International Journal of Basic and Applied Sciences, 14 (4) (2025) 624-629

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/dq7ksd55
Research paper

Effective and Efficient Use of Elliptic Curve Cryptography (ECC) for The Security of Vehicular Data Platform/Networks

Amol Phatak [1] *, Dr. Rajendran T. [2]

[1] Research Scholar, CSE Dept, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India
[2] Professor and Head, Dept of CSE (Cyber Security), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India
**Corresponding author E-mail: amol1911@gmail.com*

Received: July 7, 2025, Accepted: August 15, 2025, Published: August 24, 2025

Abstract

Nowadays, with the widespread use of numerous sensors in vehicular data platforms/networks to enhance communication and support systems, a substantial amount of data is generated. The information gathered through this data is not secure, and it is necessary to apply security and privacy measures to vehicular data platforms/networks. This paper proposes the use of the ECC (Elliptic Curve Cryptography) method to achieve security and privacy. The large amount of vehicular data is divided into different types, such as live status data, vehicle details data, insurance data, maintenance data, etc. The proposed method categorizes this data into high-level, medium-level, and low-level categories to apply the appropriate cryptographic methods, thereby enhancing security and ensuring privacy for end-users. The ECC is implemented and analyzed on data of different sizes and compared its performance with a private key (symmetric) algorithm, DES (Data Encryption Standard), and AES (Advanced Encryption Standard), as well as the public-key (asymmetric) algorithm RSA (Rivest-Shamir-Adleman). The result shows that the use of ECC is effective and efficient for the security of vehicular data platforms/networks, compared with other traditional cryptographic algorithms.

Keywords: *ECC;Vehicular Data Networks; Security and Privacy; Private Key; AES; Public Key; RSA.*

1. Introduction

The vehicular data security has become more and more important, as all recent vehicles are equipped with a lot of sensors and electronic devices used to facilitate different kinds of vehicular information to the end users. The data generated and received through these sensors is not secure and raises security and privacy issues [1][2].

To deal with the lack of security concerns, the adaptive security mechanism was proposed to provide security and privacy to vehicular data platforms/networks. The traditional and standard private key that is symmetric cryptographic methods (DES, AES) and public key that is asymmetric cryptographic methods (RSA) are implemented to provide the security and privacy to vehicular data [7]. The time requirement of encryption and decryption using DES, AES, and RSA algorithms is comparatively higher and introduces a delay for real-time applications. The proposed method uses the Elliptic Curve Cryptography (ECC) to deal with a minimum time requirement for real-time scenarios and applications [6].

A good privacy protection mechanism selects the degree of privacy based on the vehicular data received. The proposed method divides the privacy degree into high level, medium level, and low level as per the importance of data and user demand. The user who is least worried about security and pays little attention to vehicular data security can select the low-level privacy degree, whereas the person of high importance, who is a Very Important Person (VIP), having very high concern, requires a high level of privacy to protect vehicular data from hackers/intruders.

The standard vehicular data is categorized into Vehicle Identification & configuration data, running status data, Maintenance data, Insurance Data, Driving Safety data, etc.

Table 1 indicates the different vehicular data categories based on the input data received through sensors and electronic devices or a database server that maintains the vehicular information.

Table 1: Vehicular Data Categories and Recommended Security Level

Sr. No.	Vehicular Data Category	Data Parameters	Recommended Security Level
1	Identification and Configuration data	Vehicle Authenticated Number given by RTO, Chassis/Engine number, Size and Shape of Vehicle, Fuel type (CNG, diesel, petrol, or electric), Vehicle Type, etc.	Medium
2	Live Location data	Current location of vehicle on map, Latitude and Longitude, etc.	High
3	Running Status Data	Vehicle speed, Seat Belt status, Fuel indicator, Light status, etc.	High
4	Vehicle Maintenance data	Number of Kilometers, Engine Oil level, Clutch status, Break status, Power/Battery status, Tire conditions, etc.	Low
5	Safety Data	Airbag status, ABS(Anti-Breaking System), Speed Limit, Seat belt status, Door Lock, Child Lock, Electronic Stability Control,	Medium
6	Vehicle Insurance data	Vehicle Insurance Number, Vehicle Insurance Type, Term/Duration of Insurance, Insured Name, Vehicle ID, etc	Low

As illustrated by the vehicular data categories and recommended security level in Table 1, data received through sensors, vehicular monitoring systems, or Intelligent Driver Assistant Systems is analyzed using the proposed model of Vehicular Data Analysis to categorize it according to Table 1. The security level of data is identified as per the category of vehicular data, and appropriate lightweight cryptographic algorithms are applied to provide the degree of privacy.

The details of the vehicular data analysis model, which is used to collect, process, and categorize the data, are given in Section 2. The experimental setup and its details are mentioned in Section 3; Section 4 provides the ECC algorithm and its working; Section 5 further showcases the results and analysis of the proposed method. Section 6 puts remarks in the conclusion and future scope.

2. Vehicular data analysis model

The data collected or received from Inertial Measurement Unit (IMU) sensors, Advanced Driver Assistant Systems (ADAS), etc, are given to the Data Acquisition System.

Data Acquisition is a process of collecting and analyzing data from physical phenomena and converting it into a digital format that can be processed by a computer. A block diagram of the same is shown in Figure 1.

The sensors detect and measure various characteristics and then make the measured signal suitable for storage and digitization. The analog-to-digital converters are used to convert the analog signals from the sensors into digital values that can be processed by a computer.

Therefore, the block of Data Acquisition is used for converting analog or real-world signals coming from sensors into a digital form used to store, display, and analyze.

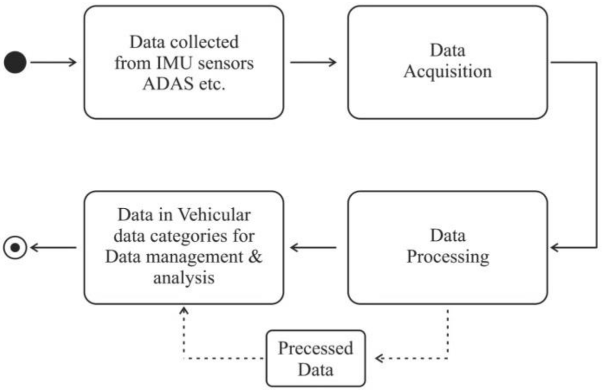
Data collected from IMU sensors ADAS etc.
Data Acquisition
Data Processing
Data in Vehicular data categories for Data management & analysis
Precessed Data

Fig. 1: Block Diagram of Vehicular Data Processing and Analysis Model.

After the transformation of information, the processing of information is carried out to determine the category of data by analyzing the various parameters and dividing the data into appropriate categories. The processed data is then given to the Data Management unit to distribute and apply the private-key, public-key, and ECC algorithms as per the recommended security levels.

3. Experimental setup

The modern era of vehicles uses many ECUs (Electronic Control Units) that use different ways of communication to connect with the CAN (Controller Area Network) protocol, which is the most widely used. However, several vulnerabilities, such as a lack of authentication and a lack of data encryption, have been pointed out by several authors [4][19].

The main component of the design is the vehicular simulator, the vehicle instrument cluster, and the rogue devices, which are all connected using the CAN_H and CAN_L wires, as shown in Figure 2, which indicates the block diagram. The instrument cluster was chosen as the vehicle dashboard that the driver interacts with and displays information related to the vehicle in a meaningful and useful way.

The simulation of remaining vehicle information is the responsibility of the Vehicular Simulator by sending the useful and relevant CAN messages over the network as if the cluster were installed in a real vehicle or car. The setup for the vehicle simulator consists of a CAN bus attached to an Arduino. The data inside the CAN message changes accordingly to the status of the car. It makes it easier to build a user interface for the simulator.

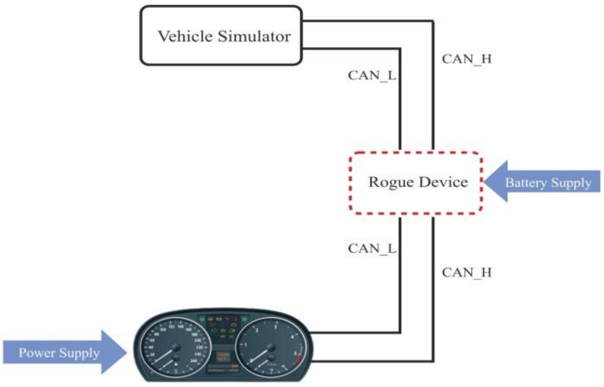

Fig. 2: A Block Diagram of the Research Experimental Setup.

The rogue device acts as a man-in-the-middle device between the instrument cluster and the vehicle simulator. The data transmitted by sensors can be modified by the rogue device, indicating a security attack and the lack of built-in security. It indicates the lack of security in the CAN bus protocol, a lack of authentication, and a lack of data encryption.
The AC/DC adapter is used to power up the instrument cluster, and the battery power supply is applied to the rogue device.

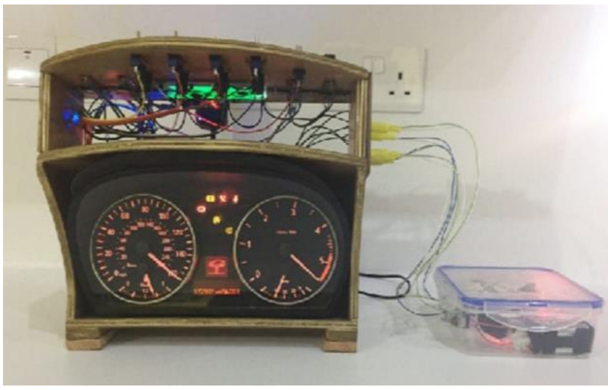

Fig. 3: Photo of Instrument Cluster.

Due to the lack of security measures implemented in the CAN Bus protocol, and to overcome the need for confidentiality and authentication, the proposed method implements the use of the ECC cryptographic algorithm to provide confidentiality, which makes the vehicular data secure. The use of the ECC algorithm helps data to be converted into an encrypted form and overcome attacks by unauthorized users who are using devices like rogue devices. In the implementation of ECC using Java, the data transmitted is in encrypted form, and the rogue device used for a man-in-the-middle attack cannot recognize the data, so we can overcome this attack. The testing of data of different categories as mentioned in Table 1, with different sizes (10KB to 100MB), was performed to calculate the performance of ECC to analyze its time complexity with other cryptographic algorithms. After taking more than 100 test cases/trials and their respective time values, the average value of all the test cases is used in the result analysis.

4. Elliptic curve cryptography

Elliptic Curve Cryptography (ECC) uses the algebraic elliptic curves architecture with finite fields and is an asymmetric encryption algorithm.

- Elliptic Curve Cryptography (ECC) is an asymmetric (public key) encryption technology like the RSA public key algorithm.
- While RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys.
- The elliptic curve ciphers were proposed separately by Neal Koblitz and Victor Miller. These are like public-key cryptography, where arithmetic can be replaced by elliptic curve operations.

Different blocks of Elliptic Curve Cryptography are as follows:

1) ECC uses a pair keys {Private key, Public Key}:

The Private Key of ECC is generated similarly to the generation of a random integer number between a given range. In ECC, the private key is any integer number in the field. Public keys are generated using Elliptic Curve points that are a pair of integer coordinates (x, y) on a curve. Due to the characteristics of Elliptic Curve points, it can be compressed into a single coordinate. The compressed point is used as a public key of 256 bits.

2) Generator Point:

A base point G is a pre-defined point generated by ECC to establish elliptic curves over finite fields. This base point G is useful for the generation of subgroup position points over the elliptic curve by multiplying base point G with some integer in the range of [0..r]. The ordering of a cyclic subgroup is known as r. Now the subgroups contain various generator points. The cryptologist then selects one of them to generate the complete subgroup. This procedure is known as the G Generator.

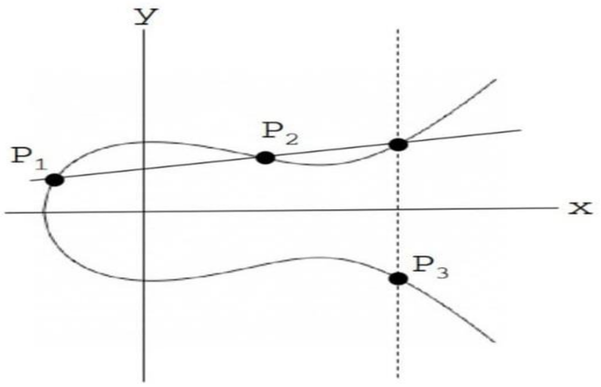

Fig. 4: Elliptic Curve Picture.

Consider Elliptic Curve E: y2 = x3 – x +1
We can define P2 = P1 + P2 if P1 and P2 are on E, as mentioned in the above diagram.
Now we need addition in affine coordinates:

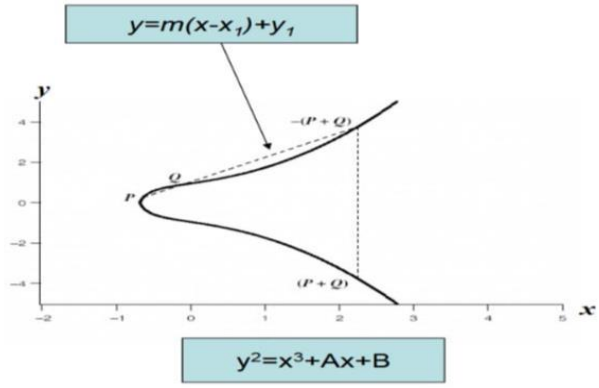

Fig. 5: Additions in Affine Coordinates.

P = (x1,y1), Q = (x2,y2)R = (P+Q) = (x3,y3)

Let, P != Q

M = y2 - y1 % x2 - x1

To find the intersection with,

(m (x-x1) + y1) 2=x3 + Ax + Bor0 = x3 – x1 – x2 + …..

So, x3 = m2 – x1 – x2
Therefore, y3 = m (x1 - x2) – y1
Encryption algorithms:
A public-key (PU) is used in an encryption algorithm for authentication purposes, which uses a key-derivation function, a special key referred to as the Medium Access Control(MAC) key. The private key (PR) generated from it is kept as a secure (secret) key.
A public-key cryptography, which is equivalent to ElGamal encryption, is referred to as Elliptic Curve-based ElGamal ECC. It is an asymmetric (two-key/public key) algorithm that is useful for sending messages over a long distance in a secure manner. The algorithm is vulnerable to a man-in-the-middle attack if the encrypted message is short, so padding is used to avoid sending short messages over a long distance.

5. Result and analysis

5.1. Merits and demerits of the ECC algorithm

Merits:
- The main advantage of ECC is that it works purely on an elliptic curve mathematical model.
- ECC gives significant bandwidth savings as compared to RSA.
- The encryption time required for ECC is less compared to other algorithms.

Demerit:
- Though the encryption time requirement is less, it takes more time for decryption.

5.2. Performance analysis of algorithms

The vehicular data are categorized using the proposed vehicular data analysis model. The category where a High-Security level is needed is encrypted using ECC. The ECC provides the same type of security as provided by DES, AES, and RSA. The use of ECC for high-importance of data makes it suitable as well, and the encryption time required is less compared to traditional DES, AES, and RSA.
To evaluate the performance of the ECC compared with the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), and the RSA on vehicular data of different categories, the vehicular data of different sizes are considered, evaluated, and analyzed.
The following Table 2 indicates the encryption time required for DES, AES, RSA, and ECC, based on the different vehicular data sizes:

Table 2: Encryption Time Comparisons of AES, RSA, and ECC Based on Encryption Time

Algorithm/Data or File Size	DES	AES	RSA	ECC
	Encryption time in ms	Encryption Time in ms	Encryption Time in ms	Encryption Time in ms
10 KB	6	600	956	421
1 MB	115	747	1260	726
10 MB	993	1083	2120	972
50 MB	3174	2001	6650	2360
100 MB	6838	4220	26033	11350

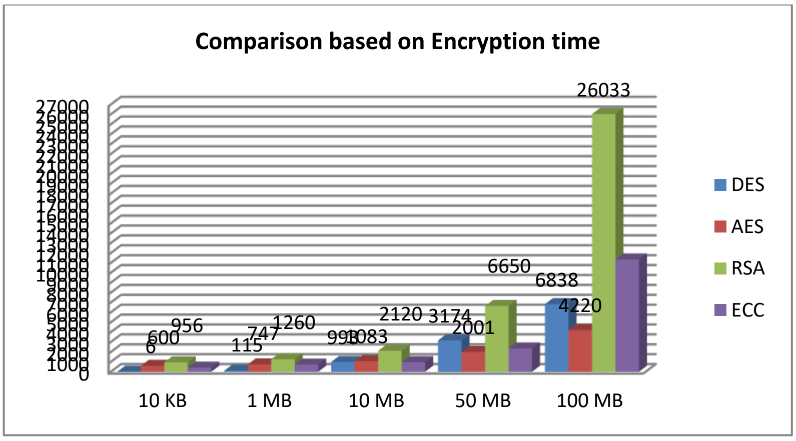

Fig. 6: A Bar Chart Indicating the Encryption Time Comparison of DES, AES, RSA, and ECC.

After analyzing the values of the above Table 2 and its subsequent graph represented in Figure 6, it indicates that ECC takes less time compared to AES and RSA for the vehicular data of size up to 10 MB. Generally, the size of vehicular data ranges from 1 KB to 1 MB; the encryption time required using ECC is less than 1000ms, which makes it faster compared to AES and RSA. The DES algorithm takes less time compared to the ECC for the file size of 10KB to 1MB, but ECC is comparatively more secure as compared to DES. The ECC time requirement is superior to DES, AES, and RSA for files of size 10MB to 50MB.
The ECC time requirement increases as the size of the file is larger than 50MB, due to the complexity of the algorithm as compared to DES and AES. On the other hand, it is more secure as compared to others. So there is a tradeoff between the time required for encryption and decryption versus the security level. The ECC proved to be more effective and efficient, considering the vehicular data ranges from 10MB to 50MB in size. The comparison of the ECC algorithm with AES and the RSA based on the key size is analyzed and presented in Table 3 below. The size of the key used for encryption varied from 6 bits to a maximum of 128 bits.

Table 3: Encryption Time Comparison of AES, RSA, and ECC Based on Key Size

Key Size (bits)	Encryption time required in ms		
	AES	RSA	ECC
6	1000	800	400
25	850	500	250
48	1100	720	300
102	2500	1200	650
128	250	120	70

The subsequent graph of Table 3 is shown below in Figure 7:

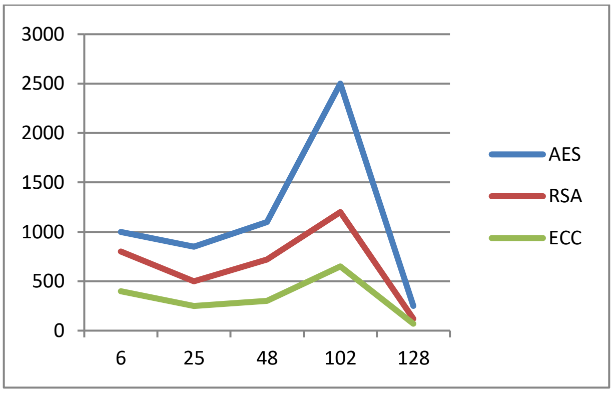

Fig. 7:A Graph Indicating the Encryption Time Comparison of DES, AES, RSA, and ECC Based on Key Size.

In Figure 7, the x-axis indicates the key size, and the y-axis indicates the time required for encryption in milliseconds. The analysis shows that the encryption time requirement of ECC is less for all key sizes compared to AES and RSA. Therefore, the use of ECC is effective for real-time applications such as autonomous driving, connected cars, and vehicle-to-vehicle communication, with the high-level security merits of ECC. For a key size of 128 bits, AES takes 250ms, RSA takes 120ms, whereas the proposed ECC algorithm takes only 70ms.

6. Conclusion and future scope

The proposed method of Elliptic Curve Cryptography (ECC) is an effective and efficient method for privacy and security of vehicular data. The experimental setup and implementation of the ECC were applied to different types of vehicular data. It divides the data into different categories and suggests/a suitable algorithm considering the high-level, medium-level, and low-level security demands.

The experimental results show that ECC is suitable and recommended for high-security applications as it provides similar security features compared to AES and RSA. The encryption time required for ECC is less and recommended for vehicular data up to 10 MB to 50MB. The results show that ECC proved to be faster and secure compared to DES, AES, and RSA. The ECC algorithm is more suitable for the privacy and security of vehicular data platforms.

In the future, it can be applied to a wide range of cryptographic algorithms, such as 3DES, Crypto, IDEA, etc., to analyze their performance with existing/proposed approaches. The existing work is useful in providing the security measures in a variety of applications, such as autonomous driving cars, vehicle-to-vehicle (V2V), and Vehicle to Everything (V2X) secure communication. Though the applications that demand less security and fast processing can use lightweight cryptographic protocols, the ECC proves to be more efficient and effective in achieving a very good security level.

References

[1] M. De Vincenzi, J. Moore, B. Smith, S. E. Sarma and I. Matteucci, "Security Risks and Designs in the Connected Vehicle Ecosystem: In-Vehicle and Edge Platforms," in *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 442-454, 2025, https://doi.org/10.1109/OJVT.2024.3524088.

[2] S. Khokha, "From Standards to Implementation: Functional Safety and Cybersecurity in Modern Autonomous and Electric Vehicles," 2024 International Conference on Cybernation and Computation (CYBERCOM), Dehradun, India, 2024, pp. 52-56, https://doi.org/10.1109/CYBERCOM63683.2024.10803155.

[3] P. A. W. Putro, F. Amelia, J. Pidanic, H. Suhartanto, I. A. Rahardjo and E. Imandeka, "Cybersecurity of Sensors on Smart Vehicles: Review of Threats and Solutions," 2023 6th International Conference of Computer and Informatics Engineering (IC2IE), Lombok, Indonesia, 2023, pp. 266-270, https://doi.org/10.1109/IC2IE60547.2023.10331330.

[4] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), Amman, Jordan, 2019, pp. 1-6, https://doi.org/10.1109/ICTCS.2019.8923077.

[5] Mehrabi, Ali & Jolfaei, Alireza. (2022). Efficient Cryptographic Hardware for Safety Message Verification in Internet of Connected Vehicles. ACM Transactions on Internet Technology. 22. 1-16. https://doi.org/10.1145/3431499.

[6] Xiao, Jiongen& Liu, Yi & Zou, Yi & Li, Dacheng& Leng, Tao. (2024). An Efficient Elliptic Curve Cryptography-Based Secure Communication with Privacy Preserving for Autonomous Vehicle. Journal of Advanced Transportation. 2024. https://doi.org/10.1155/2024/5808088.

[7] Phatak, A., & Rao, V. S. (2023). Adaptive Security Mechanism for Vehicular Data Networks or Platform using Degree of Privacy. International Journal of Intelligent Systems and Applications in Engineering, 12(2), 594–598.

[8] Ahmer khan jadoon, Lincheng Wang, Tong Li, “Lightweight Cryptographic Techniques for Automotive Cyber security” volume 2018.https://doi.org/10.1155/2018/1640167.

[9] Specification defines the standard for vehicle data https://www.w3.org/TR/vehicle-data.

[10] C. Kaiser , A. Stockerl , G. Viscusi , A. Festl , P. Mörtl , M. Glitzne, “Quantified Cars An exploration of the position of ICT start-ups vs. car manufacturers towards digital car services and sustainable business models”, Virtual Vehicle Research Center.

[11] D. Coopersmith “The Data Encryption Standard and its strength against attacks”, IBM J RES, Vol 38 no. 3 1994. https://doi.org/10.1147/rd.383.0243.

[12] Seung-Jo Han, Heang-Soo Oh, “The improved Data Encryption Standard (DES) Algorithm” Jongan Park IEEE Transaction 1996

[13] Muzafer H, Mohamed Elhoseny, Mahmoud Mohamed Selim, and K. Shankar, “Data Encryption Standard for IoT Applications based on Catalan objects and Two combinatorial structure” IEEE Transaction 2020.

[14] KO-FENG LEE1, XIU-ZHI CHEN1, CHAO-WEI YU1, KAI-YI CHIN, “An Intelligent Driving Assistance System Based on Lightweight Deep Learning Models”, IEEE Vehicular Technology Society Section, Volume 10, 2022.

[15] Suresh Timilsina, Sarmila Gautam, “Analysis Of Hybrid Cryptosystem Developed Using Blowfish AndEccWith Different Key Size”, TECHNICAL JOURNAL Vol 1, No.1, July 2019, Nepal Engineers' Association, Gandaki Province, ISSN : 2676-1416.https://doi.org/10.3126/tj.v1i1.27582.

[16] V. Kaur and A. Singh, “Review of Various Algorithms Used in Hybrid Cryptography”, International Journal of Computer Science and Network December 2013, vol. 2, no. 6, pp. 157–173, 2013.

[17] A.P Shaikh, V. kaul, “Enhanced Security Algorithm using Hybrid Encryption and ECC,” IOSR Journal of Computer Engineering, vol. 16, Issue3, pp. 80-85, May 2014.https://doi.org/10.9790/0661-16348085.

[18] N. Garg and P. Yadav, “Comparison of Asymmetric Algorithms in Cryptography,” International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 1190–1196, 2014.

[19] T. Hoppe, S. Kiltz, and J. Dittmann, “Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-term Countermeasures”, Reliability Engineering & System Safety, vol. 96, no. 1, pp 111-25, 2011.https://doi.org/10.1016/j.ress.2010.06.026.