The false acceptance rate (incorrect sample is accepted as correct) is 0.001% (scanner limitation). It was 0 when carried out. The false rejection rate (correct sample is taken as incorrect) was 0.1% (scanner dependent).

5. Conclusions

The paper begins by studying the existing literature, conceptualizing the solution for a more secure system, then development, installation, testing and validation. It provides a high-level security solution to vehicles in the smart city. It is optimally one of the most secure applications available. It is simple and the communication overhead is minimum. Drivers are registered from a predefined or authorized mobile number of the authorized user thereby providing only authorized people access to the vehicle. Only registered drivers can operate the vehicle. A record of all the drivers and activities is kept within the system. Proper tracking of the driver is done. It may be used by the police, insurance companies and the government for various purposes. The results validate the solution. The results in table 4 show that the time required in matching the sample (test sample of individual) to the registered driver is shorter when the comparison is made locally at the VTD than at the server. The solution is very simple in design and it is very much practically viable. The application may be scaled if needed for a fleet of vehicles. It can be used to study driver behavior which is not included in the present work.

References

[1] Mecheva, T. & Kakanakov, N. (2020). Cybersecurity in Intelligent Transportation Systems. MDPI: Computers 9(4), 83. DOI: 10.20944/preprints202008.0082.v1.

[2] Hahn, D.A., Munir, A. & Behzadan, V. (2019). Security and Privacy issues in ITS: Classification and challenges. IEEE ITS Magazine 13(1), 181-196. DOI: 10.1109/MITS.2019.2898973.

[3] Baker, T., Asim, M., Samwini, H., Shamim, N., Alani, M. & Buyya, R. (2022). A blockchain-based Fog-oriented lightweight frame-work for smart public vehicular transportation systems. Computer Networks 2022, 20, 108676. DOI: 10.1016/j.comnet.2021.108676.

[4] Ying, Z., Cao, S., Liu, X., Ma, Z., Ma, J. & Deng, R. (2022). PrivacySignal: Privacy-Preserving Traffic Signal Control for Intelligent Transportation System. IEEE TITS, 1-14. DOI: 10.1109/TITS.2022.3149600.

[5] Tran, C., Tat, T., Tam, V. & Tran, D. (2022). Factors affecting intelligent transport systems towards a smart city: a critical review. T&F: Int. J. of Construction Management, 1-17. DOI: 10.1080/15623599.2022.2029680.

[6] Elahi, M., Rahman, M. & Islam, M.M. (2022). An efficient authentication scheme for secured service provisioning in edge-enabled vehicular cloud networks towards sustainable smart cities. Sustainable Cities and Society 76, 103384. DOI: 10.1016/j.scs.2021.103384.

[7] Abdulrahman, S. & Alhayani, B. (2021). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. In Proceedings of the Conference of Materials today. DOI: 10.1016/j.matpr.2021.07.

[8] Liu, S. & Silverman, M. (2001). A practical guide to biometric security technology. IEEE IT Professional Magazine 3(1), 27-32. DOI: 10.1109/6294.899930.

[9] Rettore, P., Campolina, A., Souza, A., Maia, G., Villas, L. & Loureiro. (2018). A. Driver Authentication in VANETs based on Intra-Vehicular Sensor Data. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil. DOI: 10.1109/ISCC.2018.8538506.

[10] Padmanabha, K., Basarkod, P. & Asuti, M. (2018). Automotive Electronic safety for Intelligent Transportation System. In Proceedings of the 2018 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). DOI: 10.1109/RTEICT42901.2018.9012644.

[11] Muhammad, M. & Safdar, G. (2018). Survey on existing authentication issues for cellular-assisted V2X communication. Vehicular Communications 12, 50-65. DOI: 10.1016/j.vehcom.2018.01.008.

[12] Diewald, S., Leinmuller, T., Atanassow, B., Breyer, L. & Kranz, M. (2012). Mobile Device Integration with V2X Communication. In the Proceedings of the 19th 2012 ITS World Congress, Vienna, Austria. Retrieved March, 2022, from https://trid.trb.org/view/1264269.

[13] Husain, S., Kunz, A., Prasad, A., Pateromichelakis, E. & Samdanis, K. (2019). Ultra-High Reliable 5G V2X Communications. IEEE Communications Standards Magazine 3(2), 46 – 52. DOI: 10.1109/MCOMSTD.2019.1900008.

[14] Hasan, M., Mohan, S., Shimizu, T. & Lu, H. (2020). Securing Vehicle-to-Everything (V2X) Communication Platforms. IEEE Transactions on Intelligent Vehicles 5(4), 693 – 713. DOI: 10.1109/TIV.2020.2987430.

[15] Rogobete, M. & Marin, E. (2020). Improved authentication method in embedded networks systems. An autonomous vehicle approach. Scientific Bulletin of Naval Academy 23(1), 253-256. DOI: 10.21279/1454-864X-20-I1-035.

[16] Huang, J., Fang, D., Qian, Y. & Hu, R. (2020). Recent Advances and Challenges in Security and Privacy for V2X Communications. IEEE Open Journal of Vehicular Technology 1, 244-266. DOI: 10.1109/OJVT.2020.2999885.

[17] Ekanayake, L., Nawarathna, R., Gunathilake, P., Yapa, R. & Pinidiyaarachchi, A. (2019). Smart Protector: A Real-time Theft Prevention System for Transportation Management. In the Proceedings of the 2019 14th Conference on Industrial and Information Sys-tems (ICIIS), Kandy, Sri Lanka. DOI: 10.1109/ICIIS47346.2019.9063319.

[18] Pothirasan, N. & Rajasekaran, M. (2018). Retrofitting of Sensors in BLDC Motor Based e-Vehicle—A Step Towards Intelligent Trans-portation System. In Book series Smart Innovation, Systems and Technologies 105, 61-69. DOI: 10.1007/978-981-13-1927-3_7.

[19] Nafrees, A., Raseez, S., Ubeshanan, C., Achutharaj, K. & Hanees, A. (2021). Intelligent Transportation System using Smartphone. In the Proceedings of the 2021 5th International Conference on Electrical, Electronics, Communication, Computer Technolo-gies and Optimization Techniques (ICEECCOT), Mysuru, India DOI: 10.1109/ICEECCOT52851.2021.9708053.

[20] Ezzini, S., Berrada, I. & Ghogho, M. (2018). Who is behind the wheel? Driver identification and fingerprinting. Journal of Big Data 5(9). DOI: 10.1186/s40537-018-0118-7.

[21] Marchegiani, L. & Posner, I. (2018). Long-Term Driving Behaviour Modelling for Driver Identification. In the Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA. DOI: 10.1109/ITSC.2018.8569610.

[22] Guerrero-Ibáñez, J., Zeadally, S. & Contreras-Castillo, J. (2018). Sensor Technologies for Intelligent Transportation Systems. Sensors 18(4), 1212. DOI: 10.3390/s18041212.

[23] Vasudev, H. & Das, D. (2019). Work-in-Progress: SAFE: Secure Authentication for Future Entities Using Internet of Vehicles. In the Proceedings of the 2019 IEEE Real-Time Systems Symposium (RTSS), Hong Kong, China. Retrieved February, 2022, from https://research.iitj.ac.in/publication/work-in-progress-safe-secure-authentication-for-future-entities

[24] Yoo, J. & Yi, J. (2018). Code-Based Authentication Scheme for Lightweight Integrity Checking of Smart Vehicles. IEEE Access 6, 46731 – 46741. DOI: 10.1109/ACCESS.2018.2866626.

[25] Jiang, Q., Zhang, N., Ni, J., Ma, J., Ma, X. & Choo, K. (2020). Unified Biometric Privacy Preservation Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles. IEEE Transactions on Vehicular Technology 69(9), 9390 – 9401. DOI: 10.1109/TVT.2020.2971254.

[26] Hakeem, S., El-Gawad, M. & Kim, H. (2019). A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Net-works. IEEE Access 7, 119689 – 119705. DOI: 10.1109/ACCESS.2019.2937182.

[27] El Faouzi, N.E., Leung, H. & Kurian, A. (2011). Data fusion in intelligent transportation systems: Progress and challenges–A survey. Information Fusion 12(1), 4-10. DOI: 10.1016/j.inffus.2010.06.001.

[28] Raiffa, H. (2007). Negotiation analysis: The science and art of collaborative decision making. Harvard University Press. Retrieved May, 2022, from https://www.pon.harvard.edu/wp-content/uploads/images/posts/nas.pdf