ACTA SCIENTIAE

ISSN: 2178-7727
DOI:

10.17648/acta.scientiae.6369

MATHEMATICAL ANALYSIS OF ADAPTIVE CRYPTOGRAPHIC COMMUNICATION & CAT-BOOST BASED INTRUSION DETECTION IN IOV

[1]R.Anitha Jyothi
Department of Mathematics & Statistics
VFSTR Deemed to be University, Vadlamudi,
University,Vadlamudi,
Guntur, India.
[1]anitha.suryadevarg@gmail.com
Orcid id:0009-0002-2224-3022

[2*]P.Siva Prasad.
Department of CSE,SOCI
VFSTR Deemed to be

Guntur, India.
[2*]pusapatisivaprasad@gmail.com
Orcid id: 0000-0002-2789-7431
*) Corresponding author:
pusapatisivaprasad@gmail.com

Abstract—The advanced computing technologies such as cloud computing, IoT, IoV, and machine learning create vast amounts of information that require efficient, reliable, and prompt processing. The use of the IoV technology becomes essential since it allows establishing communications between the vehicle and roadside infrastructure.
Nonetheless, IoV communication networks are highly exposed to security vulnerabilities due to their decentralized architecture. Such threats as malicious vehicles, data injection attacks, and others can significantly influence the operation of the network and its users. To tackle the problem, the present research paper offers an architecture for secure communication based on trust management and hybrid encryption. Considering the idea of the hybrid encryption algorithm, both of the algorithms should be taken into account, as both of them are efficient in their specific areas. For instance, since the RSA algorithm may be employed for user authentication and key exchange, the efficiency of the AES algorithm will be helpful in encrypting the data quickly. Moreover, the Cat-Boost classifier should be utilized in our study, in order to create a novel IDS that will detect all malicious behaviour exhibited by vehicles and traffic problems according to the UNSW-NB15 dataset. We found out that the efficiency of our model equals 93.57
Some of the accomplishments which have been recorded using this suggested method have included the application of machine learning algorithms to analyse the data sets that include the UNSW-NB15 data set, which were analysed using the Cat-Boost technique, and which yielded an accuracy of 93.57
On the other hand, IoV -based networks suffer from many security issues due to their open and decentralized structure. There is no central entity managing the communications in this network. Hence, malicious vehicles can inject false data into the system, affect traffic behaviour, and even pose threats to the system as a whole by pretending to be some of the legitimate nodes. Thus, data protection and authentication have become crucial concerns that need to be addressed properly.

Key words—IoV, Hybrid Encryption, RSA, AES, Cat-Boost, Intrusion Detection System, Cybersecurity, Machine Learning

I. INTRODUCTION

The Internet of Vehicles (IoV) is a sophisticated model of communication that allows for interactions among vehicles, roadside infrastructures, and central systems through vehicular

ad-hoc networks. The Internet of Vehicles is regarded as one of the key enabling technologies in building intelligent transportation systems and smart cities. It enables the exchange of essential information about roads, accidents, congestions, and optimal routes in real-time. This kind of constant communication leads to improved road safety, traffic efficiency, and driving experiences. Nevertheless, the openness and dynamism of IoV networks make it highly vulnerable to cyber-attacks. With wireless communication in IoV networks, eavesdropping, data manipulation, replay attacks, and spoofing become common risks. The presence of malicious entities in IoV networks can send erroneous information to misguide other vehicles. For example, notifications regarding fake accidents or traffic could result in unnecessary congestion or wrong routing. Other than security attacks, the communication networks for Internet of Vehicles include data exchange that includes personally identifying information, thus presenting considerable privacy issues.

The current designs of vehicular communication systems use centralized cloud-based approaches. Though scalable and capable of storing information, these systems are characterized by high latency, since the distance of the communication path between vehicles and cloud servers is usually quite big. For this reason, they cannot be used efficiently for accident warnings, emergency brakes, and other activities which require immediate reaction from vehicles to avoid accidents.

As far as the methods of security used now are concerned, most of them are based on cryptographic techniques that concentrate on either encrypting or authenticating messages. Therefore, in addition to being inefficient, the security provided by these systems does not allow for addressing all issues, namely, ensuring both security and efficiency. Besides, no efficient trust assessment procedures are introduced into the system under discussion.

Hence, there is an urgent need for creating a system which would ensure reliable, low-latency, and safe communications. In this context, it becomes necessary to develop a system in which trust-based node evaluation combined with hybrid encryption techniques would be applied. By doing this, the security level of the entire system will increase significantly, since malicious vehicles can easily be detected and isolated from the system.

A. *Motivation*

Due to the fast growth of intelligent transportation systems and smart cities, the need for secure communication in the Internet of Vehicles (IoV) becomes more acute. Vehicles share the information about the current traffic state, accidents, road situations, and routing options at all times. Such exchange is essential for ensuring safety and comfort in driving.

At the same time, the IoV environment is highly dynamic and open since the vehicles can freely join and exit the network. Therefore, such an architecture raises the problem of protection against multiple potential attacks such as false dissemination, Sybil attacks, impersonation, and data tampering. A malicious vehicle may spread inaccurate information, thereby putting the drivers in danger.

Besides, a lot of IoV solutions use centralized cloud infrastructures to store and process data. While this architecture offers good scalability and storage opportunities, it introduces communication delay caused by data transfers over long distances. This delay may be fatal in case of emergency situation such as an accident warning.

This means that there is a need to develop a reliable communication protocol that is both secure and efficient. This gives the motivation for proposing a communication solution that incorporates trust and hybrid encryption methods.

B. *Related Work*

A number of research studies have attempted to solve the security issues in IoV networks through diverse techniques. For instance, trust-based schemes have been employed widely to

assess the behavioural patterns of vehicles and distinguish any malicious node based on a set of parameters including direct interaction, indirect feedback, and past behaviour. On the other hand, machine learning techniques have been adopted to enhance the precision of evaluating trust based on analysing huge amounts of data and detecting anomalies. Moreover, anomaly detection through data fusion is applied for the same purpose, where deep learning algorithms can recognize sophisticated attacks.

Block chain technology has been adopted for providing decentralized security, data integrity, and transparency in IoV, and explainable artificial intelligence has been applied for enhancing trust and improving interpretability of decisions.

However, all these technologies suffer from some weaknesses; trust evaluation does not guarantee securing the transmitted data, while encryption techniques cannot detect any malicious nodes. Also, many of these schemes require high computational effort and introduce a significant delay which makes them inappropriate for IoV applications.

These limitations indicate a clear gap in the field which needs to be filled by a combination of trust evaluation and encryption techniques.

C. *Contributions*

Contributions made by this study are listed below:

- Trust based evaluation model which evaluates the behaviour of vehicles using various parameters for detection of malicious nodes in IoV networks.
- Hybrid encryption schemes (RSA + AES), where RSA scheme is used for secure and reliable authentication and key exchange while AES scheme is used for efficient data encryption.
- A low-latency of communication approach that aims at reducing the delay of compared to the reasonable approaches using cloud-based models.
- An efficient approach with respect to issues of security and performance.
- Combined emphasis on both security and performance problems since most of the previous literature has considered each of these independently.

D.*Paper Organization*

The remaining sections of this paper are structured as follows:

In Section II, the purpose of the work being suggested and its objectives will be identified. Section III will contain a literature survey in the field of IoV security, trust management, and encryption techniques and their limitations.

Section IV will explain the existing IoV frameworks and models and the way they operate, their classification, and the problems associated with them. In Section V, the working process of the proposed solution will be explained.

In Section VI, the basic concepts and assumptions that form the basis of the system will be introduced. In Section VII, the suggested methodology will be described, which will include the use of trust evaluation within the hybrid encryption.

In Section VIII, the performance analysis of the proposed system will be presented, and its conclusions will be outlined in Section IX. Further information about the proposed system can be found in Section X.

The strengths and weaknesses of the proposed system, along with the security analysis, will be presented in Sections XI and XII, respectively. The results will be discussed in Section XIII, while the conclusions will be drawn in Section XIV.

II. OBJECTIVES

The main objectives of this work are as follows:

- For studying contemporary computing systems such as **cloud computing, Internet of Things (IoT), Internet of Vehicles (IoV), and machine learning** producing huge amounts of data and necessitating high computing power.
- For exploring the features of IoV systems like **handling huge data, communication in real time, and resource sharing** among cars and infrastructures.
- For analysing the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication system and assessing the potential security risks associated with data transmission, including both inside attacks and outside attacks.
- For proposing and implementing a trust-based scheme that evaluates the behaviour of vehicles to enable successful identification of malicious vehicles.
- For calculating trust based on direct trust, indirect trust, and role-based trust to improve the security level of IoV systems.
- To compensate the shortcomings of existing cloud-based schemes, especially for high latency of cloud-based schemes in real-time applications, and for examining effective communication schemes.
- For discussing the constraints of the existing machine learning schemes, especially in terms of huge datasets required for learning, and for examining how cloud or distributed computing helps in solving such problems.
- For devising a secure and efficient communication scheme by overhanging the hybrid encryption schemes, such as RSA and AES.

III. LITERATURE SURVEY

Recently, numerous studies have tried to deal with security and reliability problems of IoV communication by applying current technological achievements.

Thus, when conducting their study, Alalwany et al. in 2024 identified possible risks associated with the communication channel using the IoV technology and suggested that the assessment of the trust factor can be one of the best techniques for identifying any malicious attacks [1]. [Online] Available.

Secondly, the development of the security management system based on the trust factor suggested by Siddiqui et al. in 2023 uses machine learning algorithms. In particular, the researchers' contribution is in the use of multiple trust metrics for differentiation of malicious nodes [2]. [Online] Available

In addition, Sun et al. in 2022 applied the algorithm of machine learning in data fusion to guarantee the security of IoV communication. Nevertheless, because of the big data problem, the proposed model encounters certain challenges during its application [3]. [Online] Available

Another approach to IoV security based on machine learning is suggested by Khan et al. in 2025 when working on an IDS for detecting complex attacks [4]. [Online] Available

Finally, Alohali et al. in 2025 developed a malware detection system using explainable AI and IoV technologies [5]. [Online] Available

A trust management framework based on reinforcement learning in conjunction with block chain was proposed by Shamili et al., which addresses issues of security, integrity, and decentralization but at the same time raises the level of computational complexity [6]. [Online] Available

All the above research shows that current systems concentrate either on enhancing the security or increasing the efficiency of the communications within IoVs. There remains a necessity to develop a single system ensuring both properties.

A. Advantages

The current techniques have been found capable of detecting malicious nodes in the network, thus ensuring improved reliability. Additionally, these approaches provide secure communication among entities by ensuring confidentiality and integrity of the transmitted data.

B. Limitations

These schemes, however, pose problems due to their low efficiencies caused by high latency in processing the messages. Moreover, they involve heavy computation processes, hence making them inefficient when implemented in systems with limited resources.

C. Research Gap

While many researchers have proposed efficient algorithms for trust management techniques as well as for hybrid encryption schemes, an efficient combination of both approaches has not yet been suggested.

Despite that, according to the results obtained from recent researches, it is seen that gradient boosting techniques such as Cat-Boost have shown their superiority to classifiers when it comes to intrusion detection since Cat-Boost is capable of handling categorical input data without overfitting. That is why Cat-Boost can be used within the IoV security model.

IV. EXISTING SYSTEM AND MODELS IN IOV SECURITY

Internet of Vehicles (IoV) is an emerging field where considerable attention has been drawn by researchers because it enables real-time communication between vehicles and roadside infrastructure. Several models/architectures have been suggested for achieving better security, reliability, and efficiency in communications between various components of IoV. Nevertheless, almost all proposed solutions have focused only on some particular aspects of this issue.

A. Classification of Existing Models

The existing approaches that assure security in the IoV can be grouped as follows:

1) Trust-Based Approaches: In these schemes, the nodes' behaviour inside the network is analysed using certain parameters, such as direct trust, indirect trust, and reputation trust. The trust level of each vehicle is determined by the following equation:

$$T = \alpha T_d + \beta T_i + \gamma T_r \qquad (1)$$

Where T_d refers to direct trust, T_i represents indirect trust, and T_r is role-based trust. Despite being beneficial in detecting malicious nodes, these approaches cannot guarantee the security of the transferred data.

2) Machine Learning Approaches: The machine learning approaches make use of classification and clustering approaches for detecting anomalies in the network. Although these approaches attain better accuracy rates, they require additional computation.

3) Blockchain Approach: Blockchain methodology uses a decentralized model via block chain technology. 4) Cryptography Approach: Cryptography approach employs cryptographic algorithms such as RSA and AES to offer encryption services for transferring data. Key Generation:

$$n = pq$$
$$\phi(n) = (p-1)(q-1)$$

Encryption:

$$C = M^{e} \bmod n$$

Decryption:

$$M = C^{d} \bmod n$$

AES is employed for encryption purposes by employing various transformations. Nonetheless, despite providing security and authentication, these methods cannot protect against malicious nodes.

5) Edge and Cloud Computing Model: Cloud computing architectures are scalable and have the capability of storing data whereas the edge computing techniques reduce latency through local processing. The cloud computing architecture has the issue of high delay, while edge computing does not offer any security features.

6) Hybrid Approach: Hybrid methods try to integrate all the above approaches of trust, cryptography, and routing. Such methods work efficiently than other approaches; however, they are complex and inefficient.

B. Workflow of Current Scheme

The current IoV network uses a series of steps that involve authentication, encryption, trust evaluation, and malicious node detection. However, they function independently, causing inefficiencies in the workflow.

Step 1: Identification of Vehicles with RSA RSA-based cryptography is used to authenticate each vehicle.

Step 2: Encryption of Data with AES Once the authentication step is completed, data is encrypted with AES and transmitted. AES works on:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

Step 3: Determination of Trust Values The model determines the trust values by:

$$T = \alpha T_d + \beta T_i + \gamma T_r$$

Step 4: Detection of Malicious Nodes For the trust value being less than the threshold, the nodes can be considered malicious:

$$T < T_{threshold} \qquad (3)$$

C. Comparison of Existing Models

TABLE I
COMPARISON OF EXISTING IOV SECURITY MODELS

Model	Security	Latency	Limitation
Trust-Based	Medium	Low	No encryption
ML-Based	High	High	Computational cost

Blockchain	High	High	Scalability issues
Cryptography	High	Medium	No attack detection
Cloud-Based	Medium	High	High delay
Edge-Based	Medium	Low	Weak security

D.Limitations of Existing System

In spite of the utilization of state-of-the-art technologies, currently available IoV solutions face multiple drawbacks:

- Latency associated with cloud computing
- Computational complexity in RSA and ML algorithms
- Insufficient coordination among authentication, cryptography, and trust management
- Poor identification of suspicious devices on a timely basis
- Lack of compromise between secureness and efficiency

E. Research Gap

Based on the review of prior research presented above, it becomes clear that the current systems are not capable of addressing both aspects of trust assessment and hybrid cryptosystems, ensuring highly efficient communication at the same time.

V. SYSTEM FLOW

In this work, a simple and secure communication process is designed for IoV networks. Whenever a vehicle enters the network, it first needs to register itself. During this process, a unique ID is given to the vehicle, which will be used for further communication.

After registration, the vehicle sends a request to communicate. The verification process of the car involves authentication through RSA algorithm where keys will be generated and shared in such a way that only the authentic cars can enter the system.

After the car has been authenticated, the next step is to create a communication channel between the system and the car. When transmitting information, AES encryption algorithm will be used since it runs fast. So, RSA is mainly used for key exchange, while AES is used to protect the actual data.

Apart from security, the system also looks at the behaviour of each vehicle. A trust value is calculated based on its previous activities. If the value is high, the vehicle is allowed to continue communication. If the calculated trust value is low, the vehicles treated as suspicious, and in some cases, it may be marked as malicious. This decision-making process is not done arbitrarily but rather takes into consideration the behavioural pattern of the vehicle involved including the communication ability and adherence to the network protocol.

The identified malicious vehicle cannot communicate in the future. Simply put, the network avoids communicating with those malicious vehicles as much as possible to limit any threat. This is an important step taken in securing the message by avoiding any malicious attack.

The message delivered by the sender is verified upon receipt by the system. Verification involves checking whether the message has been tampered with in any way or whether it has been generated by unauthorized individuals. False information included in the message, even in the slightest, will affect the efficiency of the network.

The system supports both the Vehicle-to-Vehicle and Vehicle-to-infrastructure communications. Once the message is received, the encryption will be reversed to get back the plain text. After getting the text, validation of the sender is done by the receiver.
In summary, the technique emphasizes the importance of balancing the issues of security and trust in the network. Unlike in cases that utilize encryption alone, this approach also takes into consideration the nature of the behaviour of vehicles. What is more, the trust values are dynamic and keep varying from time to time depending on the activities taking place.

VI. FUNDAMENTAL CONCEPTS AND SYSTEM BACK GROUND

A.IoV Communication Framework

Internet of Vehicles (IoV): It is an advanced mode of communication system that establishes communication between vehicles and infrastructures for the establishment of intelligent transportation systems. The Internet of Vehicles

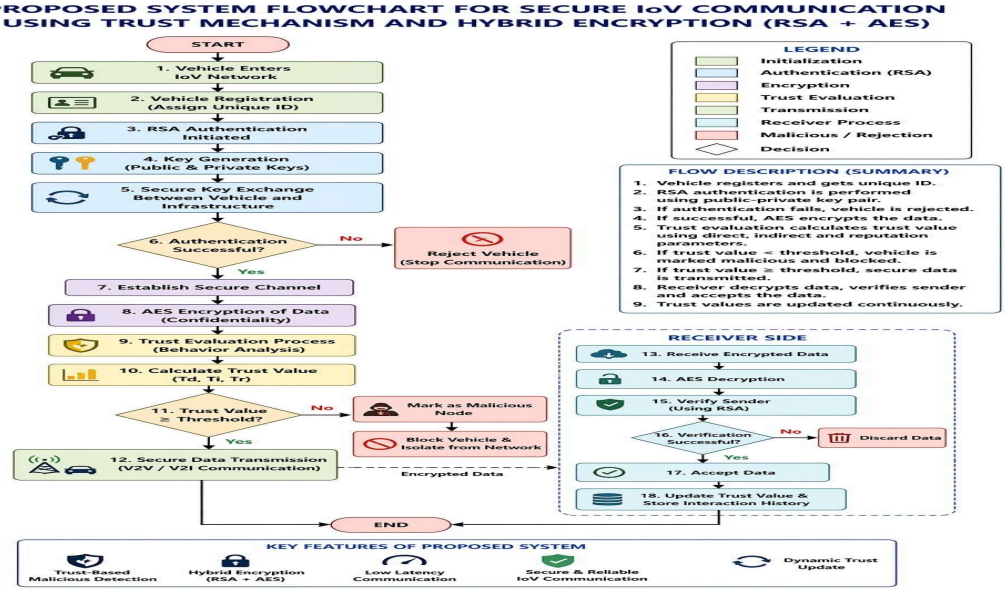

Fig. 1. Proposed System Architecture for Secure IoV Communication

provides facilities to exchange real-time data such as traffic conditions, accidents, road conditions, and many other data.
Vehicle to Vehicle (V2V) Communication: In this communication, vehicles exchange information regarding their position, direction, and speed among each other in order to prevent any accident.
In V2I communication, vehicles connect with the roadside units (RSU), traffic signals, and controls in order to manage traffic. Low Latency Communication: IoV systems have to establish low latency communications as IoVs need timely response during any emergency condition like accident.

B. Trust Evaluation Mechanism

For evaluating the trustworthiness of the vehicles in the IoV system, a trust mechanism is utilized for evaluating the behaviour of the vehicles.
The trust value is calculated as:

$$T = \alpha T_d + \beta T_i + \gamma T_r \quad (4)$$

Where:

- T_d = Direct trust (based on direct interactions)
- T_i = Indirect trust (based on recommendations)
- T_r = Role-based trust (based on vehicle role)
- $\alpha + \beta + \gamma = 1$

Decision condition:

$$T \geq T_{threshold} \Rightarrow \text{Trusted Node} \quad (5)$$

$$T < T_{threshold} \Rightarrow \text{Malicious Node} \quad (6)$$

It helps in identifying any malicious node and improves reliability.

C. Encryption Techniques

Encryption becomes necessary to maintain data privacy. RSA Algorithm (Asymmetric Encryption): This algorithm is used for authentication and key exchange.

$$n = p \times q \quad (7)$$

$$\phi(n) = (p-1)(q-1) \quad (8)$$

Encryption:

$$C = M^e \bmod n \quad (9)$$

Decryption:

$$M = C^d \bmod n \quad (10)$$

AES Algorithm (Symmetric Encryption): AES encryption is done by transformations like:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

High-speed and effective data protection are achieved by AES.

D. Threat Model and Challenges

IoV can be targeted for different types of attacks because of communication being open in nature.

- **Interception of Data:** Accessing data by someone unauthorized
- **Injection of Fake Messages:** Spreading false data about accidents etc.

E. Comparative Analysis of Key Components

TABLE II
COMPARISON OF KEY IOV COMPONENTS

Component	Purpose	Advantage	Limitation

Trust Model	Node Evaluation	Detects attacks	Needs accurate data
RSA	Authentication	Strong security	High computation
AES	Encryption	Fast processing	Key management needed
V2V/V2I	Communication	Real-time data	Security risks

F. Problem Context

Although trust-based models and encryption methods are used, there are some issues that the IoV communication systems still encounter.

- The lack of integration between trust and encryption
- The difficulty in achieving both latency and security simultaneously
- Poor node identification

These challenges emphasize the necessity to implement an effective framework for IoV secure communication.

VII. PROPOSED METHODOLOGY

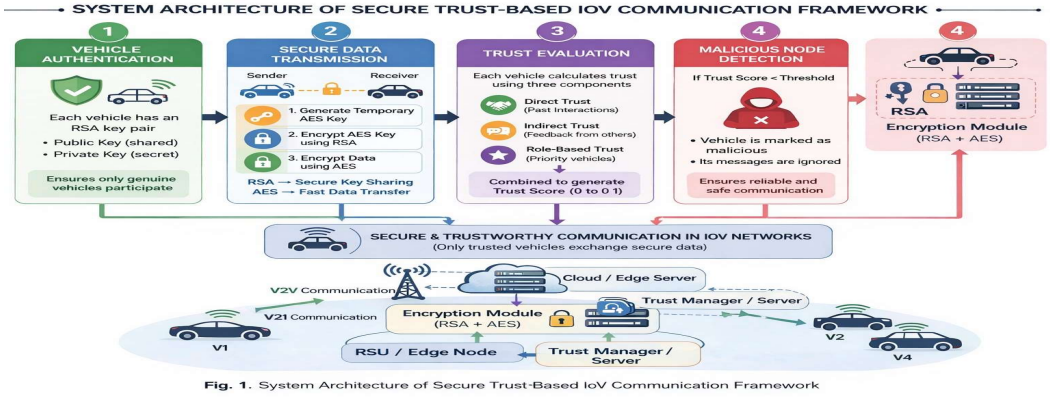

Fig. 1. System Architecture of Secure Trust-Based IoV Communication Framework

Fig. 2. Proposed System Architecture for Secure IoV Communication

A. Problem Model

The IoV network comprises automobiles communicating in V2V and V2I modes. Because of its **openness and dynamism**, the network is extremely prone to malicious attacks, spoofed message insertion, and tampered data.

In response to these issues, a **secure and effective communication framework** must be established, which will guarantee:

- Verification of the automobiles
- Security of the transmitted data
- Discovery of the malicious nodes
- Efficient communication latency

This solution combines **RSA for verification, AES for encryption, and trust evaluation of the nodes.**

B.RSA Algorithm for Authentication

RSA is used to provide security in authentication and key exchange.

Key Generation:

$$n = p \cdot q$$

$$\phi(n) = (p-1)(q-1)$$

Public Key: (e,n)

Private Key: (d,n)

Encryption:

$$C = M^e \bmod n$$

C. AES Algorithm for Encrypted Communication:

The AES algorithm is used to encrypt data in an efficient way.

AES Encryption Steps:

- SubBytes - Substitution
- ShiftRows - Permutation
- MixColumns - Transformation
- AddRoundKey - Key Addition

D. Trust Evaluation Model:

For the evaluation of the trustworthiness of each vehicle, the trust value for each is evaluated using an equation that combines direct trust, indirect trust, and role-based trust with the following formula:

$$T = \alpha T_d + \beta T_i + \gamma T_r \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (11)$$

Where $\alpha + \beta + \gamma = 1$.

1) ***Direct Trust (T_d):*** The calculation of the trust value of direct trust is made with the help of previous experiences of interaction.

$$T_d = \frac{\text{Number of Successful Interactions}}{\text{Total Interactions}} \quad (12)$$

2) ***Indirect Trust (T_i):*** Indirect trust comes from the recommendation from neighbouring vehicles, and is computed as follows:

$$T_i = \frac{1}{N}\sum_{k=1}^{N} R_k \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

Where R_k is the recommendation score and N is the number of vehicles.

3) ***Role-Based Trust (T_r):*** The computation of the role based trust considers the priority in terms of the vehicle type:

$$T_r = \begin{cases} 1.0, Emwrgency\ vehicles \\ 0.8, PublicTransport \\ 0.5, \text{Re}\, gularVehicles \end{cases} \quad \ldots\ldots\ldots\ldots\ldots (14)$$

4) ***Trust Decision Rule:***

$$T \geq T_{\text{threshold}} \Rightarrow \text{Trusted Node} \ldots\ldots\ldots\ldots\ldots\ldots (15)$$

$T < T_{threshold} \Rightarrow$ Malicious Node……(16)

E. System Work flow:

The proposed system uses an integrated approach:

- Vehicle joins IoV network
- Authentication with RSA
- Key exchange with security
- Encryption with AES
- Trust value calculation
- Detection of malicious nodes
- Data transmission with security

Unique Feature: Unlike other systems, all the parts work in an integrated fashion.

F. Performance Comparison:

TABLE III
COMPARISON OF EXISTING VS PROPOSED SYSTEM

Parameter	Existing System	Proposed System
Security	Medium	High
Latency	High	Low
Authentication	Separate	Integrated
Attack Detection	Weak	Strong
Efficiency	Moderate	High

G. Analysis:

The proposed system improves IoV communication by:

- Providing strong security using hybrid encryption
- Reducing latency through efficient processing
- Detecting malicious nodes effectively
- Ensuring reliable and real-time communication

VIII. IMPLEMENTATION OF THE HYBRID SYSTEM AND DISCUSSION

A. Algorithm Setup:

For the implementation of the suggested approach, the following were used: Python programming language, alongside libraries like Pandas, NumPy, Scikit-learn, and Catboat. UNSW-NB15 data set for training the model for detecting intrusive nodes in the IoV networks. In the hybrid approach proposed, a combination of RSA and AES cryptographic methods is suggested for intrusion detection through machine learning. RSA is used for user authentication and key exchange; AES is used for encryption of data in real time. catboat classifier is incorporated into the scheme to distinguish between normal and malicious data packets.

B. Data Preparation:

This is just an example of the processes that we carried out on our dataset while performing the pre-processing stage:

- Removal of the negative values (-)
- Treatment of missing values

- Label encoding for categorical features (for instance protocol type, services, and states, amongst others)
- Feature selection -
- Stratification of training and test data sets these are necessary data pre-processing tasks.

C. Hybrid Encryption Mechanism:

The hybrid encryption technique helps in achieving a secure communication process:
RSA (Asymmetric Algorithm) It is used for authentication and key exchange among vehicles where both sender and receiver have their own public and private keys. In this method, the AES key is encrypted by using the RSA public key of the receiver.
AES (Symmetric Algorithm) It allows fast data encryption and decryption.

Steps Involved in Hybrid Mechanism:

- Generation of session key at the sender's end
- Encryption of session key by using RSA
- Encryption of message/data by using AES key
- Decryption of session key by using RSA
- Decryption of message/data by using AES

Thus, here the speed of AES encryption technique along with security provided by RSA algorithm reduces the latency.

D. Ensemble Learning Approach:

Selection of the above-described approach depends entirely on the effectiveness of the application of Cat-Boost technology for working with categorical values and the accuracy of its predictions when compared to other methods of machine learning. The following is a benefit that arises from the use of Cat-Boost technology:

- Accuracy of classification tasks resolution.
- Efficiency regarding the process of generalization.
- No overfitting.
- Efficiency of data processing concerning the resolution of cybersecurity-related issues.
- Efficiency regarding the detection of malware.

From the perspective of efficiency metrics, it needs to be stated that Cat-Boost proved to outperform several machine-learning algorithms, including XG-Boost and Random Forest.

E. Operation Flow Chart of the System:

The suggested system works in the following way:

- Gathering of input values from the vehicle to IoT
- Authentication of the vehicle using RSA encryption technique
- Exchange of keys for AES encryption
- Transfer of data among nodes using AES encryption
- Calculation of trust value based on the vehicle's performance
- Traffic classification using Cat-Boost algorithm
- Blockage of malicious nodes

F. Accuracy Considerations:

The assessment of the proposed model was done using the UNSW-NB15 dataset. The scores obtained are as follows:

Total Records: 2,56,000
Training set: 1,75,000
Testing set: 82,332

Confusion Matrix:

	Prediction-Attack	Prediction-Normal
Actual-Attack	TP(37,850)	FN(3,650)
Actual Normal	FP(1,650)	TN(39,182)

- Accuracy = 93.57
- Precision = 97
- Recall = 93
- F1-score = 9

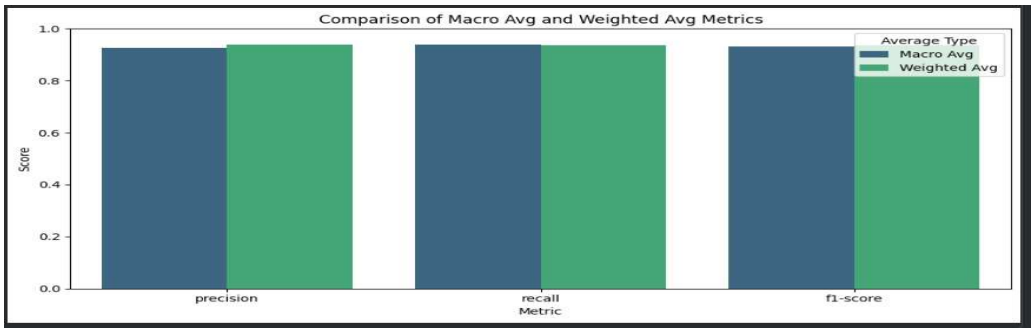

Fig. 3. Comparison of Macro Avg and Weight

- ROC-AUC score = 0.9888

From the above scores, it can be noted that the proposed model has great intrusion detection capabilities for IoV communications.

It is also worth noting that extremely high accuracy scores might suggest either overfitting or data leakage. Hence, the appropriate pre-processing techniques were implemented.

IX. PERFORMANCE EVALUATION OF PROPOSED IOV SYSTEM

RSA authentication technique, AES encryption technique, dynamic trust evaluation and intrusion detection using catboat approach have been proposed for designing an effective, secure, and intelligent communication scheme for IoV systems.

Several performance metrics have been proposed for measuring the effectiveness and efficiency of the secure communication scheme proposed. Some of these performance parameters are Accuracy, Precision, Recall, F1-score, ROC-AUC Score, latency, security strength, Throughput, and Packet Delivery Ratio.

The proposed scheme utilizes RSA authentication technique, AES encryption technique, dynamic trust evaluation approach, and catboat intrusion detection technique for detecting malicious nodes.

Experimental analysis was carried out using the UNSWNB15 data set. Results obtained indicate that the proposed architecture obtains classification accuracy of 93.57

A high value of the Precision score, namely 97

X. KEY INSIGHTS AND CHALLENGES

A. Key Insights of the Proposed System:

A number of advantages can be derived from the suggested design in terms of achieving secure and intelligent communication.

- Secure Communication: The use of hybrid cryptosystem with RSA and AES ensures data confidentiality, integrity, and authenticated communication.
- Efficiency of Authentication: The use of RSA for public key infrastructure helps in ensuring secure authentication and appropriate generation of session keys.
- Fast Encryption/Decryption: The use of AES facilitates the process of very fast data encryption and decryption.
- Intrusion Detection: The catboat algorithm helps in detecting malicious behaviour of nodes.
- Evaluation of Trustworthiness: It becomes possible to identify untrustworthy nodes through trust evaluation.
- Prevention of Fake Messages: Besides the intrusion detection, the trust evaluation helps in preventing fake messages.
- Fast Communication: Due to fast data encryption and decision-making, there is no issue with latency of communication.
- Road Safety: Proper communication facilitates accident prevention in IoV networks.

B.Challenges in IoV Communication:

Although the current systems have improved, there are some problems associated with IoV systems due to the dynamic and open nature of the communication environment.

- Open Wireless Channel: The wireless channel used for vehicular communication is subject to attacks such as listening, spoofing, retransmission, and interception of messages.
- Injection of Misinformation: Malicious entities may spread erroneous alarms and other types of false information.
- Latency Constraint: There is a need for rapid deployment of security measures that should react fast enough during emergencies.
- Scalability: The proposed security mechanism must be scalable and capable of handling the massive communication requirements in many vehicles.
- Privacy: Confidentiality of each vehicle’s identity, position, and communication should be guaranteed.
- Computing and Storage Limitations: Some computing and memory limitations exist for some vehicular nodes.
- Manipulation of Trust Value: The attackers can manipulate trust value computation using false recommendations.

XI. PROPOSED FRAMEWORK

A. Overview:

The above-described proposed system will operate as follows:

Step 1: Vehicle Authentication Every vehicle possesses an RSA public key and private keys generated by itself. Only those vehicles that can be considered reliable may be allowed entry into this network.

Step 2: Creation of Secure Channel The temporary key is created by the sender. It is sent out using the RSA algorithm. All the information sent out through this channel is secured with the help of AES algorithm.
Step 3: Estimating Trust Level the following factors determine the level of trust of a particular vehicle in this network:
• The direct trust level is defined by the direct interactions of vehicles in the network. • The indirect trust depends on the opinion of neighbouring nodes. • Cars possessing special roles, for instance, ambulances, are trusted due to their importance.
The formula for estimating the level of trust is presented below:

$$T = Td + Ti + Tr$$

Step 4: Intelligent Intrusion Detection System catboat Classifier evaluates the network traffic and classifies all vehicles based on their normal behaviour or malicious intentions.
Step 5: Isolation of Malicious Nodes Those nodes that have very low trust levels will be isolated.

B. Methodology:

Consequently, the communication becomes reliable and secured. The proposed architecture utilizes a procedure consisting of the following phases:
Phase One: Car Authentication Each automobile receives its private-public RSA key set. Consequently, only certified and authenticated cars may participate in networking.
Phase Two: Establishment of a Reliable Channel for Communication During the process of communication, a session key through AES is produced by the sender. After that, the RSA algorithm will be utilized to transfer the session key created to the recipient via a dependable communication channel. Finally, the message will be encrypted using AES.
”RSA encrypts the transmission of keys, while AES assists in transmitting messages.”
Phase Three: Trust Evaluation Various parameters will influence the trust assessment process for each vehicle:

- Direct trust, based on the last experience with the vehicle.
- Indirect trust, influenced by the opinion of other cars.
- Priority trust, influenced by priority vehicles (ambulance and rescue teams).

These values are combined to compute an overall trust score:

$$T = \alpha T_d + \beta T_i + \gamma T_r \qquad (17)$$

Step 4: Malicious Node Detection If a vehicle’s trust value falls below a predefined threshold:

$$T < T_{threshold} \qquad (18)$$

The vehicle is classified as malicious, and its communication is restricted or ignored.

C.Main Contributions:

The contributions of the proposed approach include:

- Both RSA and AES encryption techniques are used in order to provide secure yet fast communication.
- Identification of vehicles based on trust to detect any malicious nodes in the system.
- Realization of a design that offers low-latency communication in real time.
- Combination of security and performance in an efficient way.

D. Advantages:

- Strong Security: Usage of hybrid cryptography for guaranteeing security and authentication.
- Low Latency: Fast processing of encryption and decryption using AES
- Prevention of Fake Messages: Trust-based mechanism filters out unreliable information.
- Safe Information Transmissions: Improvement in making decisions by using reliable information.

Subsection Limitations

- High Resource Consumption: Computational resources consumed when using RSA algorithm.
- Vulnerability in Trust Values: Actors can exploit trust values in the system.
- Not Easily Scalable: Implementation becomes problematic when trying to scale up.

XII. ADVANTAGES AND LIMITATIONS

A. Advantages:

Below are some of the advantages that would be achieved once this framework is implemented for secure communication in the IoV network:

- High Security Levels: High security levels will be attained during the communication process through the application of RSA and AES algorithms in the processes of authentication and encryption, respectively.
- Quick Communication: Through the application of AES algorithm, there will be quick communication within the vehicle because of AES being involved in encryption.
- Malicious Cars/Communications Identification: With catboat classification, we will be able to detect and identify malicious vehicles/communications so as to classify them as such.
- Spam-free Communication: Carrying out spam communication will be difficult since machine learning has been incorporated into the system and trust has been assessed.
- Secure Communication Process: Malicious cars' isolation will make the whole communication process very secure.
- Cryptography Techniques: RSA and AES algorithms will be involved in authentication and encryption process, respectively.
- Improved Road Safety: Road safety will be improved through this secure communication technique as the number of traffic accidents will be minimized.
- Scalability: This framework can be made scalable in order to cater to many vehicles and roadside infrastructures.

B. Limitations:

While this solution offers many benefits, the following cons can also be attached to it:

- Costly Process: The employment of RSA for authentication purposes implies that there will be higher expenses related to the process.
- Dependence on Trust Levels: The entire process relies on the correctness of the computation of trust values.
  Errors while computing such values lead to issues in the course of the algorithm.
- Challenges Associated with Keys' Management: The management of keys may become problematic where there are many cars.

- Scaling Challenges: There will be difficulties with computations when it comes to high numbers of cars.
- Security Threats: Hacking attacks are to target trust levels or the anti-hack measures used.
- Challenging to Implement: The process of implementing trust values in a system using hybrid encryption becomes complicated.

XIII. SECURITY ANALYSIS

The security of communication in Internet of Vehicles (IoV) is a critical concern due to the open and highly dynamic nature of the network. In the proposed system, RSA based authentication, AES, and trust estimation techniques have been incorporated to offer a threefold security solution. Not only does this protect information, but it also guarantees that only trustworthy vehicles engage in communication.

A. Countermeasures against Sybil Attack:

In a Sybil attack, the malicious vehicle creates multiple false identities to dominate the network. In the proposed system, each vehicle must undergo RSA based authentication, which assigns a unique cryptographic identity. Due to difficulties in creation of numerous valid key pairs, chances to have fake identities decrease considerably. In addition, the trust evaluation model continuously monitors the behaviour of vehicles. If multiple identities exhibit suspicious or similar malicious patterns, their trust values decrease, and they are eventually classified as malicious nodes.

In addition, the trust evaluation model continuously monitors the behaviour of vehicles. If multiple identities exhibit suspicious or similar malicious patterns, their trust values decrease, and they are eventually classified as malicious nodes.

B. Replay Attack Mitigation:

In a replay attack, the attacker captures real data communication and transmits it again at some future time, thus causing some confusion in the network. . In order to counter this problem, the model employs AES encryption with persession keys. As a result, since each communication instance uses different keys, any data packets intercepted will not have any significant impact when sent back to the network.

C. Detection of Fake Message Injection:

IoV systems may be subjected to attackers who send misleading messages such as false traffic updates or accidents. The proposed model tackles this threat using the trust score evaluation process. Vehicles that regularly broadcast inaccurate data have a declining trust value. When the trust value goes below a certain threshold level, it is established that the vehicle is malicious and its communication should be terminated.

D. Mitigation of Man-in-the-Middle (MITM) Attacks:

In a Man-in-the-Middle attack, an attacker attempts to intercept and manipulate communication between two vehicles. This is because the proposed system implements RSA to achieve the process of key exchange while using AES for the process of encrypted communication. Therefore, even when an attacker intercepts the information transmitted through this system, they cannot interpret the encrypted data since it requires decryption keys

to read the information contained therein. Thus, the communication between the vehicles will be secure and confidential.

E. Data Confidentiality and Integrity:

The confidentiality of the data transmitted is guaranteed by means of using AES encryption since only authorized receivers will have the capability to decrypt the data. On the other hand, any attempt to modify the encrypted data during its transmission will automatically cause decryption failure, thus maintaining data integrity. This dual protection mechanism ensures that the data is both secure and reliable.

F.General Security Perspective:

Basically, the system implements a strong security solution by combining strong encryption with intelligent trust-based assessment of vehicles. In other words, while RSA and AES are protecting the communications, the trust model ensures that only well-behaved vehicles participate in the communication process. This means that such a system will be able to withstand multiple attacks in IoT environments.

***G. Security Characteristics of Proposed System*:** TABLE IV

SECURITY ANALYSIS FEATURES

Attack Type	Defense Mechanism
Sybil Attack	RSA + Trust-Based
Replay Attack	AES-Based
False Message Injection	Trust-Based
MITM Attack	RSA + AES Based
Tempered Data	Encryption Based

XIV. RESULTS

The experiment has been performed in order to evaluate the efficiency of the developed secure trust-based communication framework in IoV networks. As mentioned earlier, the framework comprises RSA-based authentication, AES-based encryption, trust evaluation, and catboat-based intrusion detection.

The UNSW-NB15 dataset has been used in the process of training and testing the module responsible for malicious nodes detection. Following data pre-processing, feature selection, and stratified train-test set splitting, the developed classifier provided good classification results.

The following table summarizes the acquired classification metrics:

Accuracy: 93.57
Precision: 97
Recall: 93
F1-score: 95
ROC-AUC Score: 0.9888

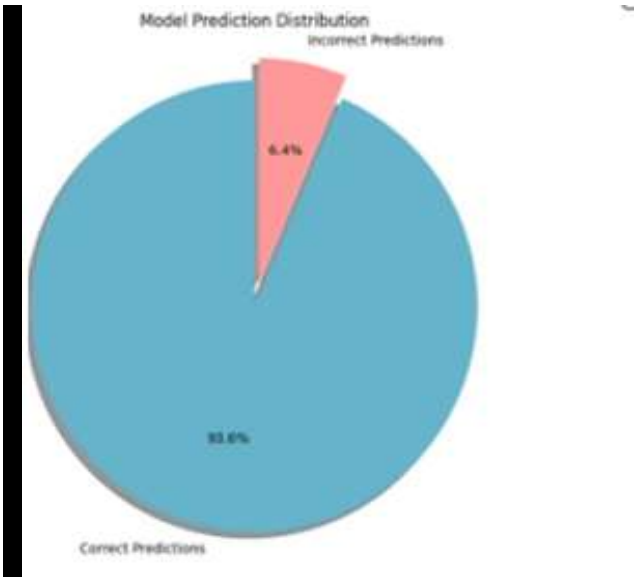

Fig. 4. Model prediction

As shown above, the proposed solution offers an efficient tool for detecting malicious behaviour with a low false positive rate and strong recall. In other words, the model allows for separating normal network traffic from attacks.
Moreover, apart from the classification results, the RSA authentication mechanism guarantees that only authorized users can access the IoV network, while the AES encryption algorithm provides secure message delivery with minimum latency. Trust evaluation allows excluding suspicious or low reliability vehicles from the network.
Therefore, it can be stated that the suggested framework enhances the communication security, minimizes the number of malicious participants, and enables reliable vehicular communication.

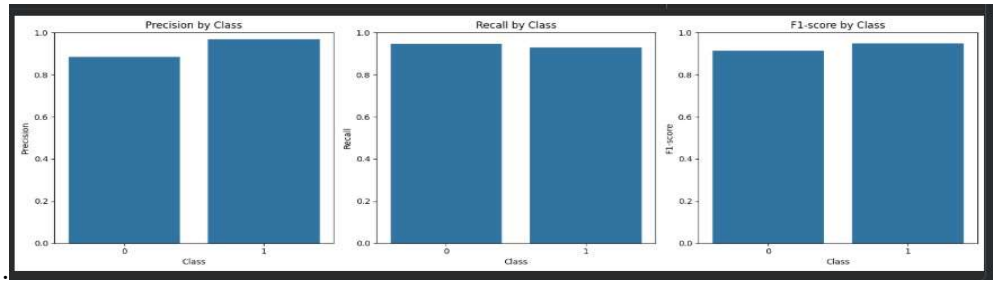

Fig. 5. Accuracy, Precision, Recall

XV. CONCLUSION

The framework of this paper discussed the idea of designing a trust-based communication system for the Internet of Vehicles (IoV), which used encryption based on hybrid methods and an intelligent approach towards intrusion detection.
According to the results obtained from experimentation with the UNSW-NB15 dataset, the proposed framework was found to yield an accuracy rate of 93.57

Through cryptographic methods and machine learning technology, the proposed approach can provide benefits in terms of improving confidentiality, integrity, ability to detect any attacks and enhance communication efficiency simultaneously. Malicious nodes can easily be detected and separated from normal users, and trusted vehicles will be able to communicate in a secured environment with reduced latency.

In conclusion, the framework designed in this paper serves as a promising method in securing future IoV networks.

For future research, the use of block chain technology and federated learning could be applied as an extension of this work.

TABLE V
COMPARISON OF INITIAL AND IMPROVED MODELS

Parameter	Initial Models	Improved Model
Algorithms Used	XGBoost, Random Forest, Voting Classifier	CatBoost
System Accuracy	86%	93%
Performance Level	Satisfactory	High
Categorical Data Handling	Requires pre-processing	Directly handles categorical data
Overfitting Control	Moderate	Better control
Prediction Efficiency	Good	Excellent
Hyper parameter Tuning	More required	Less required
Reliability	Moderate	High
Final Selection Status	Not selected as final model	Selected as final model

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our research guide for the constant encouragement, valuable suggestions, and insightful guidance provided throughout the course of this work. The continuous support and expert advice greatly contributed to the successful completion of this research.

We also extend our heartfelt thanks to the reviewers and publishers for their constructive comments, professional suggestions, and valuable observations, which helped improve the quality and presentation of this research work. Their feedback played an important role in refining the study and enhancing its academic contribution.

Finally, we acknowledge all the researchers and scholars whose published works and scientific contributions served as an important foundation for carrying out this research successfully.

- Lastly, our deep sense of gratitude goes to our friends who have motivated us throughout this research process.

REFERENCES

1) . A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive Radio-Based Internet of Vehicles: Applications, Architectures, and Challenges," IEEE Access, 2020. Available: https://ieeexplore.ieee.org/
2) M. A. Javed, S. Zeadally, and E. B. Hamida, "Data Analytics for Cooperative Intelligent Transport Systems," IEEE Communications Surveys & Tutorials, 2020. Available: https://ieeexplore.ieee.org/
3) H. Menouar, F. Filali, and M. Lenardi, "A Survey and Qualitative Analysis of MAC Protocols for Vehicular Ad Hoc Networks," IEEEWireless Communications, 2020. Availa https://ieeexplore.ieee.org/
4) S. Sharma and B. Kaushik, "Trust-Based Secure Routing in Internet of Vehicles," International Journal of Communication Systems, 2021. Available: https://onlinelibrary.wiley.com/
5) Y. Liu, L. Wang, and H. Yang, "Blockchain-Based Secure Communication in Internet of Vehicles," IEEE Transactions on Intelligent Transportation Systems, 2021. Available: https://ieeexplore.ieee.org/
6) X. Zhang, J. Liu, and Y. Chen, "Efficient Hybrid Encryption Scheme for Secure Data Transmission in IoT," IEEE Access, 2021. Available:https://ieeexplore.ieee.org/
7) R. Gupta and N. Kaur, "Machine Learning-Based Intrusion Detection System for IoV," Journal of Network and Computer Applications, 2022. Available: https://www.sciencedirect.com/
8) P. Sharma, S. Agarwal, and R. Singh, "Lightweight Cryptographic Framework for Secure IoV Communication," IEEE Access, 2022. Avail-able: https://ieeexplore.ieee.org/
9) .M. Singh and A. K. Verma, "Trust Management System for SecureVehicular Networks," Wireless Networks, 2022. Available: https://link. springer.com/
10) . K. Patel and D. Mehta, "Hybrid Security Mechanisms for Internet of Vehicles," International Journal of Information Security, 2023. Available: https://link.springer.com/
11) E. Alalwany and I. Mahgoub, "Security and Trust Management in Internet of Vehicles (IoV): Challenges and Machine Learning Solutions,"Sensors, vol. 24, no. 2, p. 368, 2024. Available: https://www.mdpi.com/ 1424-8220/24/2/368
12) . H. Han et al., "Trust Management Scheme of IoV Based on Dynamic Sharding Blockchain," Electronics, vol. 13, no. 6, p. 1016, 2024. Available: https://www.mdpi.com/2079-9292/13/6/1016
13) . Y. Wang et al., "TM-IoV: Multilabeled Trust Parameter Dataset for IoV," Data, vol. 9, no. 9, p. 103, 2024. Available: https://www.mdpi.com/ 2306-5729/9/9/103
14) Y. Wang et al., "Towards Distinguishing Trust-Based Attacks in IoV Network," 2025. Available: https://link.springer.com/
15) . G. Routis et al., "Cryptography-Based Location Privacy Protection in IoV," 2024. Available: https://link.springer.com/
16) E. Khezri et al., "Security Challenges in Internet of Vehicles for ITS," Tsinghua Science and Technology, 2025. Available: https://www.sciopen. com/
17) L. Prokhorenkova et al., "CatBoost: Unbiased Boosting with Categorical Features," NeurIPS, 2018. Available: https://papers.neurips.cc/paper/ 7898-catboost-unbiased-boosting-with-categorical-features.pdf

18) *T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of KDD, 2016. Available: https://dl.acm.org/doi/10.1145/ 2939672.2939785*
19) *L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001. Available: https://link.springer.com/article/10.1023/A: 1010933404324*
20) *N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," MilCIS, 2015. Available: https://research.unsw.edu.au/projects/unsw-nb15-dataset*
21) *. CatBoost Official Documentation. Available: https://catboost.ai/*
22) *. XGBoost Official Documentation. Available: https://xgboost. readthedocs.io/*
23) *Scikit-learn Official Documentation. Available: https://scikit-learn.org/Pandas Official Documentation. Available: https://pandas.pydata.org/ NumPy Official Documentation. Available: https://numpy.org/*