Security Enhancement in IoV using User and Vehicle Certification

Akansha Singh
Department of Information Technology and Computer Application
Madan Mohan Malviya University of Technology
Gorakhpur, India

Shiva Prakash
Department of Information Technology and Computer Application
Madan Mohan Malviya University of Technology
Gorakhpur, India

ABSTRACT
Internet of Vehicles (IoV) provides new opportunities for the coordination of vehicles for enhancing and improving safety and transformation performance because many accidents occur in road. So, safety plays an important role. To prevent the vehicle from hijacked this proposed model is designed. If it was discussed about the authentication of vehicles, then there are protocols proposed by another author, but does not work of authentication of the vehicular user in the network. so, to remove this drawback this proposed model is discussed. This ASC protocol is used for vehicular user authentication and certificate used for vehicle authentication and also to avoid collision due to unnecessary delivery of messages. Both ASC protocol and certificate are combined for the authenticity of vehicular user and vehicle. To verify this protocol working condition Example, flowchart and algorithms are discussed for the authenticity of vehicle and user. This proposed approach is verified by using the SUMO (Simulator for Urban Mobility) simulator and NETEDIT ID. Result and analysis has also discussed this dissertation.

Keywords
Internet of vehicle, Vehicular user, Vehicles, Roadside Unit, Trust Authorities

1. INTRODUCTION
The changing era in IoT [1] (Internet of Thing) there is changes in schematic ADHOC network to IoV (Internet of Vehicle) [2]. First of all, it should be well understanding that work of IoV. IoV concerned to the real-time data collected and interchanges their data between vehicle and roads, vehicles and vehicles, as well as cities and vehicles, with help of the mobile-communication technology, GPRS systems, and information platforms to secure communication and information exchange and a driving instruction monitoring and controlling system network.

IoV ensure that collecting information, processing information, computing information, monitoring information, and sharing information related with vehicles, surrounding and roads. IoV is a network of integrated for supporting various application in IoT technology in ITS (intelligence transportation system) in road sides they are traffic management intelligence, dynamic information system intelligence and vehicle control intelligence.

IoV is a complex integrated network system, which connects different people within vehicles, different environmental entities, and different vehicles within cities. With the rapid development of computation and communications technologies, IoV promises huge commercial interest and research value. IoV (Internet of Vehicle) [3] state that communication of vehicle to vehicle. So, when the cooperation between vehicles can be done by VANETs (Vehicular Ad hoc Networks) with different routing protocol [4]. So, vehicle can communicate with each other for avoiding collision, for getting the best route for avoiding waiting time in charging station in electric vehicle or for parking zone, to search the route for less traffic so that wastage of time should be minimum.

IoV has issues in security and privacy of vehicular user and vehicles. So, in this proposed model work done on security accept of vehicular user and vehicle. So, these research gap should be filed to make secure of Internet of Vehicle more effective and useful. There gap should be fulfilling by providing security (double security) for vehicular user and vehicle.

This paper presents an overview of the proposed model of IoV for the security of vehicular user as well as vehicles. It is organized as follows: section Ⅱ presents a literature survey on based on Internet of Vehicles. Section Ⅲ represent proposed approach which contain flow diagram, example and algorithm. Section Ⅳ represent of result and analysis.

2. Literature Survey
The key goal of Internet of Things (IoT) has been the provision of value-added services based on the ubiquitously available smart devices that can offer diverse services by interacting with each other. However, the paradigm has evolved to its next phase, Social Internet of Things (SIoT), with the inception of an idea to empower these devices with consciousness. This cognizance enables these smart devices to socialize with each other based on shared context and mutual interests. The Social Internet of Vehicles (SIoV) applies SIoT concepts in the vehicular domain to revolutionize the existing ITS (Intelligent Transport System) [5] by adding value to existing VANET (Vehicular Ad-hoc Network) technology. This paper presents a scalable SIoV architecture based on Restful web technology. Furthermore, this paper emphasizes the importance of web technology to meet the required interoperability to support the composition of numerous services. The paper also discusses the enabling technologies and protocols [6].

[7] Author uses fog computing as real time for car parking system. Car parking is a vacant parking place where we can park our car especially in peak hours. For searching a parking slot in urban area take much time. So, by this there is wastage of long time, traffic also occurs, and waste significant gasoline that harms the environment. So, the author find along so that a vehicle can find a desirable parking slots more efficiency by communication and information technology such as VANET. So, in real time parking slot information and prediction on future processing parking slots. The user can also provide a benefit of it. Therefore, fog computing concepts is used for smart parking architecture which can improve smart parking in real time and also data transfer is

show higher efficiency as compare to other parking strategies.

[8] Two concepts occur Roadside Unit (RSU) and vehicle on board unit (OBU) equipped with capabilities of wireless communication. RSU is placed on road side unit, which is fixed in nature and also infrastructure backbone of VANET but OBU (vehicle on board unit) are placed on vehicle, so it move with vehicle where vehicle is going OBU will move with vehicle. Infrastructure communicates directly with OBU in wirelessly mode, but with communication with internet and application server in wired mode. On the other hand, OBU can only communicate with either themselves or infrastructure. Safety can be considered in large through broadcast. Elliptic Curve digital signature algorithm is applying in VANET for authentication.

[9] In this paper an agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles it clearly states that in transportation of electric vehicle, vehicle can get charge time to time. Now a day EVs electric vehicle are replacing or taking place of previous cars. When number of electric vehicles are increases, then due to increase of vehicle some challenges are arise such as the increasing waiting time in fast charging station. Author work on addressing these challenges by means of some mechanisms. Electric vehicle can follow such mechanism which can test different route planning and also explained by simulation strategy on communication for booking system in charging stations.

Author JoongAng [10] the stable and seamless connection of the mobile communication system is expected to closely link an unprecedented number of things, including smart cars such as autonomous vehicles, in the near future. These vehicles will operate based on the data transmitted over hundreds of sensors. However, an attacker could remotely control a car by intercepting and tampering with these data, and even threaten the life of the driver. In this paper, we propose a code-based authentications scheme that provides both secure booting and lightweight data integrity checking to prevent unauthorized remote control. First, we split some of the core code involved in booting the car, and divide it into several secret pieces known as a share polynomial. One of these is distributed to the driver and is then used to reconstruct the booting code, allowing only the driver with this share polynomial to recover the code and start the car.

3. PROPOSED APPROACH

IoV is a concept that is used for vehicle communication on road. As many authors proposed the model related to the concept of security, but there is a research gap for finding both the vehicular user as well as vehicle authentication. So, to the best of my knowledge which is used for both vehicular user and vehicle authentication protocol is prepared in this proposed approach. With the help of flow diagram, example and algorithm this proposed approach is trying to verify.

IoV (internet of vehicle) is used for a vehicle on the road in which vehicles can communicate with each other to be secure. IoV allows a vehicle on road for the self-organized network so that communication can be possible and the vehicle can be secure in context with roadside accidents, making another vehicle stop unnecessary, avoidance of collision and many more. Information provided by the vehicle should be in real-time, authenticate and validate. An important message or information is shared between the vehicle to prevent it from security and another harmful attack.

When it comes to communication then it should be clear that how the vehicle is directly communicating with the vehicle in real-time, how the data are sent to the truth authority (TA), and it is more important than the data which send to another vehicle are valid or not. For communication, it is important to authenticate the vehicle and user before it started to communicate. Before the communication started between vehicle to vehicle, the first stage is every vehicle is sending a join request to trust authority with the assist of the roadside unit. Roadside unit (R) is located between every and used for Computing device located on the roadside that provides connectivity support to passing vehicles. When TA receives the request sent by vehicles and, it checks the authentication for both vehicle and R and only it allows to commutate or join when both vehicles and R are authorized or allowable.

In the year 2017 author Ying et al. proposed an ASC protocol [11-12] for anonymous and lightweight authentication for the secure vehicular network. Author claim that this vehicle can secure for the various attack. When it comes to the secure vehicular network then ASC protocol comes in a context. ASC protocol follows five steps, they are listed below.

I. **User registration phase**: in which the user registration is done with TA and certificate is given to vehicle.
II. **User login phase:** where each user is provided a login id and password or a small card that can be used for entering the vehicle.
III. **User authentication phase and vehicle authentication phase:** which is used for secure communication established between vehicles and TA.
IV. **Data authentication phase:** is used for secure datagrams are sent.
V. **Password change phase:** where the vehicular user attempts to change his/her password.

So, this ASC Protocol is changes within steps to provide authentication for vehicular user as we65752.ll as vehicle. When the communication started between vehicle to the vehicle then it first validates from trust authority and then communicates with another vehicle. So, in this model ASC protocol is combined with a vehicle certificate for making secure communication. For communication both card and vehicle registration certificate number is required so, that trusted authority can check for the authenticity of the user.

The rest of the organization of the report is as follows. Subsection 3.1 explained about the flow chart for this proposed approach. An example related to the flow diagram is explained in subsection 3.2. Subsection 3.3 explained about the algorithm used in this model.

3.1 Flow chart

As was explained in the proposed approach the research gap between the authentication of the vehicular user as well as the vehicle. So, to fulfill that gap between them flowchart is prepared in which in each and every step explained about the different phases of the vehicular user and vehicle. The explanation of every step is explained in the flow chart.

For user authentication ASC protocol is used, in which user has to register for user identity (USER ID) and for vehicular certificate, vehicle has to be certified from official certification entity (OCE). OCE generate key which is used

for the secure communication in the data authentication phase. After registration and certification phase users will log in to their vehicle with that User ID, this phase is working for the security of the vehicle. In this phase, another person not having the card are unable to use the vehicle. The third phase is used for connecting a secure connection before the communicated should be started. A user id and vehicle certificate are concatenated and send to truth authority for verification and authentication of user and vehicle. If concatenated between them is valid then join the channel otherwise reject and end. If vehicular user and vehicle authenticate is valid then secure communication start between the vehicle. If not ignore the information. When information is sent, between vehicle then there should be a validation of information. Means first the information sent by the vehicle is validated from the camera present in the road. After then the communication started between vehicles present nearby them. This is explained in flow chart 3.1 each step is explained with help of flowchart.

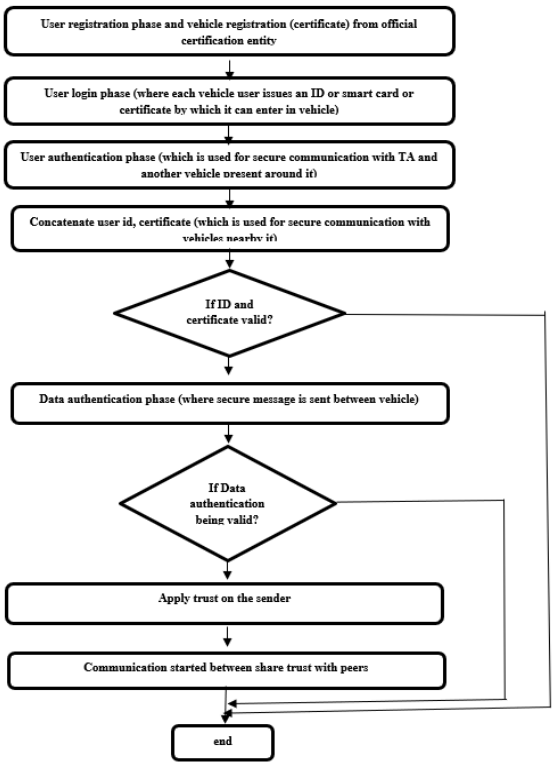
In this way, the security of the vehicle is maintained by using ASC (authentication for secure vehicular) network and vehicular certificate.

3.2 Example

In this section, there is a brief explanation of the example of the proposed model. This example shows different stages from where the vehicle has to pass for the security purpose. As in the figure, there are different terms used like trust authority, roadside unit, official certification entity. These terms are used for a different role in the IoV network. let's us explain it one by one.

Trust Authority: Trust Authority or TA is responsible for generating a unique card to the vehicular user, also user Id and password are given to them. This card contained a number of notations like [Ai, g, y, p, H0], this will come work in the login phase where a user will try to login vehicle. Trust Authority is also responsible for the user authentication phase where the vehicle request sends by the help of the roadside unit. TA matches the validity by collecting information on vehicular user USER ID and certificate from the vehicle, then they are compared

Official Certification entity this OCE is responsible for generating a certificate that contained a unique number. The unique number is generated from the number plate of the vehicle by concatenating it with random number r_i. **Road Side Unit** is responsible for collecting a request to the vehicle and forwarding it to TA for further work. Now it is important to learn how the example works in real life. As shown in figure 4.2 different numbers are listed like 1,2,3 and so on. Let us understand the different phases used in this proposed model.



Flowchart 3.1: Flow Diagram of Communication of User and another Vehicle for Authentication

1. **Registration phase:** This phase is the starting phase. In this phase, two work has been done first registration of the vehicular user and second registration of the vehicle. Let us take about one by one. Registration of the vehicular user is done for security purposes, where if any unauthorized users will try to enter the vehicle, they need a smart card to enter in it. If they get a card without the knowledge of the user then there is a requirement of user id and password. In the second registration, OCE will provide the certificate which contains a unique number. This unique number is generated with the help of the number plate of the vehicle.
2. **Login phase:** This phase is done so that the authentication of the vehicular user is verified. This phase is work as, when vehicular user wants to enter the vehicle, they required few things like the card, user id, and password. When the user used it card then user id and password present in the card are matched. If they are verified then the user is allowed to enter in vehicle.
3. **User authentication phase:** This phase is used for connecting a secure channel by which a vehicle communicates with each other. When any vehicle V_i wants to communicate with each other then the first communication channel should be prepared. This can be done with the help of the user authentication phase. In which vehicular user send a request to TA followed by RU. Vehicular user will send the user is given by TA and certificate number given by OCE. TA verified that user id and certificate if it is valid then a secure channel is established between vehicle to vehicle.
4. **Data authentication phase:** Now a secure communication channel is established, then the user

should send a request. But here in this phase again the data authenticate is validate, to verify that the vehicle which is trying to communicate is valid or not. So, the data is collected from the sensor and verified that the vehicle which wants to communicate is present nearby it. Its means that vehicle present and they want to communicate. So, allow if verification is done by sensor present in that area.

3.3 Algorithm

The algorithm for the proposed model is explained bellow in which different phases are described. The algorithm used for different vehicular users and the different vehicles is explained below. Which the first stage is the user registration phase in which the vehicular user and vehicle both are registered with their user id and they provided a smart card that contains id and password. Login phase has consumed for security where there should be a validation of smart card and id password enter by the user, when validation is not valid it delays the login request else allow for login. The next phase is the user authentication phase where the connection established between TA and authenticity of the user is validated when the user enters the smartcard and certificate correct then they are allowed for secure communication.

3.3.1 The user registration phase for vehicular user and vehicle

3.3.1.1 For vehicular user

For vehicular user registration phase users of vehicular are requested to register with for trust authority for its unique id and password. Trust authority generates a private and comparable public key using the Diffie Hallman problem. For which few steps are performed.

1. $\mathbf{V_i}$ is a vehicular user, V_i is required to produce a random number $\mathbf{r_i}$.
2. $\mathbf{V_i}$ sends its identity $\mathbf{(IDV_i)}$ and $\mathbf{H0(PW_i||r_i)}$ through a secure channel to TA (trust authority).
3. The role of trust authority is to collect the following information given by the vehicular user and generate a parameter for a USER ID, which is useful for the login for the vehicle.
4. Truth authority receives the request (T_{reg}) from the vehicular user and computes userid (USER ID) and password for vehicular us $\mathbf{(IDV_i))}$ password generated from vehicular user identity
   $\mathbf{(PV(IDV_i)) = H0(IDV_i)}$
   For authentication of Vi TA compute parameter known as Ai
   $\mathbf{A_i= H0(H0(PW_i/r_i)||(PV}(IDV_i)))$
5. Data issues by TA are present in the smart card they are [Ai, g, y, p, H0]

3.3.1.2 For Vehicle

For registration of the vehicle, vehicle certificate is generated by official certification authority (OCA) which gives a unique key ($\mathbf{U_k}$) for each vehicle (U_i) used for communication in the network.

1. Owner should request for digital certificate U_i provide by certifier.
2. Ui should be unique for this process it is bring to certified accreditation center (CAC)
3. Vehicle $\mathbf{(U_i)}$ number plate $\mathbf{(PU_e)}$
   $\mathbf{U_k=H0(PU_e||r_i)}$

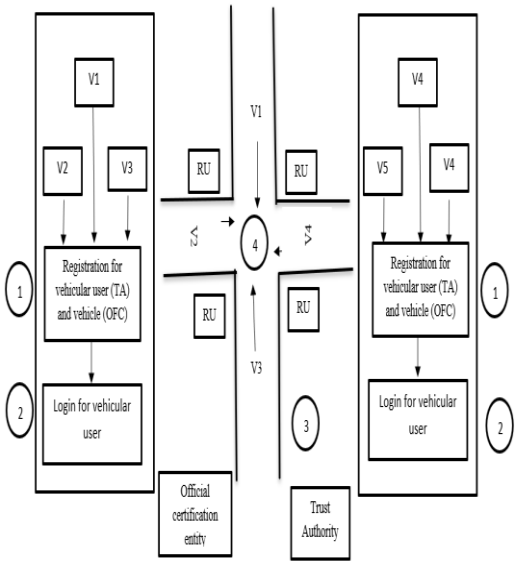


Fig: 3.2: Communication between Vehicular User and Another Vehicle for Authentication

3.3.2 User Login phase

This phase is used so that user can login in the vehicle with the help of smart card. This phase shows the authentication of user and also security of vehicle. Valid user is entering in the vehicle, no theft can allow to enter without the smart card.

1. Vehicular user Vi can enter in vehicle by inserting smart card which contain input of UserID (IDV_i*), Password (PW_i*), and random number (r_i).
2. Validation check
   If ((IDV_i=IDV_i*) and (PW_i=PW_i*))
   Then
   Valid
   Else
   Not valid
3. Again, compute A_i* and compare it with A_i given from TA
   A_i*=$\mathbf{H0(H0(PW_i*/r_i)||(PV}(IDV_i*))$
   If A_i*==A_i
   Then
   Allow to enter
   Else
   Terminate the process.

3.3.3 User Authentication Phase

This phase work for establish a secure communication session with TA with the smart card or User ID, the user authentication phase is invoked.

When secure communication session is established then there should be concatenation between vehicular user (unique id) and vehicle (certificate) generated by Trust Authority and official certified entity.

If Ho ($IDV_i||PV_e$) is valid
Then
allow for communication
Else
Ignore

3.3.4 Data Authentication Phase

This phase basically work for secure message or information are sent. When a vehicular user is authenticated by the trust authority, then information sharing between peer to peer and TA is done.

4. RESULT AND ANALYSIS

The experiments were performed on a computer with windows 10 OS, Intel (R) core ™ i3 CPU with 4 GB RAM. The proposed method is coded using SUMO in Python language. Several experiments were performed by NETEDIT 1.5.0 as shown in figures below. Fig 4.1 shows the successful conversion of the map into a node or network. first of all, the map of the route is downloaded from the open street map then it is converted into the network by netconvert –osm- files map.osm -o test.net.xml. The next step is to add the trip.Route to the network using build-in python scripts randomTrips.py, which coded as python path\randonTrips.py -n test.net.xml -r test.rou.xml -e 50 -1.

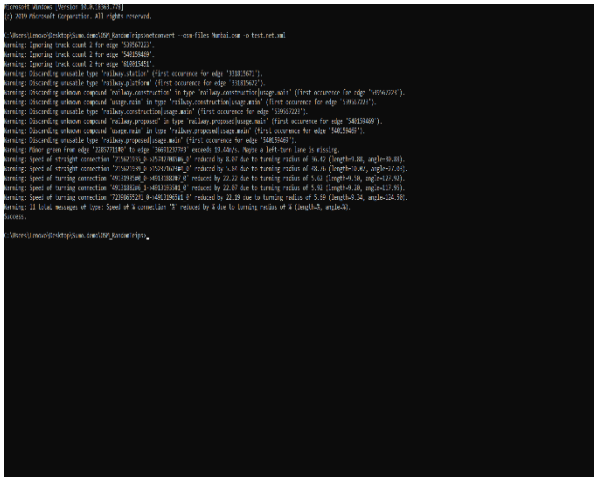


Fig 4.1: shows the successful conversion of the map into a node or network

When it runs successfully then it creates a path in SUMO from where the path should be open. We performed first level work in which the path or route is open in SUMO as shown in fig 4.2, this route contains 4 lane roads, lane number are identified as Lane1, lane 2, lane3, lane 4.
In fig 4.3 Shows junction and traffic light are created so that vehicle should move with instruction provided by the traffic light. Injunction vehicles can go with the direction which has shown by red and green color.

After giving a unique identification number to the vehicles and users of the vehicles. Communication started between the vehicles when they pass from the junction. As shown in fig 4. 4 vehicles are passed through crosssection area after only when it gets a pass from other vehicles.

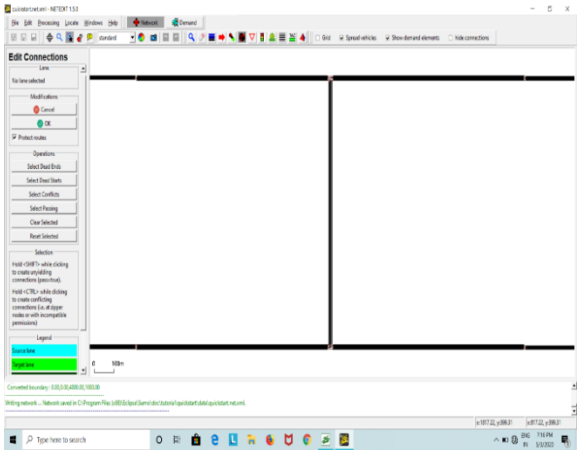


Fig 4.2: Shown the first level work in which the path is open

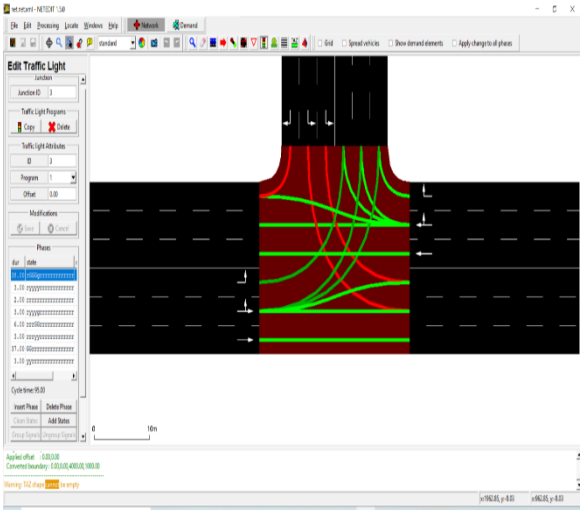


Fig 4.3*:* Shows junction and traffic light

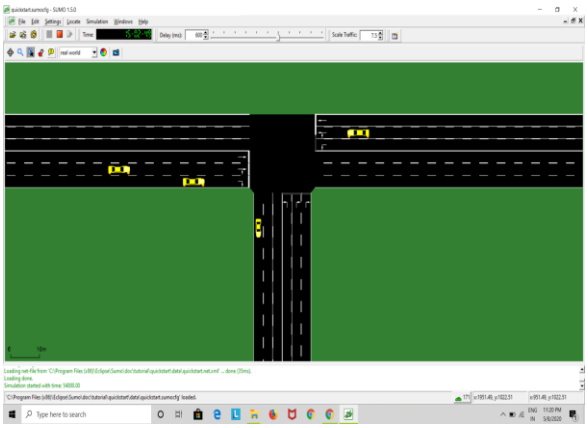


Fig 4.4: Vehicles are passed through cross-section

5. CONCLUSION

Finally, we conclude that Security Enhancement in IoV using the User and Vehicle Certification approach is secure in several attacks. The principle goal of building up this secure enhancement in IoV using user and vehicular certificate method is to fulfill security in the vehicle. Proposed method technology shows an effective method for secure vehicular users and vehicles with the help of certification. The above result shows the complete security of vehicles from the hijacker where the hijacker cannot hijack the vehicle without known the unique vehicular identification number. The test results of the purposed technique represent have demonstrated both the security and authentication of vehicles and vehicular user and robustness under attacks.

6. REFERENCES

[1] Patel, K.K., Patel, S.M., and Scholar, P.G. ,” Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”. International Journal of Engineering Science and Computing 6, 1–10,2016.

[2] Hegyi, A., De Schutter, B., & Hellendoorn, J. (2005). Optimal coordination of variable speed limits to suppress shock waves. *Intelligent Transportation Systems, IEEE Transactions on*, 6, 102-112.

[3] T. Schmidt, R. Philipsen, P. Themann, and M. Ziefle, “Public perception of V2X-technology - evaluation of

general advantages, disadvantages and reasons for data sharing with connected vehicles," in *IEEE Intelligent Vehicles Symposium*, Jun. 2016, pp. 1344 – 1349.

[4] Z. H. Gu, G. Han, H. B. Zeng, and Q. L. Zhao, "Securityaware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 10, pp. 3044–3057, Oct. 2016.

[5] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," IEEE Access, vol. 4, pp. 5356–5373, 2016.

[6] Aliedani and S. W. Loke, "Cooperative car parking using vehicle-to-vehicle communication: An agent-based analysis," Computers, Environment and Urban Systems, p. https://doi.org/10.1016/j.compenvurbsys.2018.06.002, 2018.

[7] K. Grover, A. Lim, S. Lee, and Q. Yang, "Privacy-enabled probabilistic verification in broadcast authentication for vehicular Networks," Ad Hoc and Sensor Wireless Networks, vol. 32, no. 3–4, pp. 239–274, 2016.

[8] García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, "ABSCEV: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles," Computer Networks, vol. 138, pp. 119–135, 2018.

[9] Chaogang Tang, Xianglin Wei, Chunsheng Zhi, Wei Chen,Joel J. P. C. Rodrigues," Towards Smart Parking Based on Fog Computing" ,IEEEAccess, 2018.

[10] Joonsang Yoo and Jeong Hyun Yi," Code-Based Authentication Scheme for Lightweight Integrity Checking of Smart Vehicles ", IEEE Journal, 2018.

[11] CHIEN-MING CHEN, BIN XIANG, YINING LIU and KING-HANG WANG, "A Secure Authentication Protocol for internet of vehicle", IEEE Access, Volume 7, January 2019, page number 12047-12056.

[12] Bidi Ying, Amiya Nayak, "Ananymous and lightweight authentication for secure vehicular network", IEEE TRANSACTION ON VEHICULAR TECHNOLOGY, VOL 66, DECEMBER 2017.