ECU To ECU Communication in Automotive Grade Processors and Security of Messages Exchanged

Moin I Gorikhan[1], Bhagyashri S Patil[2], Mrunali N Panhalkar[3], Kapila J Patil[4], Sushant Jadhav[5], Gujanatti Rudrappa[6], Harshal Mutkekar[7], Shreyas Anand[8], Nataraj Vijapur[9]

[1]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: moingorikhancr7@gmail.com

[2]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: bhagyapatil017@gmail.com

[3]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: mrunalipanhalkar2@gmail.com

[4]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: kapilapatil5@gmail.com

[5]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: 23sushant@gmail.com

[6]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: rudraguj@gmail.com

[7]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: harshalmutkekar7@gmail.com

[8]Department of Electronics and Communication, KLE Dr. M S Sheshgiri College of Engineering and Technology, VTU, Belgaum, Karnataka, India. E-mail: shreyasanand86@gmail.com

[9]Deparment of Electronics and Communication, RV Institute of Technology and Management (VTU) Bengaluru, India. E-mail: nvijapur@gmail.com

Abstract

An Electronic control unit (ECU) is small microprocessors in a vehicle's body which plays a major role in controlling a specific function. Vehicles recently may contain 80-100 ECUs or more, managing different functions in the vehicle like security and giving access to Passive safety measures such as airbags, as well as active safety features such as autonomous emergency braking, are all available. The various problems encountered by ECUs are because of loss of communication, incorrect protocol, memory checksum error and also by cause of illegal hacking. In this project inter and intra communication of vehicle is secured thorough encryption and decryption measure. Electronic Control Units (ECUs) create specific and telemetric data that is transferred across the vehicle's internal network. ECUs are low-resource devices with little resources to dedicate to data security. Threats to vehicle networks have recently surfaced, requiring the attention of the scientific community. We propose in this work to employ message transposition and then encrypt the transposed messages, which will assist to improve message security.

Keywords: Network security, ECU, Encryption, Decryption.

DOI: 10.47750/pnr.2022.13.S03.028

INTRODUCTION

ECUs (Electronic Control Units) are digital assets that interface with on-board systems. An ECU is an embedded system that controls electrical subsystems in a vehicle. It controls the fuel supply, air management, fuel injection fuel ignition, etc. In modern motor vehicles, around 80-100 ECUs are present. Electronic/engine Control Module (ECM), Power Train Control Module (PCM), Transmission Control Module (TCM), Brake Control Module (BCM or EBCM), Central Control Module (CCM), Central Timing Module (CTM), General Electronic Module (GEM), and control unit or control module are some of the different types of ECUs available. The construction of an ECU, among other things, requires both hardware and software as needed to accomplish the desired functions from that specific module.

Communication. All point-to-point contact in intra communication occurs between processes that belong to the same group. AES is used for encryption in the Inter Vehicle Communication module. To encrypt and decrypt traffic leaving and entering the node, the AES engine employs the shared key provided by the ECC subsystem

A point-to-point communication between processes in distinct groups is referred to as intercommunication. Each ECU executes the first session key generation procedure with the GECU in a predefined order in Intra Vehicle Communication, and the ECUs perform authentication and encryption using HMAC and AES. Both inter and intra communication uses the same syntax for point-to-point communication. Sender and receiver actions can both be performed using the same communicator.

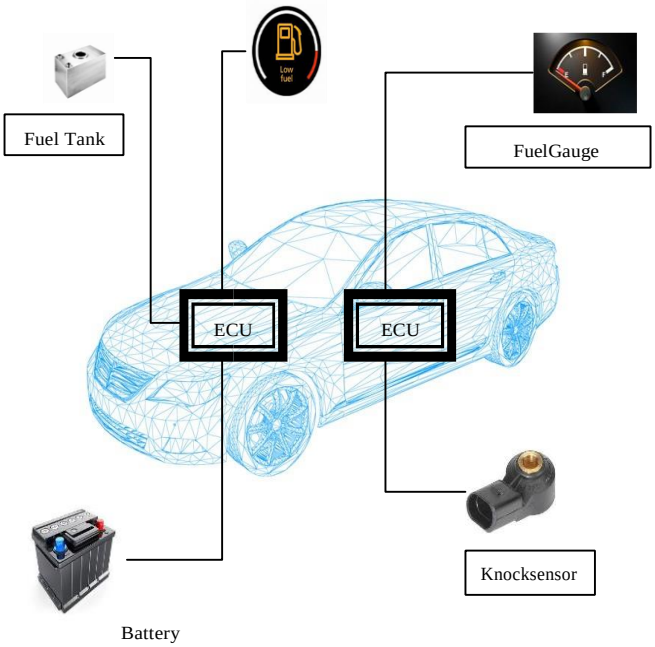

Fig. 1. Representation of Intra Communication

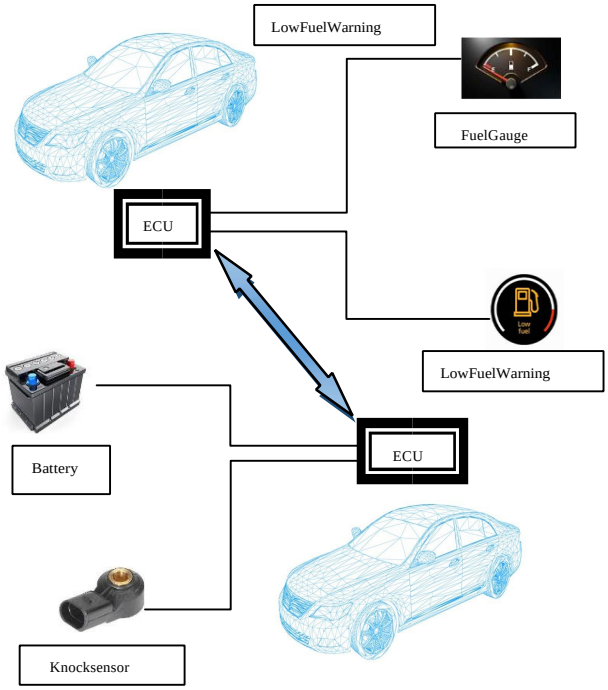

Fig. 2. Representation of Inter Vehicle Communication

ECU difficulties that result in poor performance or unexpected decreases in fuel economy or efficiency are frequently linked to on-board car computer issues or defective ECU issues. A faulty ECU can cause difficulty shifting gears in an automatic transmission, as well as jerking or halting that resembles transmission problems.

- Communication compromises/problems with ECUs:
- A control module memory checksum fault
- Incorrect communication protocol
- Loss of connection between the ECU and the Scanner.

The technique of converting plain text data into something that seems to be random and meaningless is known as encryption (cipher text). The conversion of encrypted text to plaintext is known as decryption. Asymmetric encryption is used to encrypt more than a tiny quantity of data. The encryption and decryption operations both employ a symmetric key. The key used to encrypt the data must be used to decode a particular piece of cipher text.

As a result, if one of the other ECUs is hacked, the assailant will be able to access and change data from other critical ECUs. The insufficiency of sensitive information is the main cause for this. Furthermore, if a critical ECU is compromised, an attacker may be able to modify the encrypted data.

LITERATURE SURVEY

Rohit Bhatia ET el. [1] published a paper work in which he discovered a novel voltage corruption tactic that leverages the capabilities of two compromised ECU's. CAN, VIDS mechanism is used.

S. Smys, Haoxiang Wang [2] published a paper work in which he proposed a concept of interconnecting smart vehicles and advancement in automotive automation. Block chain mechanism is used.

Geoffrey Spencer ET el. [3] published a paper work in which they p8resentedthe early stages of developing new hardware components for CAN connectivity in forest machinery The method employed is a presentation of the creation of new CAN bus electronic control units that enable communication between sensors and actuators and major machinery. CAN bus is one of the metrics used.

MU Han ET el. [4] published a paper work in which they proposed secure attributes isolated communication design for an ICV that inserts characteristics into ECUs in order to get illegal access. For ICV, an ECU access control mechanism has been created. ICV, ECU metric are used. ICV will work in autonomous contexts in the future.

Nan Zhang ET el. [5] he proposed He recommended that the Polar Research Centre at Jilin University in China create a novel Antarctic sub glacial drilling technique. The complete system is made up of surface, bore holes, and software subsystems. Metric here used is Glaciological instruments.

Murugesan Lakshmanan & Senthil Kumar Natarajan [6]

proposed a paper work on the security enhancement employing shortened message authentication code for CAN ECU authentication mechanism is presented. Mechanism used here is IDEA, CAN Algorithm is tested with Canoe software. Future research may be carried out for implementing the proposed ECU authentication scheme in real time embedded system hardware and real vehicles.

Ali Shuja Siddiqui ET el. [7] proposed the objective that demonstrates data security threats in automobile. Mechanism used here is Controller Area Network (CAN) bus. The metric employed here is a security framework that uses lightweight cryptographic primitives and proposes a hardware-based authentication mechanism called HSM.

Omid Avatefipour and Hafiz Malik [8] proposed a study in in-vehicle network communication protocol CAN bus & its corresponding vulnerabilities are introduced. CAN bus mechanism is used. Metric used here is CAN Bus protocol.

David SLIVKA ET el. [9] proposed a paper work in which free scale digital signal controller 56F8037 used and main subject. Metric used is CAN Bus.

Rudrappa B Gujanatti ET el. [10] proposed a paper on how to secure communication between ECUs (Electronic Control Units).Mechanism used here is RSA algorithm and elliptic curve cryptography. Metric used here is Timing analysis, Memory analysis. Future studies will look forward to maintaining track of the affected ECUs.

Basavarj Chougula et al. [11] proposed the use of communication between ECU for automatic parking system. The system also provided communication for providing reservation facilities for parking.

BLOCK DIAGRAM SENDER ECU

Fig. 3 represents the block diagram of communication between ECU's.

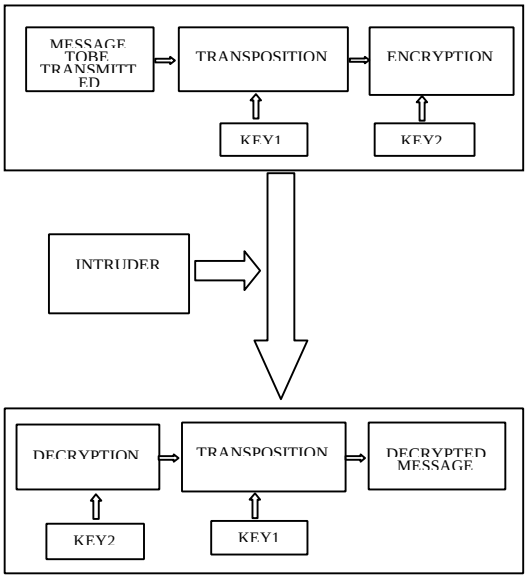

Fig. 3. Representation of Communication between ECU's

A. Sender ECU

In the sender ECU, the message is transmitted to the Transposition cipher. In the Transposition cipher the message is rearranged or the plain text is arranged in new order which uses key 1 for encryption. The encoded text/message from the transposition is encrypted using key2 where the plain text or message is encrypted in number using Nihilist cipher.

- Message to be encrypted: The message generated by the ECU based on the program written in the ECU.
- Transposition: Consists of writing the plain message in a table or grid. Then rearranging the columns of this table according to the given permutation
- Key1: Permutation key is a series of number which indicates in what order plain message is to be rearranged.
- Encryption: The transposed message is then Encrypted using Nihilist cipher, which further generates key2. It transforms the cipher into fractionated polyalphabetic cipher with numbers
- Key2: The key2 which is also a word and encoded in terms of number by Nihilist method. This key2 is added with the Encrypted message.

B. Intruder

Intruder is the one who is trying to gain the access to messages exchanged between ECU's. When the sender ECU sends the encrypted message to the receiver ECU, the intruder may attempt to access the encrypted message.

C. Receiver ECU

The encrypted message under goes decryption using Decryption method. The encrypted message is decrypted using key 2 in which the numbers are decrypted into plain text/messages using the Nihilist cipher. The decrypted message from the Nihilist cipher is decoded using key 2 using the transposition cipher. Then the decoded message is decrypted and we receive the decrypted message at the receiver end.

- Decryption: The Encrypted message undergo decryption using Nihilist cipher method .It is the same key2 with which the message is Encrypted, then the message is decrypted by subtracting this key2 from the encrypted message.
- Transposition: The decrypted message is to be transposed to get the required message using the key1.
- Decrypted message: After applying the different Decryption method, this is the actual message generated by the sender ECU.

METHODOLOGY USED FOR ENCRYPTION AND DECRYPTION

A. Transposition method for Encryption

Transposition is an initial encryption method which rearranges the plain text letters in different order. Transposition cipher is also known as columnar transposition, where the plain message is written in table or grid. Then based on the key generated the columns are rearranged. The key generated during this process is the permutation key.

Permutation key is the number which suggests that in what order the plain text has to be re arranged. The numbers will be under the length of the plain text, i.e., N. The columnar transposition put the plain text in the table of width N, row by row, to get the results as per the permutation key.

B. Nihilist Cipher

Nihilist Cipher is a first transposition cipher. It transforms the cipher into fractionated polyalphabetic cipher with numbers. It generates 5x5 key squares of alphabets which is required to encrypt the plain text. These 25 alphabets must be unique and each alphabet has it own coordinates. The alphabets of plain text are changed into number based on the coordinates in 5x5 square matrix. This number is added to the random key, which is also encoded into number. After addition the numbers will be in between 22 to 110. Hence by this method the total encryption is done.

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

EXPECTED RESULTS

In present scenario, since we are involving transposition and encryption together we are looking forward for high security of the messages which have been exchanged. Implementation of security mechanism for communication to be achieved. Secured communication is to be observed between the ECU's using the Encryption method identified. With the help of the Transposition and Nihilist encryption method we are able to encrypt & decrypt the messages.

A. Transposition method

Message generated by the ECU is transposed as shown below using the key1.

Example:
Plain text-" HELLO9"
Permutation key- 3, 4, 2, 5, 1, 6

Message H, e, L, L, O, 9
Key 1 3, 4, 2, 5, 1, 6
Transposed Message L, L,e,O,H, 9

Hence the encrypted cipher will be" LLe9HO" for "HeLLO9".

2. Plain text- "EnCrYpT"
   Permutation key- 1, 3, 4, 2

TABLE I. Sample Transposed Message

Message	E,n,C,r,Y,p,T
Key 1	1 , 3 , 4, 2
Transposed Message	E , n , C, r
	Y , p , T , 6

If the grid contains any void space, that void space or empty box is replaced by the letter x

Hence the encrypted cipher will be "EYnpCTr6" - for "EnCrYpT6"

B. Encryption method

The transposed method is encrypted by Nihilist method using key2.

The Nihilist Cipher generates 5 x 5 key squares of alphabets. The coordinates consist of digits which are obtained by considering row and column of the alphabets in 5 x 5 grids.

TABLE II. Table Type Styles

*	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

The letters of the plain text is marked with respect to the coordinates in the grid [row, column]

Example:

A is coded as 11 (1st row, 1st column), S is coded as 44(4th row, 4th column).

Plain text: "REPLACE"

This plain text can be encoded as 43, 15, 41, 32, 11, 13 and 15.

The encoded result of the plain text is added with the key which is also a word and encoded in terms of number by Nihilist method Example:

Let the key be "SYSTEMS", hence it is encoded as44, 54, 44,45,15,33 and 44

Therefore, the result encrypted cipher text will be given by adding these two encoded numbers as show below.

TABLE III. Table Type Styles

Plain text	**R**	**E**	**P**	**L**	**A**	**C**	**E**
Encode (plain text) letter	43	15	41	32	11	13	15
Key2	S	Y	S	T	E	M	S
Encoded (key2)letter	44	54	44	45	15	33	44
Encrypted message	87	69	85	77	26	46	59

The final encrypted message is 87698577264659

C. Decryption method

The encrypted message is subtracted from the encoded key result which is in term of number and the resultant number is divided in pair of digits.

This pair represents the row and the column of actual message in the grid.

TABLE IV. Table Type Styles

Coded message	87	69	85	77	26	46	59
Encode(plain text) letter	44	54	44	45	15	33	44
Subtractions	43	15	41	32	11	13	15
Letter in the grid	R	E	P	L	A	C	E

Hence here we get the actual message i.e. “REPLACE”

Transposition at the receiver end:

If the message's length is not a multiple of permutation, the grid's empty boxes are recalculated, as in encryption.

Example:

TABLE V. Sample Encryption and Decryption Of A Message

Column	3 , 1 , 2	**Actual columns**	1 , 2 , 3
Cipher text	N , L , E	**Plain text**	L , E , N
	H , G , T		G, T, H

RESULTS

The Fig. 4 shows the secured communication between ECUs, the model consists of two ECUs (Arduino), two Bluetooth that is one at the transmitter end and another at the receiving end. It has two display devices one is connected to sender ECU that displays the message that is to be encrypted and one is connected to the receiver ECU where the decrypted message is to be displayed.

Potentiometer is used to vary the contrast of the display.

There are four switches and four LEDs which acts as indicator.

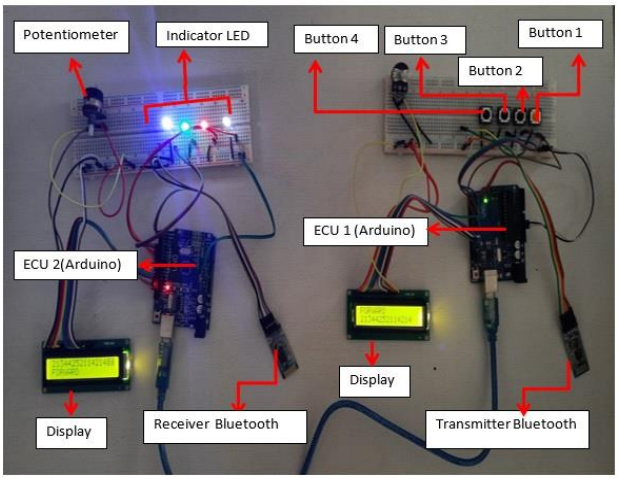

Fig. 4. Secured Communication between ECUs

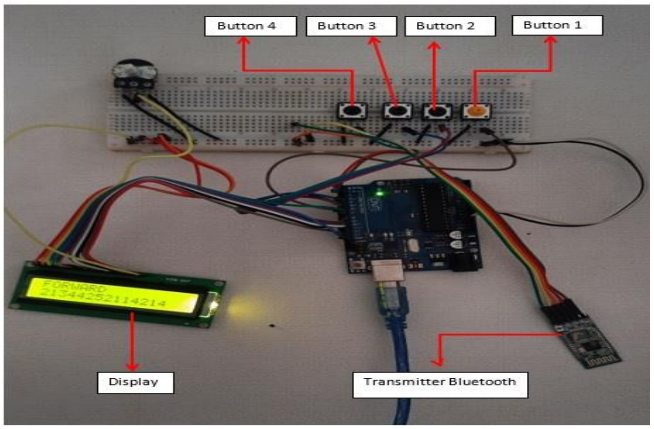

Fig. 5. Sender ECU

The Fig. 5 shown above is the transmitter model which consists of display, transmitter bluetooth and four switches. The message to be encrypted is displayed. In the sender ECU the message is encrypted and send to the receiver ECU.

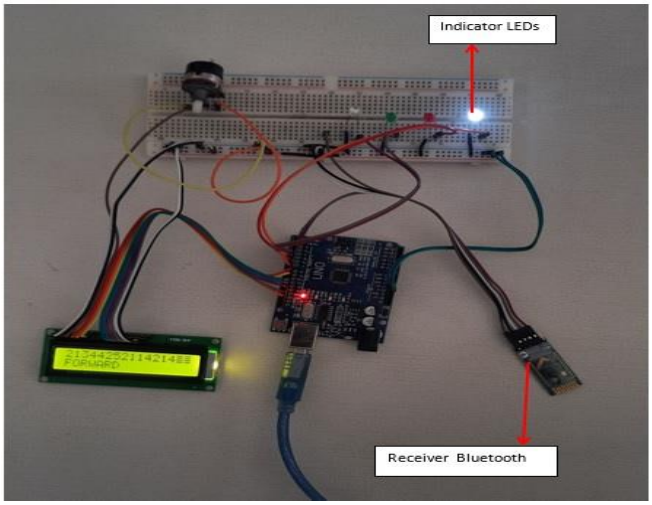

Fig. 6. Receiver ECU

The Fig. 6 shown above is the receiving model which consist of display, receiver bluetooth and four LEDs. The encrypted message send by the sender ECU is received and decrypted, and then the decrypted message is displayed. The LED's are used as indicators.

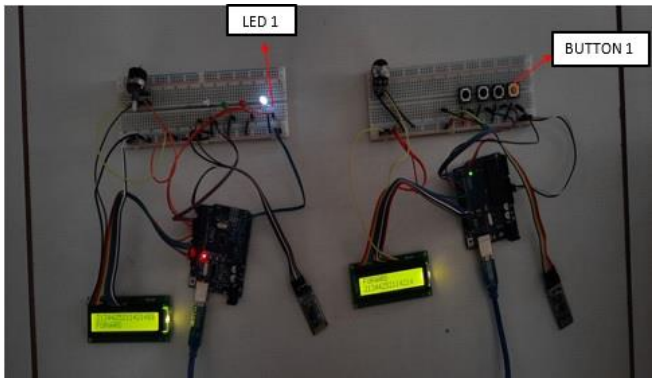

Fig. 7. Encryption of message "FORWARD" and Decryptionmessage indication

Fig. 7 shows the encryption of message "FORWARD" and Decryption of the message "FORWARD". When Button 1 is pressed the message will be encrypted and then it is transmitted to receiving ECU. And then the message is decrypted and displayed on LCD and as an indication "WHITE LED" Is blinked.

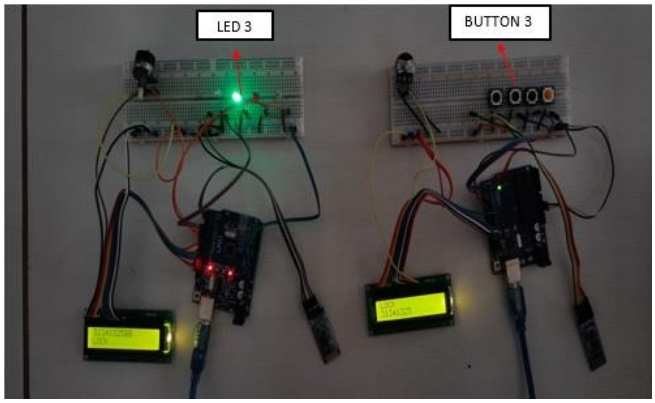

Fig. 8. Encryption of message "LOCK" and Decryptionmessage indication

Fig. 8 shows the encryption of message "LOCK" and Decryption of the message "LOCK". When Button 3 is pressed the message will be encrypted and then it is transmitted to receiving ECU. And then the message is decrypted and displayed on LCD and as an indication "GREEN LED" Is blinked.

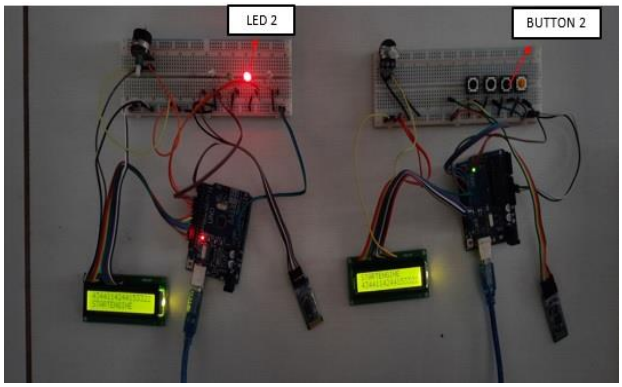

Fig. 9. Encryption of message "STARTENGINE" and Decryptionmessage indication

Fig. 9 shows the encryption of message "STARTENGINE" and Decryption of the message "STARTENGINE". When Button 2 is pressed the message will be encrypted and then it is transmitted to receiving ECU. And then the message is decrypted and displayed on LCD and as an indication "RED LED" Is blinked.

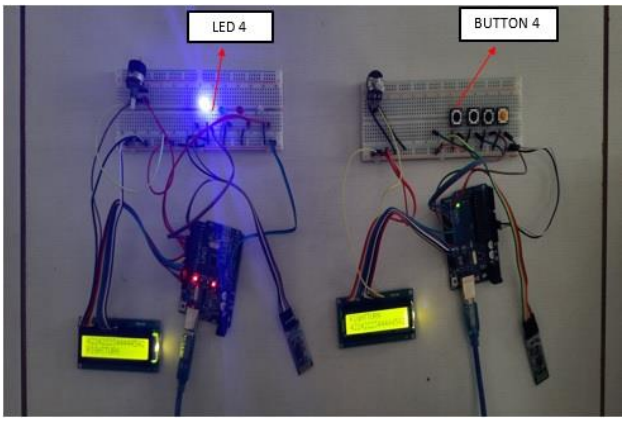

Fig. 10. Encryption of message "RIGHTTURN" and Decryptionmessage indication

Fig. 10 shows the encryption of message "RIGHTTURN" and Decryption of the message "RIGHTTURN". When Button 4 is pressed the message will be encrypted and then it is transmitted to receiving ECU. And then the message is decrypted and displayed on LCD and as an indication "BLUE LED" Is blinked.

CONCLUSION

We were successful in securing inter and intra vehicular communication, using Hardware system. The point-to-point communication between ECUs are secured by encryption and decryption methods. Here we are trying to use Transposition cipher and Nihilist cipher for encryption and decryption of the messages. Where the message in transposition cipher is rearranged. The arrangement of plain message is determined by the permutation key, this encoded plain text or message is encrypted using Nihilist cipher in

which the message is converted into numbers using the key generated in nihilist. Therefore, required plain text is "LENGTH" cipher. This transmitted message is decrypted by the decryption method using nihilistic cipher which decodes the number into alphabet using the key generated and in this decrypted message is arranged with the help transposition cipher and we receive the message which is send by the sender ECU. This will also aid in the security upgrade of ECU communication by keeping track of compromised ECUs and the technique by which they were compromised.

ACKNOWLEDGMENT

We thank Vision Group of Science and Technology (VGST) for providing the funds (under KFIST-L1) to establish the lab (titled "Establishment of IoT and Artificial Intelligent Lab for Problem Based Learning") which will be helpful in implementation of the proposed methodology.

REFERENCES

Rohit Bhatia, Vireshwar Kumar, KhaledSerag, Z. BerkayCelik, Mathias Payer and DongyanXu, "Evading Voltage-Based Intrusion Detection on Automotive CAN," Network and Distributed System Security Symposium (NDSS). 2021, pp.1-17.

S. Smys and Haoxiang Wang, "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework," Journal of Artificial Intelligence and Capsule Networks, 2021, Vol-03, issue-02, pp. 90-100, DOI: https://doi.org/10.36548/jaicn.2021.2.002

Geoffrey Spencer, FrutuosoMateus, Pedro Torres, RogérioDionísio and Ricardo Martins, "Design of CAN Bus Communication Interfaces forForestry Machines," 2021, vol-10, issue-144, pp1-15, DOI: https://doi.org/10.3390/computers10110144

Mu Han, Alian Wan, Fengwei Zhang, and Shidian Ma, "An AttributeIsolated Secure Communication Architecture for Intelligent Connected Vehicles," IEEE Transactions on Intelligent Vehicles, December 2020, VOL. 5, issue-4, pp.545-555.

Nan Zhang, PavelTalalay, Jingbiao Liu, Xiaopeng Fan, Qingpeng Kong, Haibin Yu, Yunchen Liu, Benkun Liu2, Da Gong, Xingchen Li, Wei Wu, Jialin Hong and Mikhail Sysoev, "Antarctic subglacial drilling rig: Part IV. Electrical and electronic control system," Annals of Glaciology, 2020, vol-62, issue-84, pp. 34–45. DOI: https://doi.org/10.1017/aog.2020.40

Murugesan Lakshmanan and Senthil Kumar Natarajan, "Security Enhancement in In-vehicle Controller Area Networks by Electronic Control Unit Technology", 2019, Volume 22, issue 3– 4, pp.228–243.

Ali ShujaSiddiqui, YutianGui, Jim Plusquellic and FareenaSaqib, "A Secure Communication Framework for ECUs," Advances in Science, Technology and Engineering Systems, 2017, Vol. 2, issue-3, pp. 1307-1313, ASTESJ ISSN: 2415-6698.

OmidAvatefipour and Hafiz Malik, "State-of-the-Art Survey on InVehicle Network Communication "CAN-Bus" Security and Vulnerabilities," IJCSN - International Journal of Computer Science and Network - 2017, Volume 6, Issue 6, pp.720-727, ISSN (Online): 2277-5420

David Slivka, Petr Palacky, Petr Vaculik and Ales Havel, "Electric Vehicle Control Units Communication," Advances In Electrical And Electronic Engineering,2012, Volume: 10, Issue- 1 pp.17.

Rudrappa B Gujanatti, Suhasini Kharka, Arsiya Peerzade, Sushant S Jadhav, Shridevi Mallayyanavarmath, "Securing the Communication between Automotive Grade Processors," ISSN: 2237-0722,Vol.11 No.3 (2021), www.revistageintec.net.

Basavaraj Chougula, Arun Tigadi, Sushant Jadhav, Gujanatti Rudrappa, "Automatic Smart Parking and Reservation System Using IOT," Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020), Pp-107-113.

Ibrahim, S. (2022). Commutativity of high-order linear time-varying systems. Advances in Differential Equations and Control Processes, 27, 73-83.