RESEARCH ARTICLE

Intelligent Cyber-Attack Detection for Autonomous Vehicles Using Advanced Deep Learning Models

Fida Muhammad Khan[1], **Zeeshan Ali Haider**[1,*], **Muhammad Owais Khan**[2], **Ashraf Ullah**[2], **Muhammad Shoaib Khan**[3], **Muhammad Fayaz**[4], **Mushtaq Ahmad**[5] and **Nabila**[6]

[1] Department of Computer Science, Qurtuba University of Science & Information Technology, 25000 Peshawar, Pakistan
[2] Department of Computer Science, University of Science & Technology, Bannu, Pakistan
[3] School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), China
[4] Department of Computer Science and Engineering, Sejong University, Seoul 05006, Republic of Korea
[5] Department of Business informatics, Technical University of Vienna (TUWIEN), Austria
[6] Bangladesh University of Professionals, Dhaka, Bangladesh

Abstract

The Internet of Vehicles (IoV) has greatly influenced transportation by allowing autonomous vehicles to interact and communicate with other cars as well as with the surrounding traffic system. Even so, being interconnected comes with risks in terms of cyber attacks, for example, by injecting messages or fooling sensors through CAN systems. The study, consequently, suggests an Intrusion Detection System (IDS) that uses Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Bidirectional Encoder Representations from Transformers (BERT), and RoBERTa, to properly detect and handle these cyber threats. To solve the problem of unbalanced data, we use Random Over-Sampling (ROS), NearMiss, and Tomek Links, which makes the model work more effectively. Results from experiments show that the IDS suggested here is better than traditional machine learning models. Adopting cloud computing helps make the system more flexible and lets it be watched continually to keep AVs well protected. An IDS in smart cities greatly benefits vehicle networks, as it hinders and stops possible cyberattacks. Related work will aim to improve IDS performance for big organizations and cope with new types of attacks.

Keywords: autonomous vehicles (AVs), cyber-attack detection, internet of vehicles (IoV), bidirectional encoder representations from transformers (BERT), cybersecurity, smart cities.

1 Introduction

Recently, deep learning models have been widely used in most domains like healthcare, finance, transportation, and industry. Neural networks serve as the foundation for automated image recognition, speech processing, natural language understanding, and cybersecurity techniques [1]. Cybersecurity

Submitted: 03 May 2025
Accepted: 09 July 2025
Published: 29 August 2025

Vol. 1, **No.** 3, 2025.
10.62762/TACS.2025.952297

***Corresponding author:**
✉ Zeeshan Ali Haider
Zeeshan.ali9049@gmail.com

Citation
Khan, F. M., Haider, Z. A., Khan, M. O., Ullah, A., Khan, M. S., Fayaz, M., Ahmad, M., & Nabila (2025). Intelligent Cyber-Attack Detection for Autonomous Vehicles Using Advanced Deep Learning Models. *ICCK Transactions on Advanced Computing and Systems*, 1(3), 180–192.

has drawn special attention in the field of detection of advanced attacks and Intrusion Detection in the Internet of Things (IoT) and Industrial IoT systems [2]. Various types of deep learning architectures are being explored to detect cyber threats in different environments, like software-defined networks (SDN), IoT, and cloud computing [3]. Cybersecurity has emerged as a critical area of concern, especially in newer communication systems, as interconnected systems become even more prevalent [4].

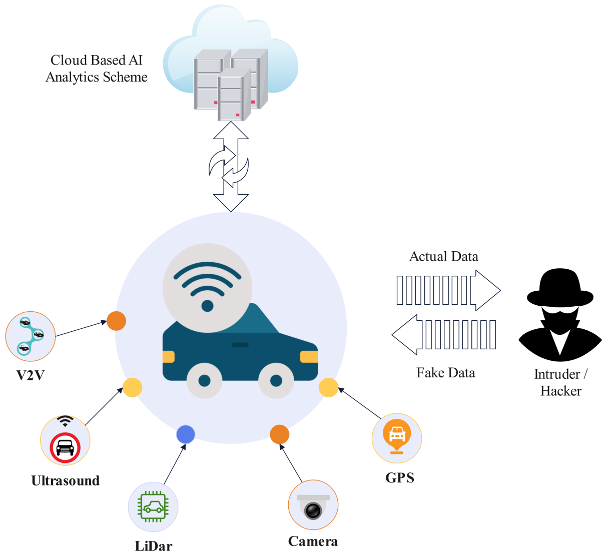


Figure 1. Cloud based AI analytics scheme for car hacking detection.

The growth of autonomous vehicles has made the transportation sector's safety a big issue. AVs use the internet, like IoT, to form the Internet of Vehicles (IoV) network, allowing vehicles to talk to outside systems in real time [5]. AVs are able to talk to each other and the surrounding infrastructure with the help of embedded systems and networks called Controller Area Networks (CAN). Automated electric vehicles (AEVs) are safer than regular vehicles, reduce the chance of errors from drivers, and improve the smoothness of city traffic [6]. Autonomous vehicles can navigate without being driven by using radar, cameras, satellite navigation, and AI, and they communicate with outside platforms through wireless telecoms, for example, 4G and 5G [7]. However, AVs are still at risk from cyber threats such as vulnerable software, sensor tampering, and various system compromises. This is the reason cybersecurity experts are making more effort to protect AEVs from such threats [8]. The use of deep learning models, including CNN, RNN, LSTM, BERT, and RoBERTa, is rising in threat detection in the automotive sector. An AI system using cloud technology has been made to find real-time vehicle hacks by processing data from V2V sensors, LiDAR, cameras and GPS [9]. A system powered by AI in the cloud was made to spot vehicle hacks as they occur, as shown in Figure 1. It explains that sensor data like V2V, Ultrasound, LiDar, Camera and GPS are sent to the cloud server to be analyzed. The software is able to detect whether data was created by an unauthorized person. Improved security for autonomous vehicles is sought by using AI and cloud computing.

Vehicles that work independently (AVs) deal with cybersecurity issues since they use complex networks and interact in real time with other vehicles, infrastructure, and street users through V2V and V2I communication [10]. As a result, their systems may fall victim to cyber threats like message injection, sensor spoofing, and Denial of Service (DoS) attacks caused by protocol flaws, services from untrusted sources, or software weaknesses [11]. AVs can be linked together through the Internet of Vehicles (IoV) for improved control of traffic and safety. Autonomous vehicles do their tasks alone, but IoV allows them to keep in touch with external devices live. Regardless of the progress made in IDS, tools currently available have issues detecting attacks in real time and dealing with data sets where not all types of data are equal [12]. In this scenario, an IDS based on deep learning models is introduced to handle these issues and make sure cyberattacks in AV systems are detected quickly.

The fact that there are many more samples for the attacker than the defender leads to sluggish detection of actual attacks. Because the number of normal data points is much greater than that of attack data, traditional machine learning models have difficulties. In contrast, with models like CNN, RNN, and LSTM, programs have more accurate and consistent solutions by learning how to recognize and handle advanced threats. BERT and RoBERTa, which are Transformer-based models, make detection more accurate by understanding both space and time. An approach to attack detection in Internet of Vehicles (IoV) security is described here, using CNN, RNN, LSTM, BERT, and RoBERTa to address unbalanced data and provide strong real-time cyber defense for both internal and external vehicle infrastructure against complicated attacks. The key contributions of this work are summarized as follows:

- We develop a smart cyberattack detection framework utilizing deep learning models (CNN, RNN, LSTM, BERT, RoBERTa) for real-time intrusion detection in autonomous vehicle systems.

- To propose a Deep-learning-based method, being a comprehensive strategy to address the skewed distribution of car-hacking datasets.
- To conduct performance analysis of the proposed architecture on benchmark datasets to show deep learning models outperform classical machine learning models in identifying cyber-attacks in IoV frameworks.

This paper is structured as follows: Section 2 outlines the related work referenced in this study. Section 3 details the proposed deep learning-based high-level framework for predicting car attacks within the IoVs system. Section 4 covers the dataset, evaluation metrics, and the analysis of the results. Finally, Section 5 concludes the paper by summarizing the findings and suggesting potential areas for future work.

2 Related work

With the advent of autonomous vehicles incorporating the latest technology and communication protocols, securing vehicles is critical. Due to the rapid development of the Internet of Vehicles (IoV) in smart cities, vehicle systems are connected internally and externally. As these networks become central to enabling the use of vehicles, safeguarding them from cyberattacks is crucial for their safe and successful functioning [13]. The data-intensive nature of these systems, coupled with increased complexity in the operation of highly autonomous vehicle systems, has made them an ideal target for hackers or cybercriminals. In this respect, the salient task of building intelligent intrusion detection systems (IDS), which are able to detect various types of such kinds of cyber opponents, is on the rise [14]. In modern self-driving vehicles, the Controller Area Network (CAN) bus is essential for communication between Electronic Control Units (ECUs). On the other hand, external vehicle communication refers to the communication between autonomous vehicles and other suppliers, such as roadside infrastructure and other vehicles in IoV.

Advances in deep learning, especially with transformer-based architectures, have helped improve the ability to detect attacks in autonomous vehicle networks [15]. Research demonstrates that using these techniques is effective for stopping message injection and sensor spoofing, so there is a need for instant detection systems in smart cities [16]. IDS is set up to identify distinct types of attacks in the Internet of Vehicles (IoV) system. DoS attacks involve flooding a system with unnecessary messages, so the IDS notices unusual frequency changes in the traffic and activates an alert [17]. To find inconsistencies in spoofing, the system compares data from two or more different sensors (such as GPS with vehicle speed sensors). When message injection happens, the IDS uses techniques to find suspicious CAN IDs and message intervals. Transformer models such as BERT and RoBERTa are now being used, and studies show they spot cyber-attacks in vehicle networks with more accuracy than traditional machine learning models [18]. Smart city environments now rely on these models to identify threats on the spot, which is key in protecting autonomous vehicles [19].

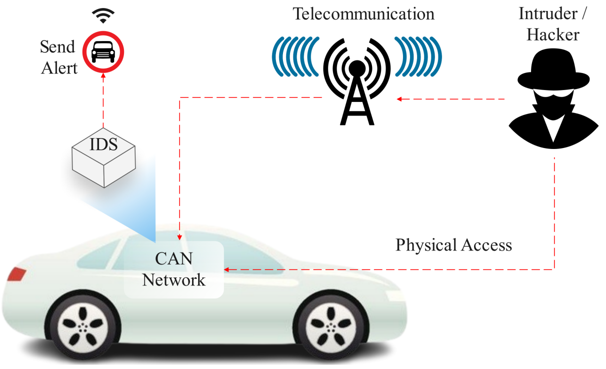


Figure 2. Intrusion detection system (IDS) for car hacking.

CAN bus helps ECUs in modern self-driving vehicles exchange information, and outside communication is necessary for interaction with road infrastructure and other vehicles on the Internet of Vehicles [20, 21]. However, such networks are at risk of different cyberattacks like message injection, sensor spoofing, and remote exploitation [22]. As a result, using reliable Intrusion Detection System (IDS) models to prevent and respond to threats from inside and outside the system is necessary. Through the Vehicle CAN IDS architecture, displayed in Figure 2, the system is informed when an intruder is found, pointing out the possible risk from the CAN network to the telecommunication systems.

The insufficiency of traditional ML methods has been seen when trying to prevent new cyberattacks on autonomous vehicles [23, 24]. Because of these issues, learning models like CNNs, RNNs, LSTMs, BERT, and RoBERTa are used. They work better than traditional methods at spotting hard-to-find patterns and detecting attacks fast [25]. A deep learning-focused Intrusion Detection System is suggested in the paper to detect and foresee cyberattacks in autonomous vehicles. It helps solve the security challenges in real-time traffic using deep models. Comparing the models to a benchmark dataset proved that deep learning helps vehicles become more secure, efficiently discovering known and unknown attack types.

Apart from using large deep learning models, approaches like oversampling, undersampling, and hybrid resampling are added to tackle the imbalance in the dataset, stopping the IDS from strictly following the dominant class.

3 Methodology

In this paper, we introduce a completely new approach for the automatic detection of cyberattacks against autonomous vehicle systems. As shown in Figure 3.

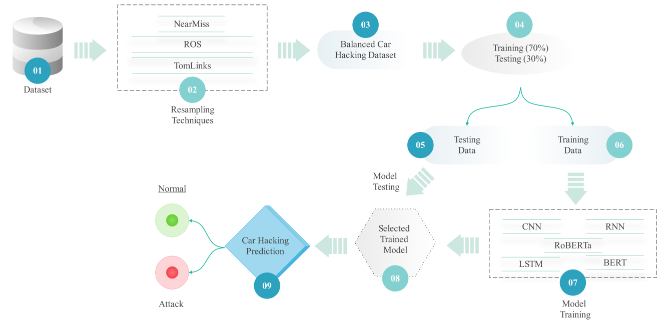


Figure 3. Workflow of the car hacking detection framework.

BERT (Bidirectional Encoder Representations from Transformers) and RoBERTa (Robustly Optimized BERT Pretraining Approach) were specifically designed to work with sequences, so they perform well at finding attacks in vehicle network traffic. BERT uses information from both the past and future and RoBERTa tweaks BERT to give it more training data and better hyperparameter settings. Both systems are effective in spotting quiet manipulations on autonomous vehicle networks. The study investigates an attack detection system built using deep learning which was studied on the Car-Hacking dataset with data from real and simulated vehicle networks. Among the records in the dataset, you can find Denial-of-Service, message injection and spoofing attacks and 818,440 in total are listed. More than 70 percent of these are normal records (701,832), while the remaining 30 percent (116,608) represent attacks. The data covers six months and shows a range of attacks, with CAN ID, timestamp, and data bytes information included, like real-life vehicle networks.

3.1 Car-Hacking Dataset

The Car-Hacking dataset is recently been used to test various intrusion detection systems of autonomous vehicle networks. The dataset presented targets various vehicular communication systems, including DoS attacks, fuzzy attacks, and spoofing attacks (altering key vehicle data like the drive gear or the RPM gauge). Our dataset is generated such that it reflects real-time attacks and contains extensive features for the detection of attacks. The Car-Hacking dataset is shown in Table 1, showing that there are many normal samples in the dataset and far fewer attack samples, which is an important factor affecting the evaluation of cyber-attack detection models.

Table 1. Car-Hacking dataset class distribution.

Class	Instances
Normal	701,832
Attack	116,608

The Car-Hacking dataset includes various attack scenarios:

1. **DoS Attack:** The attacker injects the CAN ID message ’0000’ at frequent intervals (every 0.3 ms), overwhelming the network with invalid data.

2. **Fuzzy Attack:** Randomized CAN ID and data values are injected every 0.5 ms, creating inconsistencies and causing network disruptions.

3. **Spoofing Attack (RPM/Gear):** Specific CAN ID messages related to gear and RPM data are injected every millisecond, misleading the vehicle’s control units about the vehicle’s status.

Each entry in the dataset consists of several attributes:

- **Timestamp:** The time when the data is recorded (in seconds).

- **CAN ID:** A unique identifier for the CAN message, typically represented in hexadecimal (e.g., ’043f’).

- **DLC:** The number of data bytes in the message (ranging from 0 to 8).

- **DATA:** The data values for each byte in the CAN message (e.g., DATA {0}, DATA {1}, ..., DATA {7}).

- **Flag:** Indicates whether the message is normal ('R' for real) or injected ('T' for injected).

The number of normal messages is larger than attack messages, multiple resampling techniques are used to further cope with this imbalance within the dataset. These techniques include:

- **Oversampling:** Random Over-Sampling (ROS) is employed to inflate the quantity of attack information to stabilize the class distribution.
- **Under sampling:** Some techniques like NearMiss are used for getting a subset of the majority class (normal data) that is closer to the minority class (attack data), thus providing good balance without overfitting.
- **Hybrid Resampling:** Tomek Links works as a data-cleaning method and is used for removing instances overlapping between the majority and minority classes, as the training dataset should be as cleansed and accurate as possible.

These preprocessing techniques are necessary for training deep learning models such as CNN, RNN, LSTM, BERT, and RoBERTa. These models can identify sophisticated configurations and indicate cyber-attacks that the traditional method may not cover, and also, the deep learning models are trained and tested upon the Car-Hacking dataset to identify attacks based on real-time conditions to minimize false positives and false negatives. Model performance is evaluated with metrics like accuracy, precision, recall, and F1-score. As a result, these measures enable an overall assessment of the IDS's efficiency in accurately detecting normal and attack data with high accuracy in order to ensure that cyber threats are being successfully identified and effectively offensive averted amongst the autonomous vehicle systems.

3.2 Data Preparation and Pre-processing

In this phase, we work on overcoming the imbalance presented by the dataset, since the number of normal instances is greatly higher than the number of attack ones. For data imbalance, we use resampling methods like NearMiss, Random over-sampling (ROS), and Tomek Links. When the learning model is trained on these imbalanced datasets, the model focuses more on the majority class data points while the minority class data points are usually neglected.

- **NearMiss:** The method chooses the instance from the majority class which is the closest to the instance of the minority class.
- **Random Over-Sampling (ROS):** It simply makes identical copies of instances from minority class until its instances are equal to the majority class instance
- **Tomek Links:** A data cleaning method that acts on the classes by removing any duplicate instances.

By applying these resampling methods, the dataset is balanced, providing a solid foundation for training deep learning models.

3.3 Training and Testing of Deep Learning Models

After pre-processing the data, the dataset is divided into two sections: a training set and a testing set, often in a 70-30 split. Pre-processed data is used to train the selected deep-learning models for attack detection. In this stage, we use a few state-of-the-art deep learning architectures:

- CNNs to recognize spatial patterns within the dataset.
- Use of RNNs and Long Short-Term Memory (LSTM) networks for sequential data analysis and capturing time-dependent attack patterns.
- Bidirectional Encoder Representations from Transformers (BERT) for mining spatial and contextual information from the data, especially valuable when large and complex datasets are present.
- A Robustly Optimized BERT Pretraining Approach (RoBERTa) to harness deep contextual representation of the data.

Different deep learning models were trained on the balanced dataset to make them perform better. To measure how well models could detect attacks, accuracy, precision, recall and F1-score were all used. The data for the Car-Hacking dataset was created with a controlled computer simulation of real attacks against automated vehicle networks. It includes details from different attacks such as DoS attacks, spoofing and message injection and every data point provides you with CAN ID, timestamp, data bytes and message flags. Careful balancing was done by means of vehicle-to-vehicle (V2V) simulations and by noticing which vehicle network features such as CAN bus data and sensor data were most important.

Hyperparameters like learning rate, how many layers the model has and batch size were all optimized during the training phase. Setting the learning rate to 0.001

allowed the model to converge better. CNN only had three layers, while the LSTM and RNN models included five to help capture both type of features. A batch size of 32 helped ensure the model learned fast and was not overfit, and settings were found by trying different combinations with grid search.

3.4 Car Attack Detection and Classification

In this stage, the deep learning models are validated on the testing data. The goal is to discretely detect whether each data point belongs to a normal class (negative) or an attack class (positive). Each model is evaluated based on multiple classification metrics:

- **Accuracy:** Ratio of correct predictions (of normal and attack) to total predictions.
- **Precision:** Number of true positive attack predictions over total predicted attacks.
- **Recall:** The number of true attack predictions over the total number of attacks.
- **F1-Score:** The harmonic means of the precision and recall, offering a balanced statistic for the performance of the model.

The model is assessed in terms of its speed and accuracy, making sure the streaming traffic is correctly screened into attack and non-attack traffic groups in real time. The steps for the framework workflow are to gather data, test models, make predictions, use sampling techniques (NearMiss, ROS, TomekLinks), handle data imbalances, create a test and training set, and use different models (CNN, RNN, LSTM, BERT, RoBERTa). Jamming attacks are detected using an analysis of how messages are sent over the CAN bus, spoofing is found by looking for differences in sensor readings, and applying different sensors and other attacks are identified through a detailed analysis of system data. In this case, CNNs are used to find spatial features, and LSTM models check for suspicious changes in time, mostly with DoS attacks.

Algorithm 1: Car Hacking Detection Framework Using Deep Learning

```
Data: Raw car hacking dataset (D) with features
        (X) and target (Y)
Result: Classify Car Hacking in IoVs
Import necessary libraries for data manipulation
  (e.g., pandas, numpy);
Import deep learning libraries (e.g., TensorFlow,
  Keras, PyTorch);
Import resampling techniques (NearMiss,
  RandomOverSampler, TomekLinks);
Load the raw car hacking dataset (D) into a
  DataFrame;
Separate the dataset into features (X) and target
  (Y);
Use resampling techniques (NearMiss,
  RandomOverSampler, TomekLinks) to balance
  the dataset;
Split the dataset into training and testing sets
  (70%-30% split);
Train CNN, RNN, LSTM, BERT, and RoBERTa
  models on the training data;
Perform model fine-tuning and hyperparameter
  optimization;
Test the trained models on the testing set and
  generate evaluation metrics (accuracy, precision,
  recall, F1-score);
```

Pseudocode 1 outlines steps for Detecting Cyber-Attacks (in this case, Car Hacking) in Autonomous Vehicle Systems. We first, import necessary libraries that are used for data manipulation (pandas, numpy) and deep learning (TensorFlow, Keras, PyTorch) then the raw car hacking data frame is being loaded, and features (X) and target (Y) are separated. Resampling techniques such as Random Over-Sampling (ROS), NearMiss, and Tomek Links are employed to handle class imbalance within the dataset. We Split the dataset into training and testing (70% - 30%) then train deep learning models (CNN, RNN, LSTM, BERT, and RoBERTa) on training data (including fine-tuning and hyperparameter optimization) and finally, the models are tested against the testing set to get the accuracy, precision, recall, and F1-score. All metrics are calculated to evaluate the performance of the models in detecting cyberattacks. Using this pipeline provides a structured methodology for dealing with the Car-Hacking dataset, from preprocessing and resampling of the imbalanced classes to training and evaluation of the deep learning classifier.

3.5 Suggested High-Level IDS-IoV Framework for Car Attack Prediction

A multilayer framework has been developed that utilizes the power of cloud computing, deep learning, and resampling algorithms to predict the potential future attacks under Internet of Vehicles (IoV) systems. This framework proficiently solves the complexities of vehicle attack detection and prediction owing to a mixture of Resampling Techniques (RTs) and Deep Learning (DL). This top-level infrastructure is an IDS-IoV system for smart cities that will be able to provide proactive security for autonomous vehicles dealing with real-time data and time-sensitive decisions. In particular, the methodology is designed to help vehicle security engineers with the ability to anticipate a potential attack from real-world conditions by utilizing the Internet of Vehicles (IoV), Cloud Computing, and Deep Learning for ongoing monitoring and protection of vehicle communications. The frameworks also implement AI prediction systems so that security experts can analyze the visible and invisible AI systems before responding to any security threat. The architecture consists of three fundamental phases acting in concert to deliver the system goals:

Stage 1: Data Collection and Transmission to Cloud Servers

At this level, vehicle systems (for example, car hacking detection systems) will send information of the vehicle behavior and the vehicle network interactions to the cloud system. These cloud systems become the nerve center where vast amounts of data are processed in real-time from autonomous vehicles. The data sent to the cloud is used for additional analytics to detect abnormal behaviors and potential cyberattacks on the internal and external networks of the car. At this stage, Deep Learning Models (e.g., CNN, RNN, LSTM, BERT, and RoBERTa) are used to analyze data streams and predict potential vulnerabilities or attacks on vehicle systems. The data vehicle also includes sensor readings, network data, vehicle-to-vehicle communication, vehicle-to-infrastructure communication, and much more. It can also utilize state-of-the-art deep learning algorithms to detect new attack vectors and anomalies in the vehicle network in real-time.

Stage 2: Data Processing, Analysis, and Attack Forecasting

After data is generated, it is sent to the cloud servers for processing and storage. AI models, especially deep learning algorithms, process and categorize the data within the cloud to understand the characteristics of potential cyber attackers. Cloud computing offers the necessary computational capabilities required for processing large datasets, including attack detection as well as attack predictions against vehicles. Patterns of normal and abnormal behavior are learned, and these are used to predict potential attacks. Deep learning models (e.g. LSTM, which works on sequential data, BERT, which works on both spatial and contextual analysis, and RoBERTa, which creates abstraction levels for recognizing complex patterns of understanding communication traffic) help to create highly accurate predictions of the known and unknown threats against the systems of the vehicle. Using historical data to predict future attempts at attacks enables security experts to take action before an attack even happens.

Stage 3: Cloud-Based Monitoring, Security Decision-Making, and Threat Detection

In the last stage, a cloud-based dashboard helps and monitoring application is utilized to help vehicle security investigators recognize and identify threats in wise urban areas. It gives security engineers real-time insight gathered from AI-predictive and deep learning-based analytics. Good uses a dashboard for security professionals with which they can access the relevant streams of data from the vehicles, and can detect attacks and make decisions based on the severity of the attacks. For security experts, providing an overview of vehicle network behavior and potential vulnerabilities or immediate threats will improve the overall effect of the attack detection framework at this stage. Additionally, the prediction system can be on the cloud, which can help in integrating predictive analytics to enable quick decision-making to counter vehicle network attacks, thereby keeping the vehicle and passengers safe.

3.6 Cloud Computing and AI Integration

Cloud computing and AI are introduced here to strengthen smart city plans, specifically by anticipating vehicle abuses. The system continuously gathers data from many sources and uses sophisticated models to spot unusual activities and cyber threats. Using AI on the cloud helps improve the detection of cyber security threats which helps secure autonomous vehicles in any changing situation. Through cloud computing, processors can effectively handle large sets of data, supporting capability for detecting more threats. Advances in cloud computing now make it practical to analyze a lot of data collected by AVs which helps spot cyber threats in real time. Cloud systems powered by AI are able to watch network traffic in vehicles, study ways attacks occur and warn the security team whenever problems arise. Cloud platforms work well for IDS systems in smart cities because they are scalable and flexible, handling all the data from numerous vehicles to make the IoV safer.

4 Results Analysis and Assessment

In this section, we provide the report results of the deep learning-based attack detection framework applied to the Car-Hacking dataset. The performance of the proposed deep learning models (CNN, RNN, LSTM, BERT, and RoBERTa) for detecting and classifying cyber-attacks on autonomous vehicle systems in the Internet of Vehicles (IoV) is evaluated in this study. We evaluate the performance of different models based on metrics such as accuracy, precision, recall, and F1-score.

4.1 Experimental Setup

In testing and evaluating the deep-learning models, we used the Car-Hacking dataset. This dataset is heavily unbalanced with a considerable imbalance towards the class of normal data compared to the data of attack. Multiple resampling techniques were used to mitigate this imbalance, including the Random Over-Sampling (ROS), NearMiss, and Tomek Links. These approaches guaranteed the dataset was balanced prior to training the models. The data is divided into training and testing comprising 70%–30% of the data, in which 70% of the data is used to train the models and 30% for evaluation. Below are the models that were trained on this balanced dataset:

- **Convolutional Neural Networks (CNN):** Used to detect spatial features and patterns in the data.
- **Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM):** To model sequential dependencies and temporal attack trends.
- **BERT:** Bidirectional Encoder Representations from Transformers (BERT) that are used to process spatial and contextual data.
- **A Robustly Optimized BERT Pretraining Approach (RoBERTa):** Used for recognizing intricate, context-dependent patterns in vehicular communication traffic.

4.2 Performance Evaluation

Finally, the performance of every model was measured on the following metrics:

- **Accuracy:** Correctly classified instances (normal and attack) over the total instance.
- **True Positive Rate:** The rate of all predicted attack instances that are true positives.
- **Recall:** The ratio of all true positive attack predictions to actual attack instances.
- **F1-Score:** The harmonic means of precision and recall, F1-Score provides a balanced measure of the model performance.

The results are summarized in Table 2, where the accuracy of each model was assessed via the testing dataset without the use of any resampling process. Figure 4 shows the performance of each deep learning model (CNN, RNN, LSTM, BERT, RoBERTa) on the test dataset when resampling techniques are without application. It helps to visualize how each model compares based on Accuracy, Precision, Recall, and F1-score.

This Table 2 presents the evaluation of deep learning models (CNN, RNN, LSTM, BERT, RoBERTa) on the test dataset without applying resampling techniques. It demonstrates the baseline performance of these models.

Table 2. Performance of models without resampling.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	95	94	91	92
RNN	94	93	92	91
LSTM	96	94	92	94
BERT	97	96	93	95
RoBERTa	99	98	95	97

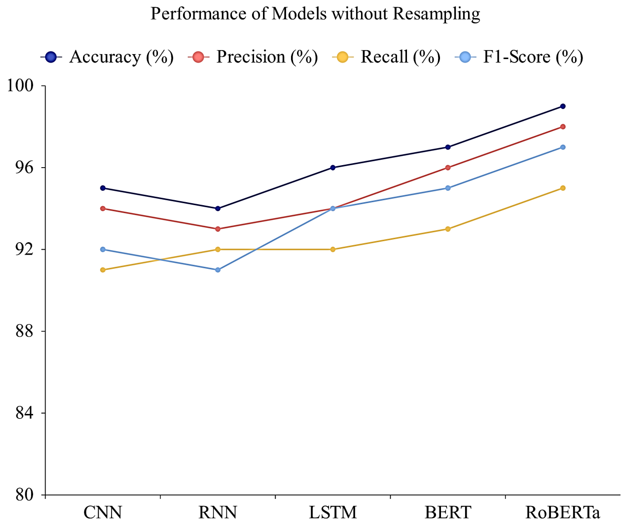


Figure 4. Performance of models without resampling.

It has been observed that RoBERTa outperformed all other models in accuracy (99%), precision (98%), recall (95%) and F1-score (97%). Followed closely by BERT, which achieved an accuracy of 97%, precision of 96%, and recall of 93%. Other ML models with promising results, but with lower accuracy, were LSTM, CNN, and RNN, which all showed a for example high value for recall, which is an important evaluation metric, especially in filters over unbalanced datasets, like an attack detection filter.

4.3 Resampling Techniques Impact

To improve how well the models recognized attacks, we used three types of resampling methods, Random Over-Sampling (ROS), NearMiss and Tomek Links, to equalize the number of different classes in our data. With these techniques in place, the model worked much better at catching evidence of attacks. To catch less common attacks, ROS makes another instance from the same attack class. Even so, it could cause overfitting because the model will concentrate too much on repeated parts of the data. For this reason, NearMiss gets a smaller number of normal class examples and instead picks instances that are similar to the examples from the minority class. Removing close and noisy samples, Tomek Links helps raise the quality of the dataset. These techniques together allow the model to identify attacks more effectively and to not become overly specific.

4.3.1 Random Over-Sampling (ROS)

To boost the number of attack entries within the data set and to make the models used more sensitive to attack patterns, ROS was utilized. The performance for models trained with ROS is presented in Table 3. The model performance after doing Random Over-Sampling (ROS) also has been shown in Figure 5. This shows your accuracy, recall, and F1-score, and how much better the RoBERTa model works than all other models in all metrics.

This Table 3 summarizes the results of applying Random Over-Sampling (ROS) to the models. It highlights the improvement in recall and F1-score after resampling is applied.

Overall, using ROS pushes RoBERTa past the top-performing model on all metrics, and although BERT is performing reasonably well, it lags well behind when it comes to the recall and F1-score. The models have been made more sensitive to detect cyber-attacks, as there is an improvement in accuracy and recall for all the models.

Table 3. Comparison of model performance with different resampling techniques (random over-sampling).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	94	92	92	93
RNN	95	93	92	93
LSTM	96	97	96	96
BERT	97	97	98	97
RoBERTa	99	98	98	97

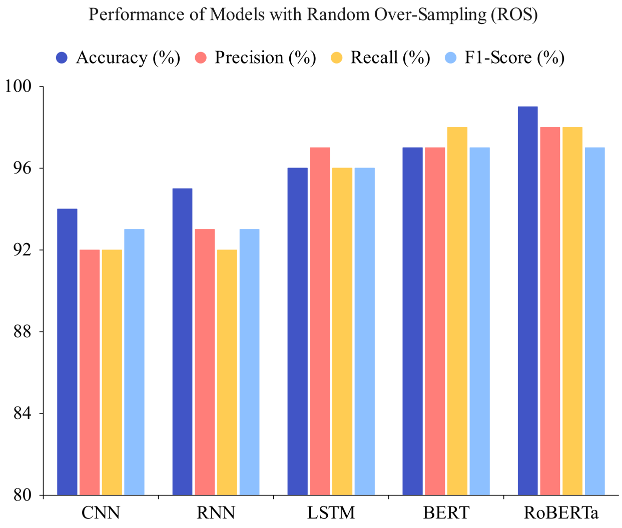


Figure 5. Performance of models with random over-sampling (ROS).

4.3.2 NearMiss

NearMiss is a method that is considered under-sampling, which removes a small number of majority examples (those samples from the normal class), in order to enhance the performance of the created model. Results for models trained with NearMiss are given in Table 4. Model performance comparison after Near Miss is illustrated in Figure 6. The graph lays down the statistics of the precision and recall and we can visually comprehend the encountered sensitivity of the attack instances of the models essentially in the case of BERT and RoBERTa.

This Table 4 presents the model performance after applying the NearMiss technique, showing the changes in precision and recall due to under-sampling.

While the LSTM and RoBERTa models show the most improvement in terms of recall, they are particularly better for rare attacks and outlier detection in the network. The accuracy for certain models, however, was slightly lower due to the reduced number of

Table 4. Comparison of model performance with nearMiss.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	94	92	88	90
RNN	93	91	85	88
LSTM	95	95	92	93
BERT	97	96	93	94
RoBERTa	98	96	95	95

Table 5. Comparison of model performance with tomek links.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	96	95	92	93
RNN	96	95	92	93
LSTM	97	96	94	94
BERT	97	97	95	95
RoBERTa	98	98	96	97

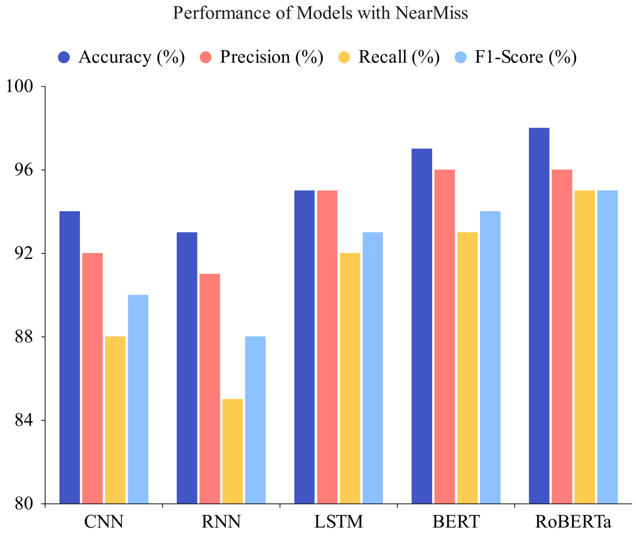


Figure 6. Performance of models with nearMiss.

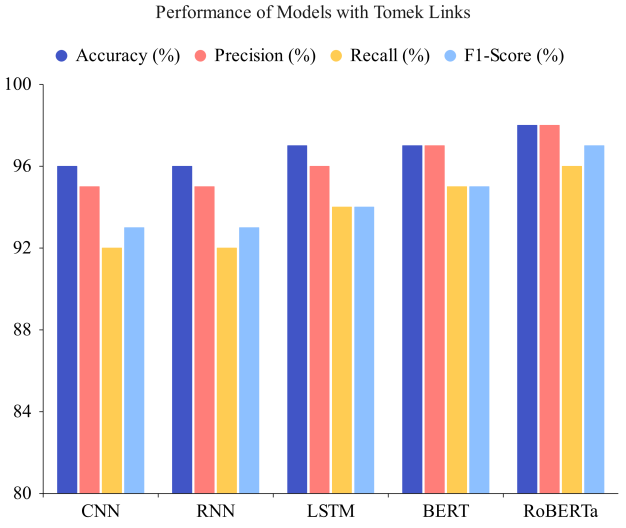


Figure 7. Performance of models with tomek links.

majority-class samples.

4.3.3 Tomek Links

To clean the dataset and remove overlapping instances from the majority class and from the minority class, Tomek Links was implemented. BERT and RoBERTa showed significant improvement in F1 scores after applying this data-cleaning technique. Table 5 displays the results of models trained with Tomek Links. We now use the Tomek Links data-cleaning technique, and below Figure 7 shows the performance of the models. It shows the improvements in F1-scores and precision of the cleaning process, with significant gains around RoBERTa.

This Table 5 shows the performance of models after the application of Tomek Links, highlighting improvements in F1-scores and precision.

Both models are very suitable for the detection of such real-time attacks in the Internet of Vehicles systems, as RoBERTa was still the best-performing model and BERT also showed great progress in precision and recall.

4.4 Real-Time Attack Detection

The suggested approach with deep learning and cloud computing is able to detect any attack in real-time on autonomous vehicles. As it processes real-time data quickly, the system can spot and address cyber-attacks right away which is very important for avoiding disastrous results. Because of cloud computing, the system is better able to cope with large IoV networks. With a Denial-of-Service (DoS) attack, the IDS spots sudden changes in the number of messages and reports accordingly. When spoofing takes place and sensor readings are modified, the system checks the new values against those usual for that time of day and uses sensor fusion to see if they differ. It is also possible to see irregular movement using temporal and spatial analysis which can be linked to message injection. As a consequence, the IDS protects autonomous vehicle systems from both usual and complex attacks.

5 Conclusion and Future Work

Investigations in this paper presented a sophisticated Intrusion Detection System based on deep learning for connected cars within IoV framework, by applying models such as CNN, RNN, LSTM, BERT and RoBERTa for timely monitoring of cyber-attacks. To correct the unbalanced nature of the car-hacking data, we used resampling techniques (ROS, NearMiss and Tomek Links) and that improved the detection rate. Traditional machine learning models were outperformed by the framework in catching message injection, sensor spoofing and attacks designed to overload the system. Real-time data processing is possible with cloud computing which plays a key role in changing AV systems. Because of the BERT and RoBERTa models, carmakers now recognize more advanced cyber threats.

Future work will focus on expanding the dataset for broader vehicle manufacturer coverage, using multi-modal data, and testing the IDS in real-world operational environments. It will also consider reinforcement learning which helps the model respond to modern attacks and try to improve the model's performance for quick, real-time identification. Working with regulatory agencies to set up standard cybersecurity guidelines for AVs will make vehicle networks more protected. Having an IDS useful in large-scale setups is a major research challenge for the future.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] AlEisa, H. N., Alrowais, F., Allafi, R., Almalki, N. S., Faqih, R., Marzouk, R., ... & Ibrahim, S. S. (2023). Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning. *IEEE Transactions on Consumer Electronics, 70*(1), 1736-1746. [Crossref]

[2] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences, 12*(3), 1598. [Crossref]

[3] Setitra, M. A., & Fan, M. (2024). Detection of DDoS attacks in SDN-based VANET using optimized TabNet. *Computer Standards & Interfaces, 90*, 103845. [Crossref]

[4] Sun, X., Yu, F. R., & Zhang, P. (2021). A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems, 23*(7), 6240-6259. [Crossref]

[5] Bilal, H., Ahmed, F., Aslam, M. S., Li, Q., Hou, J., & Yin, B. (2024). A blockchain-enabled approach for privacy-protected data sharing in internet of robotic things networks. *Humcent Comput Inf Sci, 14*(1), 71. [Crossref]

[6] Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. *IEEE Open Journal of Vehicular Technology, 5*, 869-906. [Crossref]

[7] Bergies, S., Aljohani, T. M., Su, S. F., & Elsisi, M. (2024). An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54*(9), 5717-5732. [Crossref]

[8] Anand, M., Kumar, S. P., Selvi, M., SVN, S. K., Ram, G. D., & Kannan, A. (2023, March). Deep learning model based IDS for detecting cyber attacks in IoT based smart vehicle network. In *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 281-286). IEEE. [Crossref]

[9] Wazid, M., Singh, J., Pandey, C., Sherratt, R. S., Das, A. K., Giri, D., & Park, Y. (2025). Explainable deep Learning-Enabled malware attack detection for IoT-Enabled intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 26(5), 7231-7244. [Crossref]

[10] Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. *Technologies, 11*(5), 117. [Crossref]

[11] Sepehrzad, R., Khodadadi, A., Adinehpour, S., & Karimi, M. (2024). A multi-agent deep reinforcement learning paradigm to improve the robustness and resilience of grid connected electric vehicle charging stations against the destructive effects of cyber-attacks. *Energy, 307*, 132669. [Crossref]

[12] Anbalagan, S., Raja, G., Gurumoorthy, S., Suresh, R. D., & Dev, K. (2023). IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems, 24*(12), 15866-15875. [Crossref]

[13] Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., ... & Tsolis, D.

(2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. *Journal of Cybersecurity and Privacy, 3*(3), 493-543. [Crossref]

[14] Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials, 25*(3), 1775-1807. [Crossref]

[15] Haider, Z. A., Khan, F. M., Zafar, A., & Khan, I. U. (2024). Optimizing Machine Learning Classifiers for Credit Card Fraud Detection on Highly Imbalanced Datasets Using PCA and SMOTE Techniques. *VAWKUM Transactions on Computer Sciences, 12*(2), 28-49. [Crossref]

[16] Al Isawi, O. A., Al Jaafari, K. A., & Al Sumaiti, A. S. (2025). Electric Vehicles CAN Bus Cyber Attacks Detection Using Adaptive Neuro Fuzzy Inference System. *IEEE Access, 13*, 90862-90874. [Crossref]

[17] Aloraini, F., Javed, A., & Rana, O. (2024). Adversarial attacks on intrusion detection systems in in-vehicle networks of connected and autonomous vehicles. *Sensors, 24*(12), 3848. [Crossref]

[18] Iqubal, A., & Tiwari, S. K. (2024, November). Internet of Vehicle (IoV) Cyber Attack Detection using Machine Learning Techniques. In *2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 1053-1057). IEEE. [Crossref]

[19] Campisi, T., Severino, A., Al-Rashid, M. A., & Pau, G. (2021). The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities. *Infrastructures, 6*(7), 100. [Crossref]

[20] Arshad, I., Alsamhi, S. H., Qiao, Y., Lee, B., & Ye, Y. (2023). A novel framework for smart cyber defence: a deep-dive into deep learning attacks and defences. *IEEE Access, 11*, 88527-88548. [Crossref]

[21] Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., & Linkov, I. (2022). An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks. *IEEE Transactions on Intelligent Transportation Systems, 24*(1), 1000-1014. [Crossref]

[22] Gupta, S., Maple, C., & Passerone, R. (2023). An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles. *IEEE Access, 11*, 90641-90669. [Crossref]

[23] Ramesh, S. N., Al Fardan, B. M. M., Anupama, C. S. S., Kumar, K. V., Cho, S., Acharya, S., & Yoon, C. (2025). Leveraging Cyberattack News Tweets for Advanced Threat Detection and Classification Using Ensemble of Deep Learning Models With Wolverine Optimization Algorithm. *IEEE Access, 13*, 48343-48358. [Crossref]

[24] Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems, 24*(4), 3614-3637. [Crossref]

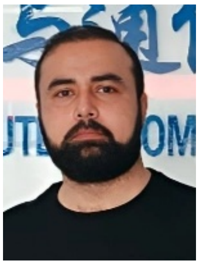
[25] Ghrib, T., Benmohammed, M., & Pandey, P. S. (2021). Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques. *Bulletin of Electrical Engineering and Informatics, 10*(2), 950-961. [Crossref]

Fida Muhammad Khan received his MS in Computer Science from the University of Science and Technology, Bannu, Pakistan in 2021. Currently, he is pursuing his Ph.D. degree in Computer Science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. His research interests include Data Mining, Cybersecurity, IoT, Machine Learning, Deep Learning, and Natural Language processing (NLP). (Email: fida5073@gmail.com)

Mr. Zeeshan Ali Haider is currently pursuing a Ph.D in computer science at Qurtuba University of Science and Information Technology, Peshawar, Pakistan. He holds an MS in Computer Science from Abasyn University, Peshawar, Pakistan, where he was awarded distinction, and a BS in Computer Science from Islamia College, Peshawar, Pakistan. He has also published a book chapter in a top-tier journal. His research interests encompass a wide range of fields, including the Internet of Vehicles (IoV), Cybersecurity, Cryptography, Blockchain, Machine Learning, Deep Learning, the Internet of Things (IoT), and Data Mining. (Email: Zeeshan.ali9049@gmail.com)

Muhammad Owais Khan is an MS Computer Science candidate at the University of Science and Technology, Bannu, specializing in AI/ML, Deep Learning, and NLP. He holds a BSc in Software Engineering from the same institution and aims to advance intelligent systems for scalable problem-solving. (Email: owaiskhan.cs@outlook.com)

Ashraf Ullah received his MS degree in Computer Science from Blekinge Institute of Technology (BTH), Sweden. He completed his Ph.D. degree in Computer Science at the University of Science and Technology (UST), Bannu, Pakistan. His research interests include Information Management, Natural Language Processing (NLP), Data Science, and Artificial Intelligence (AI). (Email: ashrafbth@gmail.com)



Muhammad Shoaib Khan received his master's degree from the University of Science & Technology Bannu, Pakistan, in 2022. Currently he is pursuing his PhD degree from the School of Computer and Communication Engineering at University of Science and Technology Beijing (USTB), China, from 2023. His research interests include DevOps, software modeling and specification, IoT, network security, machine learning, big data, and anomaly detection in social networks. (Email: imkhan101@outlook.com)

Muhammad Fayaz completed his bachelor's degree from Islamia College University Peshawar and earned a master's degree in Computer Engineering, specializing in computer vision, deep learning, and machine learning, from the Department of Computer Engineering at Cyprus International University, Turkish Republic of Northern Cyprus. He is currently a research assistant at the Computer Vision and Pattern Recognition (CVPR) Laboratory at Sejong University. His research interests span computer vision, deep learning, and machine learning, with a particular focus on both medical image analysis and land cover classification. In the realm of medical image analysis, he is contributing to the development of advanced techniques for image classification and segmentation, aimed at improving diagnostic accuracy and medical decision-making. His work in land cover classification focuses on leveraging deep learning to analyze satellite and aerial imagery, enabling more effective monitoring of environmental changes, and land cover shifts, and supporting sustainable development. Through his interdisciplinary approach, Muhammad is making significant contributions to both fields, using state-of-the-art computational methods to solve complex challenges in medical imaging and environmental monitoring. (Email: muhammadfayaz@sju.ac.kr)

Mushtaq Ahmad is currently pursuing an MS in Informatics Data Science at the Department of Business informatics, technical University of Vienna (TUWIEN), Austria. He completed his BS degree at Islamia College, Peshawar. His research focuses on Data Mining, NLP, Machine Learning, and Cybersecurity. (Email: mushtaq8653@gmail.com)

Nabila is currently pursuing masters in Computer Science and Engineering at Bangladesh University of Professionals, Dhaka, Bangladesh. She did her Bsc in Computer Science and Engineering at Southern University Bangladesh, Chittagong, Bangladesh. Her research interests include Cryptography, Cyber Security, Machine Learning, Deep Learning and Blockchain Technology. (Email: nabila@southern.ac.bd)