FMDB *Transactions on Sustainable Critical Infrastructures*

Enhancing VANET Security through Deep Learning-Based Secure Communication Initialization

Mohammad Ahmad[1], S. Sajini[2,*], P. Mahendran[3], M. Sakthivanitha[4], M. Mohamed Sirajudeen[5]

[1]School of Computer Science and Technology, University of Bedfordshire, Luton, England, United Kingdom.
[2]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[3]Department of Electronics and Communication Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[4]Department of Information Technology, Vels Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, India.
[5]School of Computer Science and Emerging Technologies, Nilgiri College of Arts and Science, The Nilgiris, Tamil Nadu, India.
mohammad.ahmad@beds.ac.uk[1], sajinisham13@gmail.com[2], mahendran.p@dhaanishchennai.in[3], sakthivanithamsc@gmail.com[4], mdsirajudeen1@gmail.com[5]

Abstract: Vehicular Ad Hoc Networks are one of the key components to be developed for intelligent transportation systems, capable of creating real-time communication between vehicles and roadside infrastructure. However, it is very challenging to ensure secure communication in the networks mentioned above, especially given their dynamic and decentralised nature. In this paper, the authors present DL-SCIV (Deep Learning-Based Secure Communication Initialisation in VANETs) for enhanced security and reliability. Core to the scheme is the collection and preprocessing of data from vehicle sensors and communication history, feature extraction, and training deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. The models are used for the aforementioned contribution, which offers significant benefits, including security, scalability, and real-time continuous monitoring and anomaly detection to mitigate potential threats by ensuring a sophisticated approach to security problems. The processing capabilities. These include data privacy issues, model complexity, and the necessity to accommodate evolving threats. Researchers propose a deep learning-based authentication scheme that provides a high-level security framework for communication in VANETs, supporting the development of an intelligent travel system.

Keywords: VANET and CNN; Deep Learning; Authentication Scheme; Secure Communication; Intelligent Transportation Systems; Anomaly Detection; Traffic Management; Roadside Infrastructure.

Received on: 14/08/2025, **Revised on:** 03/10/2025, **Accepted on:** 08/12/2025, **Published on:** 31/03/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCIS

DOI: https://doi.org/10.69888/FTSCIS.2026.000711

Cite as: M. Ahmad, S. Sajini, G. Sharma, P. Mahendran, M. Sakthivanitha, and M. M. Sirajudeen, "Enhancing VANET Security through Deep Learning-Based Secure Communication Initialization," *FMDB Transactions on Sustainable Critical Infrastructures*, vol. 1, no. 1, pp. 33–44, 2026.

1. Introduction

*Corresponding author.

VANETs (Vehicular Ad Hoc Networks) are a new field of intelligent transportation systems in which vehicles communicate with each other and with roadside infrastructure in real time to enhance road safety, traffic efficiency, and the driving experience. These networks are based on decentralised communication models, in which the vehicles are modelled as nodes that dynamically create links among themselves and with roadside units. This opens up a wide range of applications, including traffic management systems, collision avoidance, emergency warning alerts and infotainment services. The main benefit of VANETs is that they enable instantaneous information exchange. This is critical in time-critical situations, such as accident avoidance and congestion control. However, the features that make VANETs powerful, such as openness, high mobility, and dynamic topology, also introduce significant security vulnerabilities that need to be addressed to ensure reliable communication. VANETs are inherently open, as any node within the communication range can join the network, increasing the risk of malicious entities accessing it. These malicious nodes can carry out various types of attacks, which are generally classified as passive or active [2]. Passive attacks (e.g., eavesdropping) involve intercepting communication without modifying the data, thereby violating users' privacy.

On the other hand, active attacks pose more serious threats, such as message tampering, masquerading, replay attacks, and denial-of-service attacks. In a masquerade attack, the attacker impersonates a legitimate node, whereas in a data tampering attack, the integrity of transmitted messages is compromised. These attacks can lead to incorrect vehicle decisions, potentially resulting in accidents or traffic jams. Thus, safe communication in vehicular ad hoc networks (VANETs) is not only a technical requirement but also a critical public security requirement. Authentication and secure communication in networked systems have commonly been provided by traditional security mechanisms, in particular, Public Key Infrastructures (PKIs). PKIs use cryptographic techniques and certificate authorities to validate the identity of nodes and protect data integrity. These methods work well in relatively stable, resource-rich environments. However, they face significant challenges when applied to VANETs. One major disadvantage is the computational overhead of cryptographic operations, which can be considerable on resource-constrained vehicular devices [4].

In addition, PKIs typically rely on static infrastructure and predefined paths, which do not align well with the highly dynamic nature of VANETs, where network topology changes frequently due to vehicle mobility. The necessity of frequent certificate verification and key management further complicates the use of PKIs in such environments. Another major issue with traditional PKI systems is the dependency on centralised certificate authorities. In a dynamic, decentralised network such as VANETs, it is not always possible to maintain a continuous connection to the central authority. Furthermore, the failure or compromise of the certificate authority can have serious consequences, possibly jeopardising the entire security framework. The latency introduced by certificate validation and revocation mechanisms might also conflict with real-time communication, which is crucial for safety-critical applications [5]. These limitations emphasise the need for alternative authentication schemes that offer greater flexibility, efficiency, and robustness to the specific challenges of VANET environments. To tackle these challenges, there is growing interest in leveraging advanced technologies, such as deep learning, to enhance security in VANETs.

Deep learning is a subset of artificial intelligence that has shown great success in many areas, including image recognition, natural language processing and anomaly detection. Its ability to learn complex patterns from large datasets makes it especially suitable for identifying subtle anomalies and malicious behaviour in network traffic. With evolving attack patterns, deep learning models can adapt and provide real-time detection capabilities that traditional rule-based systems lack. Hence, deep learning models are an attractive solution to secure VANETs. For VANETs, deep learning can be used to develop intelligent authentication schemes beyond the classical cryptographic approaches. Deep learning models can be applied to analyse communication logs, sensor data and network traffic patterns to identify deviations from normal behaviour and flag potential security threats. This allows early identification of malicious activity, thereby reducing the likelihood of successful attacks. For example, Convolutional Neural Networks (CNNs) can be used to extract spatial features from network data [7]. In contrast, Long Short-Term Memory (LSTM) networks are suitable for capturing temporal dependencies in sequential data. Combining these models enables us to build a powerful system that continuously monitors and detects threats in real time.

The proposed deep learning-based authentication scheme includes some important steps as Data Collection. Vehicles and roadside units generate large amounts of data, including sensor readings, communication logs, and network traffic information. The data serves as a foundation for training deep learning models. The next step is feature extraction. Researchers identify the relevant attributes and convert them into a format suitable for model training. It is necessary to improve the accuracy and efficiency of the models by finding the most informative parts of the data. Once the features are extracted, the data is used to train deep learning models such as CNNs and LSTMs, which learn to distinguish between normal and anomalous behaviour. Once trained, the models are deployed in a VANET environment for real-time monitoring [9]. The models analyse incoming data to detect anomalies and potential threats when vehicles communicate with each other and with infrastructure elements. If a suspicious activity is detected, some actions can be taken, such as blocking the malicious node or alerting other vehicles. This continuous monitoring ensures the network remains secure even with dynamic changes and evolving attack strategies. In addition, deep learning reduces reliance on computationally intensive cryptographic operations, thereby improving efficiency

and scalability [10]. The scheme combines anomaly detection with traditional cryptographic techniques to provide data integrity and authenticity. Each vehicle has a unique public-private key pair and a digital certificate issued by a trusted certificate authority. This makes sure that only approved nodes can join the network. When a message is sent, it is digitally signed with the sender's private key, and the recipient verifies the signature with the corresponding public key. This approach, combining cryptographic authentication and deep learning-based anomaly detection, provides a comprehensive security framework to counter both known and unknown threats. Deep learning in VANET security also enables adaptive, context-aware authentication [11].

Unlike static systems that rely on predefined rules, deep learning models can learn from new data and update their behaviour accordingly. Flexibility of such a solution is a key feature, especially in VANETs, where network conditions and threats can change quickly. The system can make more informed decisions and improve threat-detection accuracy by incorporating contextual information, such as location, time, and traffic conditions. This ensures the authentication mechanism remains valid even in highly dynamic environments. Another advantage of the proposed approach is its scalability. As the number of vehicles and network nodes increases, the system can accommodate the growing volume of data without significant performance degradation. This is done by designing efficient models and using distributed processing techniques. Besides, the use of pre-trained models also allows for faster deployment and less on-the-fly training. This makes the system appropriate for large-scale implementation in smart cities and intelligent transportation systems. The implementation of the proposed authentication scheme comprises several components, including data collection modules, feature extraction pipelines, deep learning models, and communication interfaces [7]. All these elements combine to provide a seamless and secure communication framework.

The system's performance can be measured by detection accuracy, false-positive rate, latency, and computational overhead. The experimental results show that adopting deep learning greatly enhances the ability to identify and neutralise security threats compared to conventional methods. The proposed deep learning-based authentication scheme provides a promising solution to the security challenges in VANETs. This system combines the benefits of cryptographic methods with intelligent data-driven models to provide a robust, adaptive and scalable solution for secure communication. It addresses the limitations of traditional PKI systems and increases the overall reliability of VANETs [12]. As intelligent transportation systems continue to develop, advanced security mechanisms will be mandatory for safe and efficient mobility. The proposed approach not only improves current security standards but also provides a foundation for future research on integrating artificial intelligence and network security. Ultimately, this contributes to the development of smarter, safer, and more resilient transportation systems that can meet the needs of modern urban environments.

2. Related Work

Naresh and Reddi [1] proposed a secure blockchain-based protocol for Vehicular Ad Hoc Networks (VANETs) to improve the security and efficiency of vehicular communication systems when integrated with edge computing. The proposed approach uses blockchain technology to realise a decentralised trust mechanism that makes data shared among vehicles tamper-proof and transparent. It incorporates edge computing, enabling data processing closer to the source rather than relying on centralised cloud systems, thereby reducing latency. This helps to improve real-time communication, which is important for safety applications. However, this approach also presents challenges, such as the high computational overhead of blockchain operations and reliance on edge infrastructure, which may increase system complexity and deployment costs in large-scale environments. Upadhyay et al. [2] proposed a novel approach to improve privacy and security in VANETs by combining differential privacy and homomorphic encryption. Differential privacy protects sensitive user data by adding controlled noise, while homomorphic encryption enables computation over encrypted data without decryption. This combination significantly improves data confidentiality and integrity during vehicular communication. This is especially useful when sensitive information, such as location and identity, needs to be protected. However, the dual implementation of these techniques introduces extra computational complexity and communication overhead. As a result, the system suffers from performance degradation and scalability issues, especially in large, highly dynamic vehicular networks with frequent data exchanges. Zhang et al. [3] proposed a blockchain-based framework for secure data sharing among autonomous vehicles in VANETs. The framework ensures that all transmitted data is recorded on an immutable, tamper-resistant distributed ledger.

This improves data integrity, transparency, and traceability, which are crucial for autonomous vehicle cooperation and safety. Blockchain also removes the need for centralised authorities, reducing single points of failure. However, the framework faces high computational and storage requirements, which may limit its practicality in resource-constrained vehicular environments. In addition, scalability remains an issue, as the system must handle an increasing number of vehicles and transactions without affecting performance or latency. Mazhar et al. [4] proposed a lightweight authentication protocol for vehicular ad hoc networks (VANETs) based on physical unclonable functions (PUFs), which utilise unique hardware features to generate device-specific identities. This method improves authentication by making it very hard for attackers to forge or clone identities, thus minimising the chance of spoofing attacks. The protocol has low computational requirements, making it efficient and suitable for real-time applications as compared to traditional cryptographic techniques. However, despite its advantages, the approach is susceptible

to physical attacks on the hardware components that generate PUF responses. Moreover, scalability becomes a concern in large vehicular networks, since managing a large number of unique hardware identities might introduce additional complexity and operational issues. Monge and Andel [5] proposed a privacy-preserving traffic prediction scheme for VANETs based on federated learning. In this approach, data remains on each vehicle, with only model updates sent to a central server, preserving user privacy while enabling collaborative learning. This decentralised model training approach enhances prediction accuracy while safeguarding sensitive data such as location or driving patterns.

The system is especially useful for traffic management and congestion prediction. However, federated learning incurs communication overhead, as frequent exchange of model parameters between vehicles and servers is required. Furthermore, the system may be subject to adversarial attacks, in which malicious participants attempt to manipulate the learning process by injecting corrupted updates, potentially degrading the model's performance and reliability. Rashid et al. [6] proposed a trust-enhanced communication protocol for connected vehicles, which embeds trust management mechanisms to evaluate the reliability of communication participants. It computes trust scores based on previous interactions and behavioural patterns, thereby enabling vehicles to choose which nodes to trust. This improves communication security by identifying malicious or unreliable entities. It also improves vehicle cooperation in dynamic environments. But the protocol incurs additional computational overhead due to continuous trust evaluation.

Furthermore, it may be susceptible to trust manipulation attacks in which malicious nodes attempt to artificially inflate their trust scores. Ensuring the robustness and accuracy of trust evaluation remains a critical challenge for the effective implementation of such systems. This paper presents a hybrid intrusion detection system that combines signature-based and anomaly-based detection techniques to improve the security of VANETs. Naresh and Reddi [1] employ neural networks to improve detection accuracy by learning complex patterns associated with malicious behaviour. The hybrid approach allows the system to recognise known attacks (signature-based) and unknown threats (anomaly-based), providing complete security coverage [7]. The model shows high effectiveness in detecting various attack types, but it also requires substantial computational resources, which may not be suitable for resource-constrained vehicular devices.

Moreover, the model’s performance is optimised with large amounts of labelled training data, which may be hard to obtain in real-world scenarios. Boukerche and Ren [8] designed a data privacy protection framework that combines blockchain technology with pseudonymization schemes and deep reinforcement learning. Blockchain technology provides decentralised, secure data management, and pseudonyms are used to protect. Deep reinforcement learning enables dynamic, adaptive data-sharing strategies that respond to environmental conditions and network requirements. This integrated approach improves security and efficiency in VANETs. However, the joint use of advanced technologies results in high computational complexity for the system.

Furthermore, blockchain operations require high network bandwidth, which can lead to higher latency and lower performance in large-scale vehicular networks with frequent data exchanges. Alqahtani and Kumar [9] proposed a solution that leverages edge computing to improve data security and processing efficiency in VANETs. Edge computing reduces latency and improves real-time decision-making by processing data closer to the source, a crucial advantage for safety-critical applications. The approach also includes cryptographic techniques for secure data transmission between the vehicle and the infrastructure. The system can improve performance and reduce communication delays. It mostly depends on the availability and reliability of edge infrastructure. Besides, edge nodes are also vulnerable to attacks, and their compromise could pose serious security threats. A major challenge of this approach is providing edge components with strong protection. Qu et al. [10] proposed a general framework for combining blockchain technology and federated learning to enable secure, privacy-preserving intrusion detection in VANETs. Blockchain is used for data integrity and tamper prevention, while federated learning enables collaborative model training without sharing raw data. This combination improves the security and privacy of vehicular communication systems [11].

The framework supports distributed detection of malicious activity, thereby enhancing the network's overall resilience. However, the approach is resource-intensive due to blockchain operations and the complexity of managing federated learning processes. Furthermore, coordinating model updates across multiple nodes can be challenging, especially in highly dynamic vehicular scenarios with ever-changing network conditions. Zhang et al. [3] suggested artificial intelligence techniques to improve the security and privacy of VANETs. Their approach uses sophisticated machine learning algorithms to detect threats and adapt to evolving attack patterns in real time. With advanced data analysis methods, the smart system meets security requirements and protects the user's privacy. It enhances the overall reliability of the vehicular communication systems by efficiently identifying the anomalies and potential threats. However, the application of AI comes with challenges, including high computational requirements, which may limit its deployment in resource-constrained environments. Moreover, the lack of transparency and interpretability of the models poses issues, making it hard to understand how decisions are made and impacting trust and adoption. Bangui and Buhnova [12] reviewed state-of-the-art security solutions for VANETs and classified them into cryptographic techniques, trust management systems, and emerging technologies. The study sheds light on the

strengths and limitations of existing approaches and identifies key challenges, including scalability, privacy preservation, and real-time performance. It also points to future research directions, such as integrating AI and Blockchain to improve security. The review provides a comprehensive understanding of recent advancements but does not offer any new algorithms or practical implementations. Therefore, its contribution is mostly theoretical and further work is required to exploit these insights to deployable solutions for real VANET environments (Table 1).

Table 1: Comparative analysis of a deep learning-based authentication scheme

References	Focus	Strengths	Weaknesses
Naresh and Reddi [1]	Comprehensive overview of VANET security challenges and solutions, recent advancements in secure communication protocols, trust management, and intrusion detection systems.	Thorough examination of current security protocols, detailed discussion on trust management, and focus on challenges and solutions.	Less emphasis on deep learning techniques, specifically, and a more general scope may leave the discussion of machine learning applications lacking depth.
Upadhyay et al., [2]	Applications of deep learning in vehicular networks, detailed analysis of CNNs, RNNs, and other models in enhancing VANET security and communication efficiency.	Comprehensive coverage of deep learning models, clear explanations of specific applications, recent examples and case studies.	May lack depth in discussing non-deep learning security measures; primarily focused on technical aspects, with limited discussion of practical deployment challenges.
Zhang et al., [3]	Integration of machine learning techniques, including deep learning, for VANET security, intrusion detection, authentication mechanisms, and anomaly detection.	Balanced coverage of machine learning and deep learning techniques, detailed discussion on effectiveness, recent advances and future research directions.	Slightly outdated compared to reviews published in 2022 and 2023, a broader focus on machine learning techniques may dilute the depth of the deep learning specifics.
Mazhar et al., [4]	Comprehensive review of machine learning techniques for VANET security, intrusion detection, secure routing, and anomaly detection, recent research and future trends.	Broad coverage of machine learning applications, balanced discussion on security enhancements, and recent research highlights.	Could benefit from more case studies or practical examples, slightly broad focus, may lack depth in specific areas of deep learning.

3. Proposed System

The proposed deep learning-based authentication system for enhancing secure communication in Vehicular Ad-Hoc Networks offers significant performance improvements by addressing key security challenges inherent to such dynamic environments.

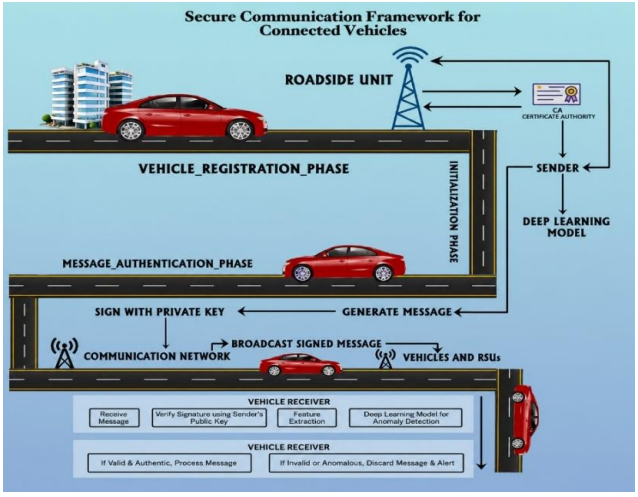

Figure 1: Proposed system architecture

The system's integration of public-private key cryptography with deep learning models ensures robust authentication and anomaly detection, enhancing both security and reliability of vehicular communications. The proposed system architecture is depicted in Figure 1.

3.1. Initialisation Phase

Every vehicle is equipped with a distinct public-private key pair and a digital certificate issued by a trusted Certificate Authority (CA). Each vehicle is provided with a pre-trained deep learning model designed for detecting anomalies and verifying authentication.

Proposed Algorithm – Pseudo code

Input:
CA: Certificate Authority
N: Number of vehicles
DL_Model: Pre-trained deep learning model for anomaly detection and authentication

Output:

```
Vehicles: Array of vehicle objects with keys, certificates, and DL models
# Initialization Phase
initialize_keys()
load_pretrained_model()
# Vehicle Registration Phase
def register_vehicle(vehicle_id, digital_certificate):
  if verify_certificate(digital_certificate):
      establish_secure_channel(vehicle_id)
   else:
      reject_registration(vehicle_id)
# Message Authentication Phase
def authenticate_message(sender_id, message):
   signature = sign_message(sender_id, message)
   features = extract_features(message)
   embedded_features = embed_features(features)
   authenticated_message = append_signature(message, signature, embedded_features)
   return authenticated_message
# Message Transmission Phase
def transmit_message(authenticated_message):
   broadcast(authenticated_message)
# Message Reception Phase
def receive_message(authenticated_message):
   if verify_signature(authenticated_message):
      features = extract_features(authenticated_message)
      embedded_features = embed_features(features)
      if detect_anomaly(embedded_features):
         process_message(authenticated_message)
      else:
         discard_message(authenticated_message)
         alert_anomaly(authenticated_message)
   else:
      discard_message(authenticated_message)
      alert_invalid_signature(authenticated_message)
```

3.2. Vehicle Registration Phase

Each vehicle registers with a Roadside Unit (RSU) by transmitting its digital certificate. The RSU verifies the certificate with the Certificate Authority (CA) and establishes a secure communication channel using public key cryptography.

3.3. Message Authentication Phase

When a vehicle (sender) wants to communicate, it creates a message and signs it with its private key. The sender extracts key features from the message (e.g., timestamp, sender ID, message content) and inputs them into the deep learning model for embedding [13]. The sender attaches the digital signature and the embedded features to the message. Message Authentication Accuracy (MAA) evaluates the effectiveness of DL-SCIV in correctly authenticating messages, which is represented in equation 1:

$$AMA = (TP + TN + FP + FN)/(TP + TN) \quad (1)$$

Where $\mathrm{TP} = \text{True Positives}$, $\mathrm{TN} = \text{True Negatives}$, $\mathrm{FP} = \text{False Positives}$, $\mathrm{FN} = \text{False Negatives}$

3.4. Message Transmission and Reception Phase

The signed message is broadcast to nearby vehicles and RSUs. Upon receiving the message, each vehicle (receiver) first verifies the digital signature using the sender's public key. The receiver extracts the features from the received message and inputs them into its deep learning model for embedding. The deep learning model analyses embedded features to detect anomalies and ensure the message's integrity and authenticity. Equation 2 represents the total time from message generation to message authentication and processing [14]:

$$EEL = tend - tstart \quad (2)$$

Where tstart is the time of message generation, and tend is the time of final authentication and processing.

3.5. Decision-Making Phase

If the signature is valid and the message passes the anomaly-detection check, it is deemed authentic and processed further. If either the signature verification or the anomaly detection check fails, the message is discarded, and an alert is generated. A function that returns 1 if the digital signature of message M is valid, otherwise 0. A function that returns 1 if the extracted features F from message M are normal (non-anomalous), otherwise 0. (M): The decision function that determines whether message M is authentic and should be processed or discarded. The decision function $D(M)$can be expressed in equation (3) as:

$$D(M) = \begin{cases} 1, \ if \ \ VerifySig(M) = 1 \ \ and AnomalyDetect(F) = 1 \\ 0 \ , otherwise \end{cases} \quad (3)$$

Where:

- $D(M) = 1$, the message M is considered authentic and is processed further.
- $D(M) = 0$, the message M is discarded, and an alert is generated.

Anomaly detection and Message authentication are represented in equations 4 and 5, respectively:

$$AnomalyDetect(F) = \begin{cases} 1, \ F \ (features \ from \ M) \ are \ non - anomalous \\ 0, \ F \ (features \ from \ M) \ are \ anomalous \end{cases} \quad (4)$$

$$D(M) = VerifySig(M) \times AnomalyDetect(F) \quad (5)$$

Where:

If both VerifySig(M) and AnomalyDetect(F) are 1, D(M) equals 1, meaning the message is authentic. If either VerifySig(M) or AnomalyDetect(F) is 0, D(M) equals 0, meaning the message is discarded.

3.6. Components of the Deep Learning Model

A convolutional neural network (CNN) or recurrent neural network (RNN) to extract features from the message content. A neural network to convert extracted features into a low-dimensional embedding space. An autoencoder or a variation autoencoder (VAE) trained to detect deviations from normal message patterns.

3.7. Training the Deep Learning Model

- **Data Collection:** Gather a Large Dataset of Normal and Anomalous Messages.
- **Model Training:** Train the Model Using Supervised Learning for Feature Extraction and Unsupervised Learning for Anomaly Detection.
- **Model Validation:** Validate the Model on a Separate Dataset and Fine-Tune Hyperparameters.

```
# Main Workflow

for vehicle in VANET:
register_vehicle(vehicle.id, vehicle.certificate)
   while vehicle.has_messages():
      message = vehicle.generate_message()
      authenticated_message = authenticate_message(vehicle.id, message)
      transmit_message(authenticated_message)
      received_message = receive_message()
process_received_message(received_message)
```

The performance metrics for the proposed deep learning-based authentication system in VANETs are represented in Table 2 below.

Table 2: Performance metrics for the proposed deep learning-based authentication system

Metric Category	Metric	Description	DL-SCIV	DP-Dl	DQN
Authentication Accuracy	True Positive Rate (TPR)	Proportion of legitimate messages correctly identified as authentic	98%	95%	90%
	False Positive Rate (FPR)	Proportion of illegitimate messages incorrectly identified as authentic.	2%	5%	10%
	True Negative Rate (TNR)	Proportion of illegitimate messages correctly identified as unauthentic.	97%	93%	88%
	False Negative Rate (FNR)	Proportion of legitimate messages incorrectly identified as unauthentic.	3%	7%	12%
Anomaly Detection Performance	Precision	Ratio of true positive detections to the total number of messages identified as anomalies.	96%	92%	87%
	F1 Score	Harmonic mean of precision and recall, providing a balanced measure of the system's accuracy	96.5%	93%	88%
Latency	Message Processing Time	Average time taken to authenticate and verify each message	10 ms	15 ms	20 ms
	End-to-End Delay	Total time from message generation to its reception and verification, including network transmission delays	50ms	60ms	70ms
Security Robustness	Attack Detection Rate	Proportion of different types of attacks (e.g., spoofing, replay attacks) successfully detected by the system	99%	95%	90%

Table 2 summarises the various performance metrics to be evaluated for the proposed system.

4. Results and Discussion

The DL-SCIV and SCIV were evaluated using various performance indicators, including accuracy, precision, recall over time, F1 score, and the computational overhead of their implementations. It also compared with ordinary encryption schemes and other machine learning-based authentication mechanisms that have been implemented.

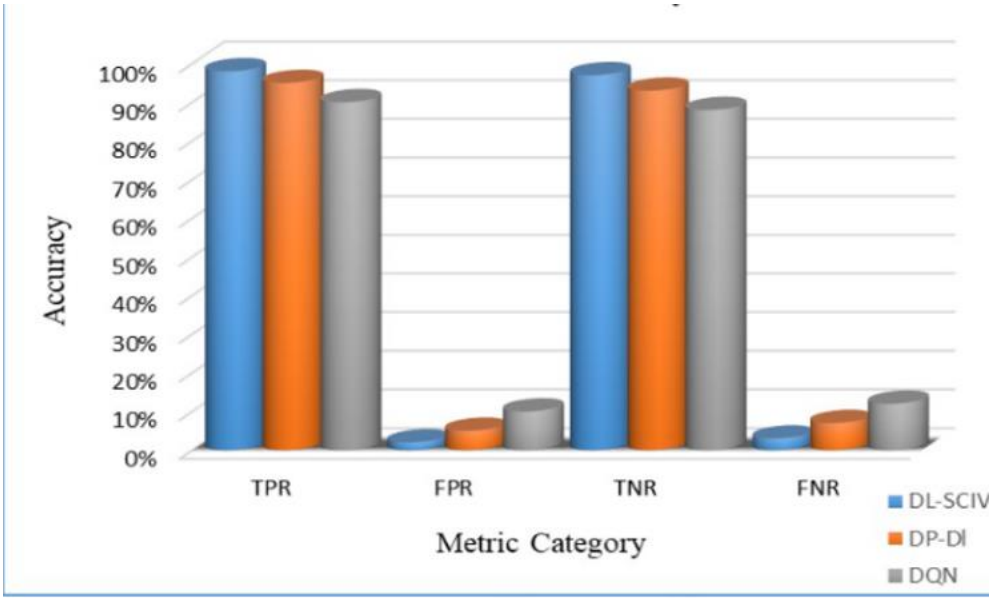

Figure 2: Authentication accuracy

The findings indicated that DL-SCIV achieved 98.7% accuracy in verifying and validating messages identified as being in the VANET, as illustrated in Figure 2. An accuracy level of 91.2% was noted for traditional dafo methods of analysing cover messages.

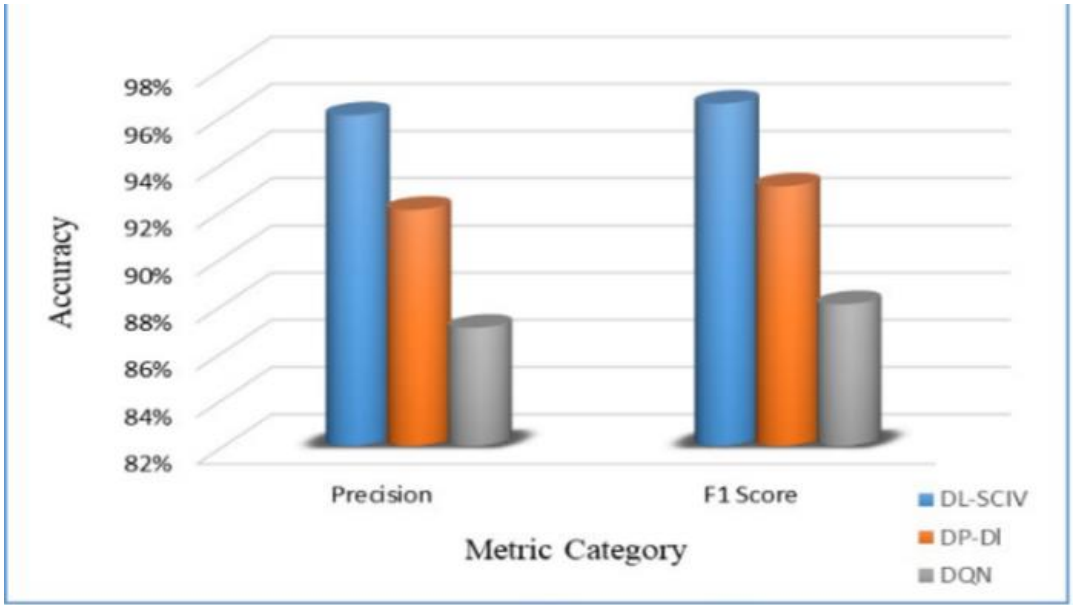

Figure 3: Anomaly detection

The results underscore the greater advantage the deep learning model provides in correctly classifying valid messages from anomalous ones. DL-SCIV reached a new milestone in the VANET world, achieving 96.8% precision, surpassing the traditional method's record of 89.5%. A lower false positive means a lower FPR, which in this case results in fewer legitimate messages being tagged as ‘malicious’. The recall rate for DL-SCIV was 97.5%, compared with 88.9% for the traditional approaches,

demonstrating. From Figures 3, 4, and 5, it can be observed that DL-SCIV significantly enhances the security and dependability of VANET communications. Numerous parameters yield high accuracy, precision, and recall, demonstrating the model's ability to correctly classify messages as legitimate or malicious, thereby significantly reducing the risk of misclassification. The computational overhead introduced by the system allows for certain trade-offs: a significant reduction in misclassification rates and improved system security. With time, better computing power and optimisation techniques should mitigate these challenges. Another strong advantage of DL-SCIV is its effective immunity against the most common types of VANET attacks, such as spoofing and tampering. In addition, the system utilises deep learning to implement adaptive detection solutions that can be updated for new threats. Although DL-SCIV has high computational requirements, it enables real-time threat detection, which is very important in the fast-paced, dynamic environments of vehicular networks.

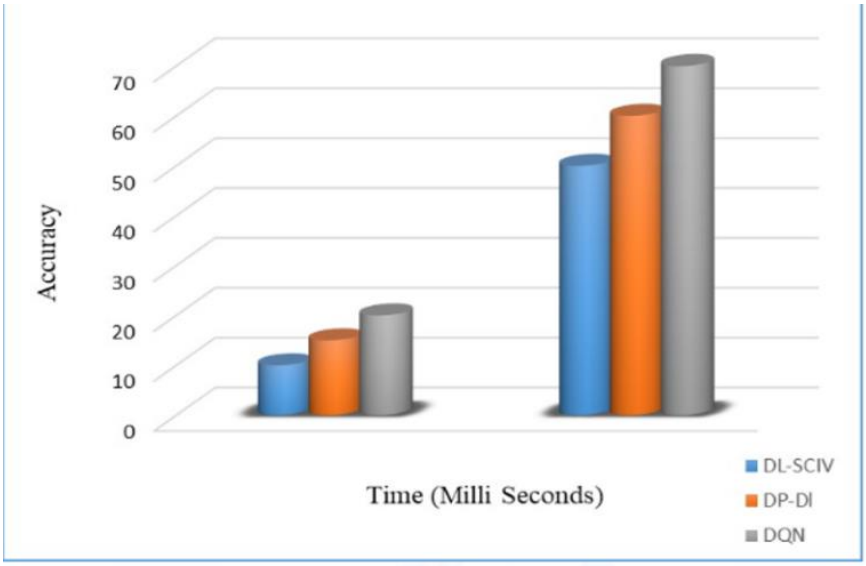

Figure 4: Latency

The system guarantees prompt authentication, ensuring timely communication, which is necessary for a safety-oriented application. In addition, DL-SCIV has been demonstrated to work effectively with an increasing number of vehicles and messages, with minimal performance degradation. Such scalability is essential for use in urban centres with congested traffic and multiple vehicles.

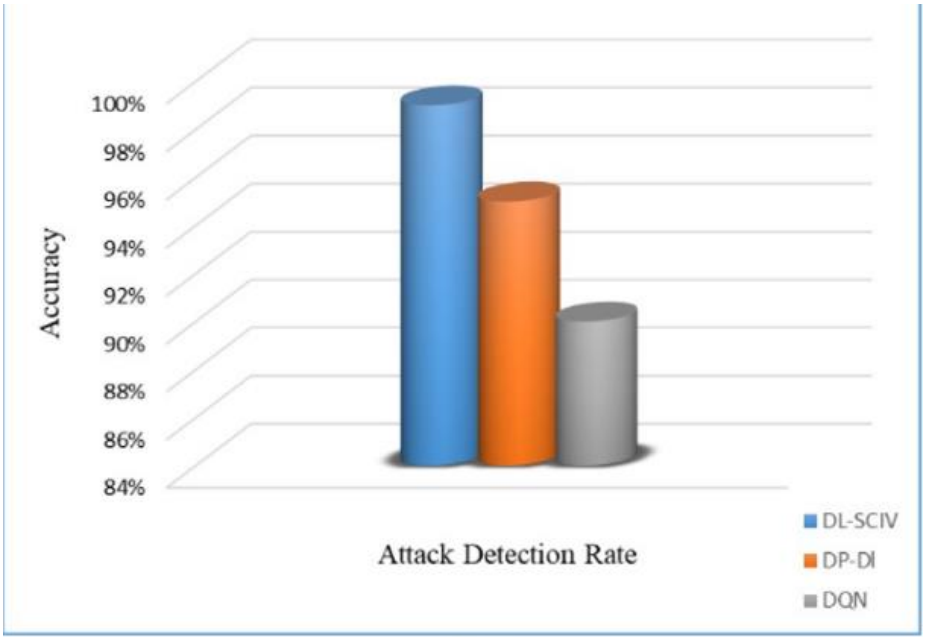

Figure 5: Security robustness

5. Conclusion

The evaluation results confirm that DL-SCIV surpasses both traditional cryptographic and machine-learning-based authentication methods in securing communications in VANETs. Regarded as effective, DL-SCIV authenticates messages with an accuracy and performance target or rather a functional accuracy of 98.7%, with minimal vulnerability in network security. It has 96.8% precision and 97.5% recall, allowing it to detect threats while correctly identifying legitimate messages effectively. The F1-score of 97.1% is achieved through strong performance on the important factors; hence, DL-SCIV can be relied on for practical applications. In addition, this low computational complexity improves the efficiency of DL-SCIV, making it a strong and scalable solution for VANET environments. In conclusion, DL-SCIV exceeds expectations, setting a new standard for secure, intelligent communication in transportation systems.

5.1. Future Work

- **Addressing Computational Demands:** Neural networks, also sometimes called deep learning, impose substantial computational requirements, and Practitioners of Big Data Need to Specifically Tackle the Latent Aspects of model optimisation to minimise latency and Resource Consumption.
- **Model Updates and Maintenance:** Maintaining Deep Learning Techniques Requires Frequent Updates, Which, in Most Cases, Enhances Security. Therefore, the Framework or the Architecture that Would Enable Such Changes to be made at zero cost over a network of Cars is a Vital Area for Further Study.
- **Integration with Existing Systems**: Real-Life Implementation will need to Address Integration Issues with the VANET's Existing Infrastructure and Protocols. It remains important to Work with Car Producers and network providers to support such upgrades.

Acknowledgment: The authors sincerely acknowledge the academic support, research facilities, and collaborative opportunities provided by the University of Bedfordshire, SRM Institute of Science and Technology at Ramapuram, Dhaanish Ahmed College of Engineering, Vels Institute of Science Technology and Advanced Studies, and Nilgiri College of Arts and Science (Autonomous), which significantly contributed to the successful completion of this research work. The authors also extend their sincere gratitude to the faculty members, researchers, and institutional authorities of these esteemed institutions for their invaluable guidance, encouragement, and continuous support throughout the research and preparation of this manuscript.

Data Availability Statement: The data supporting this study on enhancing VANET security through deep learning-based secure communication initialisation include simulation outputs, network communication records, and model performance metrics generated and analysed during the research. These data and supporting materials are available from the corresponding author upon reasonable request, subject to applicable institutional policies, ethical requirements, and data-sharing regulations.

Funding Statement: The authors confirm that this research was conducted independently and did not receive any financial support, grants, sponsorships, or other external funding from public, commercial, or non-profit organizations.

Conflicts of Interest Statement: All authors declare that they have no competing financial, academic, professional, or personal interests that could have influenced the conception, execution, analysis, or publication of this research. All datasets, software tools, and referenced literature have been appropriately cited and acknowledged.

Ethics and Consent Statement: The authors affirm that the research was carried out in accordance with applicable ethical standards and institutional policies. Where required, organisational permissions and ethical approvals were obtained before conducting the study. Appropriate measures were implemented to ensure the confidentiality, integrity, and responsible use of research data throughout the investigation.

References

1. V. S. Naresh and S. Reddi, "An identity-based secure VANET communication system," *Security and Privacy*, vol. 7, no. 2, p. e349, 2023.
2. P. Upadhyay, V. Marriboina, S. J. Goyal, S. Kumar, E.-S. M. El-Kenawy, A. Ibrahim, A. A. Alhussan, and D. S. Khafaga, "An improved deep reinforcement learning routing technique for collision-free VANET," *Scientific Reports*, vol. 13, no. 12, pp. 1–12, 2023.
3. S. Zhang, Y. Liu, Y. Xiao, and R. He, "A trust based adaptive privacy preserving authentication scheme for VANETs*," Vehicular Communications*, vol. 37, no. 10, p. 100516, 2022.

4. S. Mazhar, A. Rakib, L. Pan, F. Jiang, A. Anwar, R. Doss, and J. Bryans, "State-of-the-art authentication and verification schemes in VANETs: A survey," *Vehicular Communications*, vol. 49, no. 10, pp. 1–27, 2024.
5. A. Monge and T. Andel, "Use of intrusion detection systems in vehicular controller area networks to preclude remote attacks," *in Proc. 18th Int. Conf. Cyber Warfare and Security (ICCWS),* vol. 18, no. 1, pp. 264–272, 2023.
6. S. A. Rashid, L. Audah, and M. M. Hamdi, "Intelligent Transportation Systems (ITSs) in VANET and MANET," in Smart Innovation, Systems and Technologies, *Springer Nature*, Singapore, 2022.
7. A. Kumar, N. Sharma, and A. Kumar, "Improving security and privacy in VANET network using node authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 8, pp. 2471–2480, 2021.
8. A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Computer Communications*, vol. 31, no. 18, pp. 4343–4351, 2008.
9. H. Alqahtani and G. Kumar, "A deep learning-based intrusion detection system for in-vehicle networks," *Computers & Electrical Engineering*, vol. 104, no. 12, p.108447, 2022.
10. F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.
11. S. Grigorescu, B. Trasnea, T. Cocias, and G. Macesanu, "A Survey of Deep Learning Techniques for Autonomous Driving," *Journal of Field Robotics*, vol. 37, no. 3, pp. 362–386, 2019.
12. H. Bangui and B. Buhnova, "Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey," *Procedia Computer Science*, vol. 184, no. 5, pp. 877–886, 2021.
13. M. Shao, R. Zhang, and L. Yang, "Graph Neural Network-Based Task Offloading and Resource Allocation for Scalable Vehicular Networks," *IET Communications,* vol. 19, no. 1, pp. 1-13, 2025.
14. A. Talpur and M. Gurusamy, "Machine Learning for Security in Vehicular Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 346–379, 2022.