

Enhancing V2X Communication Security Using an MTCNN-LSTM-Based Multilevel Trust Evaluation Framework

Sanjay Kumar Sonker

sanjayknphbti@gmail.com

Sharda University

Bharat Bhushan Sagar

Harcourt Butler Technical University

Vibha Kaw Raina

Birla Institute of Technology, Mesra

Md Khalid Jamal

Sharda University

Research Article

Keywords: Smart grid, RSUs, Electrical vehicle(EV), V2X, CNN-LSTM, Trust management

Posted Date: September 18th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10914058/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Enhancing V2X Communication Security Using an MTCNN-LSTM-Based Multilevel Trust Evaluation Framework

Sanjay Kumar Sonker^{1*}, Bharat Bhushan Sagar^{2†},
Vibha Kaw Raina^{3†}, Md Khalid Jamal^{4†}

^{1,4*}CSA, Sharda School of Computing Science and Engineering, Sharda
University, , Grater Noida, 201310, Uttar Pradesh, India..

²CSE, Harcourt Butler Technical University, Street, Kanpur, 208002,
Uttar Pradesh, india..

³CSE, Birla Institute of Technology, Mesra, Ranchi, 835215, Jharkhand,
India..

*Corresponding author(s). E-mail(s): sanjayknphbti@gmail.com;

Contributing authors: bbsagar@hbtu.ac.in; vibhakaw@bitmesra.ac.in;
drkhalidjamal28@gmail.com;

[†]These authors contributed equally to this work.

Abstract

In the evolution of V2X infrastructure deployment, vehicle-to-everything (V2X) communication necessitates authentication, privacy, and dependability. Securing the V2X networks and charging issues is critical and more challenging due to the extensive infrastructure. This direction enables trust-based transactions between electric vehicles and the smart grid to fulfill energy consumption. This paper reveals the closed-loop V2X security and energy allocation system that integrates real-time multi-attack detection, dynamic trust evaluation, and battery optimization in an intelligent transportation system. In the proposed MTCNN-LSTM model, which incorporates multilevel trust and CNN-LSTM, we achieve 94.75% accuracy, 94.83% weighted F1-score, and 99.3% attack detection rate across four attack types (none, sybil, DDoS, and both). Trust based on nine telemetry features (security score, feedback score, behavior score, message frequency, message received, energy consumed, SoC, security score difference, energy consumed rate) It also optimizes the battery consumption during the attack, ensuring that the system can maintain functionality by detecting energy wastage based on the

MTCNN-LSTM model, energy waste: 550 kWh at 30 % attack out of the supply by smart grid 2000 kWh for the given dataset "Electric Vehicle Trip Energy Consumption Data" in the simulation based on real data, class-weighted training and multi-speed validation to ensuring secure, resilient and sustainable energy in smart grid enabled V2X network.

Keywords: Smart grid, RSUs, Electrical vehicle(EV), V2X, CNN-LSTM, Trust management

1 Introduction

In the Vehicle-to-everything (V2X) ecosystem, cybersecurity issues can be driven by the security of communication links, security for electric vehicles, identity and liability, access control, vehicle privacy, and overall security based on IDS[1]. The Internet of Vehicles(IoV) is an extension of the V2X network. The protection of IoV systems against dynamic cyber attacks that compromise their operation is mandatory to ensure the safety of their users. Several security mechanisms can be applied to improve the security of V2X. One of the primary mechanisms explored is trust-based security. [2] The Internet of Vehicles (IoV) is a sophisticated extension of the Internet of Things (IoT), focusing on vehicle networks. Integrated systems comprise sensors, communication devices, and processing technologies and provide a seamless connection between the vehicle, charging stations, and the cloud or fog nodes. Smart vehicles can communicate in real-time with infrastructure, vehicle-to-infrastructure, charging station-to-smart grid, people, or other devices. [3] IoV is susceptible to denial of service for internal attacks; DoS attacks could turn off or overwhelm the communication infrastructure, disrupting the data flow between vehicles and traffic lights, traffic lights to charging stations, and charging stations to the smart grid or emergency services. An attacker can breach the connection and take command and control over the charging station due to the dynamic connection between electric vehicles and the grid via charging stations. Deep learning algorithms such as LSTM and GRU perform better than traditional ML algorithms, because of their superior ability to analyze the temporal dependencies included in IoV data[4]. An overview of security issues related to the V2X infrastructure and highlights open problems that will make V2X security a challenging research area in the future.[5]

1.1 Security Challenges and Solution

Fog nodes with road side units(RSU) are installed on the traffic lights between the electrical vehicles (EVs) and charging stations to improve security as will minimize network traffic for illustration, consider the number of RSUs in a given area that can respond quickly to vehicle demands by providing resources and making decisions—all without submitting the request to the cloud via fog node install on RSU and waiting for a response. The Internet of Vehicles is especially susceptible to attacks such as DoS/DDoS and sybil attacks due to its heavy reliance on wireless connectivity.[6]

- **Denial of Service (DoS) attacks on V2X** In V2X networks, communication is vulnerable to different types of attacks. One is a DoS attack, where an attacker floods the infrastructure with unnecessary information. It can increase delays and overwhelm the networks.
- **Sybil attacks on V2X** In V2X communication, Sybil attacks occur when a single vehicle declares itself with multiple identities to other vehicles on the network. Therefore, the other vehicles cannot determine whether the information comes from a single vehicle or multiple vehicles[7].

1.2 Security solution for V2X communications

Advanced technologies are used in vehicle-to-thing (V2X) security solutions to establish a secure connection between vehicles and infrastructure, including intrusion detection systems (IDS) for real-time attack responses, blockchains for decentralized data management, lightweight cryptography for effective data encryption, and trust management to assess the reliability of information. These components create a robust architecture for reliable and secure V2X communication.

The security solution presents a layered architecture for V2X, as shown in Figure 1, providing a comprehensive framework for managing trust, security, and communication within electric vehicle (EV) networks. This framework leverages fog computing and a multilevel trust model[8]. At the Edge Layer, electric vehicles and charging stations generate and transmit real-time data that requires secure processing. The Network Layer uses Ethernet, 5G, WSN, and C-V2X technologies to enable seamless communication between vehicles and infrastructure. In the Data Processing Layer, RSUs equipped with fog nodes perform essential tasks, including packet capture, data cleaning, and assessing trust using a multilevel and deep learning approach to help detect attacks on V2X networks[9]. Propose a hybrid model that integrates trust computation and machine learning that allows dynamic attack detection and trust decisions. In the layered architecture for IoV in V2X, as shown in Figure 2, a comprehensive framework is provided for managing trust, security, and communication within electric vehicle (EV) networks. This framework leverages fog computing and a multilevel trust model. At the edge layer, electric vehicles and charging stations generate and transmit real-time data that requires secure processing. The network layer uses Ethernet, 5G, WSN, and C-V2X technologies to enable seamless communication between vehicles and infrastructure. In the data processing layer, roadside RSUs equipped with fog nodes perform essential tasks, including packet capture, data cleaning, and assessing trust using a multilevel and deep learning approach to help detect attacks on V2X networks[10]. The detection layer verifies the identities of electric vehicles, monitors communication protocols, and detects anomalies or malicious behavior, feeding this information into the analysis layer, which further interprets it to provide trust-based services and recommendations. At the top, the management layer handles intrusion response, stores long-term data, and communicates with the cloud server for deeper analytics, policy updates, and system-wide coordination. This layered architecture enables real-time trust computation and robust defense against cyber threats in V2X environments, making it ideal for dynamic and data-intensive vehicular networks[7]. In this paper, we propose a CNN-LSTM-based Trust approach,

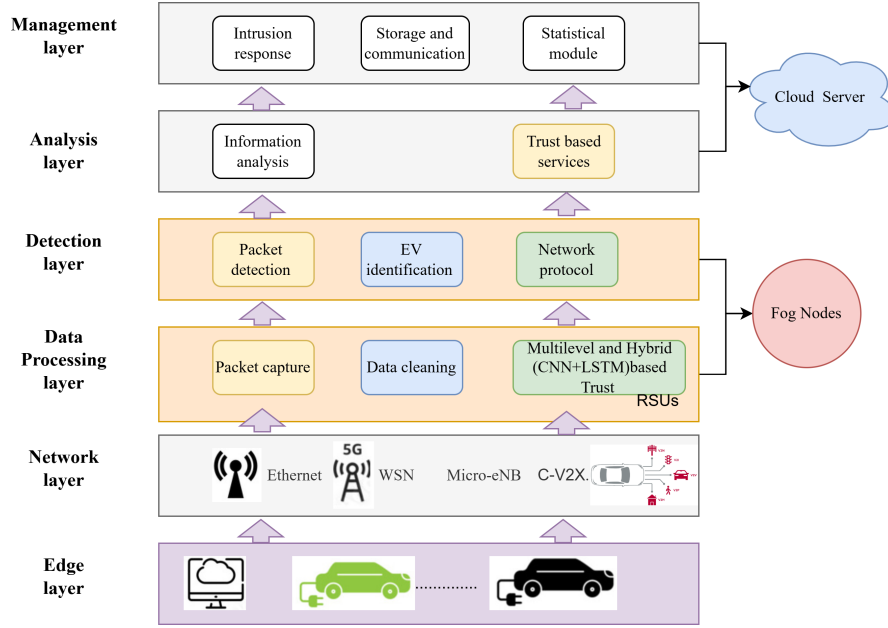


Fig. 1 V2X security solution based on trust management

namely MTCNN-LSTM, to classify attacks in V2X networks. We also present a comparison of the other existing models. Our significant contributions to this paper are highlighted here. we utilize real EV logs (SoC, current, temperature) to simulate actual V2X noise and integrate energy consumption rate, SoC, and battery temperature-based behavior anomalies into the trust layer, also detect the hybrid attack, such as Sybil, DDoS, and both in one model, after which we compute the energy allocation and battery optimization based on the multilevel trust.

1.3 Briefly of the problem

In the V2X rise the limitation of over-dependance on synthetic or static datasets, a lack of battery-conscious detection mechanisms, and computationally intensive multi-stage architectures that are unsuitable for resource-constrained EV environments. so that most of the systems cannot effectively mitigate static, dynamic, or hybrid cyber-attacks that exploit the bidirectional V2G communication channels, leading to vulnerabilities in charging authentication, data integrity, and grid coordination in intelligent transportation infrastructures.

2 Related Work

This section is divided into two parts. The first part of this section focuses on attack detection based on trust computation and machine learning. The second and final part of this section covers a significant search for machine learning-based energy allocation and battery optimization. Alnasser et al. (2019) in their paper proposed a trust-based

model for secure communication in V2X networks, their approach based on the reputation system in which the trustworthiness rate of the vehicle is based on accuracy of the information [11].

Nayak et al. (2019), A Trust-Based Distributed DoS Misbehave Detection Approach (TBDDoSA-MD) proposed for the Software-Defined Vehicular Network (SDVN); SDVN gives a high detection attack on the V2X infrastructure with an accuracy of 90% [12].

Zhang et al. (2020) proposed a trust model for electric vehicles (EVs) that integrates behavior analysis and security scores. The model dynamically updates trust levels and achieves 90% accuracy in detecting Sybil attacks while reducing false positives by at least 15%. It mitigates Sybil attacks by aggregating feedback from multiple nodes within the network proximity [13].

In this paper, Qian and Zhang et al. (2024) show the trust prediction results with high performance with models such as XGBoost and CNN, and further improved performance at the multi-minute level with deep learning models [14].

Hb tula et al.(2024) The authors proposed dedicated short-range communications(DSRC) in V2X networks to detect Sybil attacks with a high detection rate of over 98% [7].

Faizan Ullah et al.(2024) proposed the Deep Trust framework in this paper. In addition, they demonstrated with existing methods, demonstrating improved accuracy in identifying trustworthy versus untrustworthy devices, thus significantly improving accuracy 15%, precision 20%, and recall rates 18% compared to CNN models [15].

Moghadasli et al.(2022) proposed a trust-based model that highlights the importance of secure supply chains for the V2G infrastructure. Identified critical vulnerabilities in the hardware components of electric vehicles and their potential impact on grid reliability and user safety. Design the multimetric trust model to detect and control sybill and DDoS attack in V2G [16].

Allussein et al. (2022) Proposed a deep learning-based framework to enhance security, trust and privacy in IoV environments and also used neural networks (e.g. CNN / RNN architectures) for intrusion detection, anomaly detection and trust management among connected vehicles in V2V [17].

Seong Kyung Kwon et al. (2021) author proposed the system a system to classify driving behavior into defensive, normal and aggressive categories using a 4-layer CNN-2 stacked LSTM neural network with a high classification accuracy of 98% in simulations, 97% in real-world tests and a low V2X communication delay of 4.8 ms, demonstrating its potential to improve transportation safety by mitigating risks associated with aggressive driving. After reading the literature on trust management for automotive networks, one discovers that although many exciting approaches to the problem have been proposed, they all have at least one major drawback that could be more workable [18]. Cai Yanmin et al. (2024) in this paper proposed a novel Intrusion Detection System (IDS) that integrates CNN-Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) deep learning models involving a hybrid LSTM-GRU architecture, advanced data preprocessing, and training on diverse datasets CSE-CIC-IDS 2018, CICIDS 2017, CIC DoS, IoV-Hacking 2020 to detect both inter-vehicle (V2X) and intra-vehicle attacks with high accuracy rate 99.9% for network attacks

and 95.9% for vehicle hacks[19].

Qian Xu et al. (2024) in this paper proposed a machine learning-based trust management system (TMS) for connected and automated vehicles (CAV) to counter multiple misbehaviours in the Internet of Vehicles (IoV). The framework integrates basic safety messages (BSM), roadmap data, and detector data to detect misbehaviours such as constant position, random speed offset, denial of service (DoS) and grid Sybil attacks. TMS achieves high performance, with XGBoost providing F1 scores of 0.8586 to 0.9773 for per minute predictions and LSTM achieving 0.8878 to 0.9492 for multiminute predictions throughout the four misbehaviours[14]. Tejasvi Alladi et al. (2023) in this paper discuss the rapid growth of IoV and Cooperative Intelligent Transportation Systems (C-ITS), highlighting the demand for secure communication infrastructures built on Dedicated Short-Range Communication (DSRC) and 5G V2X technologies. The study points out that conventional cryptographic mechanisms alone cannot fully ensure network integrity and should be complemented by intelligent intrusion detection frameworks. To this end, the authors introduce Deep Learning Classification Engines (DCLE), which employ single-stage or multi-stage classification using deep neural models deployed on vehicular edge servers. The proposed model utilizes three suggested classification schemes to analyze data preprocessed by RSUs before it is sent to edge servers. Compared to current benchmark approaches, the model achieves F1-scores ranging from 95.58% to 96.75%, effectively differentiating 18 distinct vehicular behavior patterns[20]. Sofia Azam et al. (2022) focused only on single attacks such as Sybil attack detection using a collaborative ensemble framework at RSUs. Five classical ML classifiers (KNN, NB, DT, SVM, LR) operate in parallel, with majority voting (hard/soft) yielding 95% accuracy and 0.1s detection latency in NS-3 simulations. Although practical and lightweight, the method lacks temporal sequence modeling and is limited to a single attack type, reducing its applicability in heterogeneous threat environments[21]. Xu et al. (2024) developed a resource allocation framework specifically for the Internet of Vehicles (IoV) to address the problem of maximizing energy efficiency in V2X communication systems[22]. Wang et al. (2024) in this article the authors investigate the behavior of electric vehicles based on the influence on batteries degradation quantitatively assessed the effects of V2X functionalities, vehicle-to-grid (V2G), vehicle-to-vehicles (V2V), and vehicle-to-infrastructure (V2I) interactions—on battery lifespan and performance stability[23]. In this section identify the research gap based on related work given in the following points.

1. Reliance on synthetic datasets both papers use VeReMi[20] and NS-3[21] simulations. No real-world 5G V2X traces with urban noise, latency, or GPS errors. Models overfit to clean data. Static attacks may be missed in real interference.
2. The absence of battery and energy features makes no mention of SoC, energy consumption, battery temperature, or charging behavior in the detection pipeline. Attackers can exploit charging through fake low SoC energy fraud undetected. No link between misbehavior and battery health.
3. No Hybrid Attack Modeling 18 misbehaviors in tiered stages only Sybi. No concurrent Sybil and DDoS or static or dynamic attacks. Real-world attackers combine threats.

4. No real-time update based on energy, behavior, and security scores. Cannot adapt to changes in attack status from benign to malicious.

3 Materials and Methods

3.1 Dataset Description:

The "Electric Vehicle Trip Energy Consumption Data" dataset, provided by ETS-Data Sharing to Advance Mobility, is a widely recognized benchmark for evaluating electric vehicle (EV) energy consumption and attack detection in simulated V2X networks[24]. This dataset captures normal driving behavior from dozens of private vehicles over several months between 2015 and 2016, with a sampling frequency of one minute per second. It contains approximately 10,000 trip records, each described by key attributes such as 'Trip Energy Consumption', 'Vehicle ID', 'Trip Distance', 'Speed', 'Current', 'Total Voltage', 'Maximum and Minimum Battery Cell Temperatures', 'Trip Time Length', and electric vehicle-related parameters. Due to its richness and temporal granularity, the dataset has been widely used as a standard testbed to evaluate energy consumption and battery optimization in smart transportation systems.

3.2 Proposed Method

The objective of the proposed MTCNN-LSTM model is to detect energy theft attacks, such as DDoS, which exhaust charging resources, and privilege attacks, such as Sybil. The framework establishes a defense boundary through trust-based energy allocation, while identifying malicious attack patterns using battery health and behavioral indicators. This hybrid model can facilitate trust-based attack detection, energy allocation, and optimize resource distribution to enhance the battery lifespan in connected vehicles. Vehicles assess the trustworthiness of their peers (V2V) based on behavior, feedback, and security score. Charging stations rely on these trust scores to authorize energy transactions, preventing misuse or identity theft by suspicious vehicles. At a higher level, the cloud server connected to the smart grid aggregates regional trust data[25]. Its main objective is to enable reliability, efficiency, and sustainability. A detailed configuration description is provided below, illustrating the communication between the Figure 2, V2X networks. Figure 4 illustrates the interaction between the V2X workflow entities.

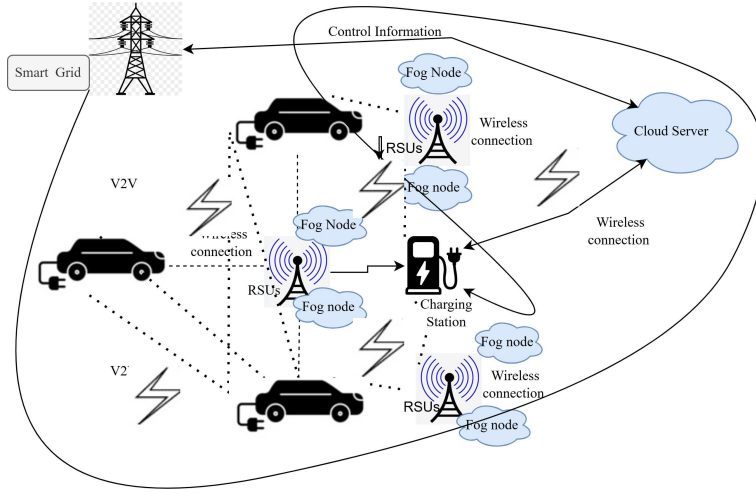


Fig. 2 V2X network infrastructure for IoV communication.

Electric vehicles (EVs) are crucial as data providers. The evaluation of EV trust involves several key parameters, such as vehicle ID, location, speed, message frequency, current, voltage, maximum temperature, minimum temperature, and state of charge, which contribute to the computation of trust in multilevel trust for V2X communication. The required steps are outlined below in accordance with the multilevel trust and deep learning approach. These are observed and assessed by RSUs with fog nodes and the cloud. The EVs initiate a connection with the charging station through the RSUs and fog nodes by sending an authentication request that contains a timestamp, location, and trust score within a multi-level trust framework, which evaluates the trustworthiness of the authentication request. Trustworthiness reflects the integrity of a vehicle, with lower local trust scores indicating potential malicious behavior such as DDoS and Sybil attacks and affecting energy allocation decisions at the charging station [14]. Charging stations serve as power delivery points for electric vehicles. They interact with electric vehicles (EVs), RSUs and the cloud to authenticate users, monitor energy usage, and detect abnormal behavior. These stations operate at the infrastructure level of the multilevel trust framework, often integrated with fog computing to process trust evaluations close to the edge. Charging stations act as an intermediary between electric vehicles and the power grid, supplying electricity to EVs if they are considered trustworthy. After authenticating the electric vehicles, the charging stations evaluate their trustworthiness and forward this information to the fog layer. Requests that the electricity needed for charging the electric vehicle be returned to the fog node from the fog server.

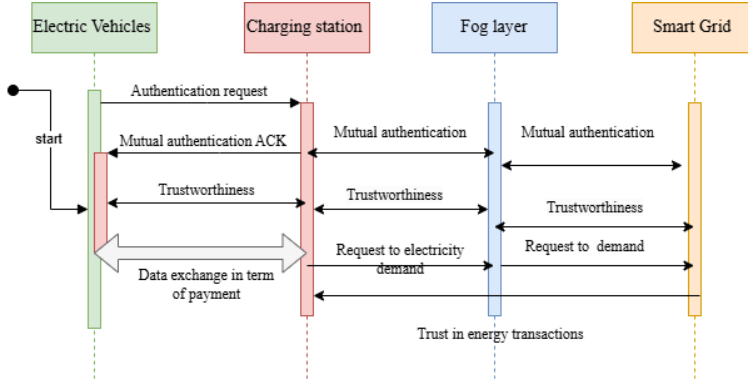


Fig. 3 V2V Communication activity between the charging station and the smart grid.

RSUs with fog nodes are interfaces to the Smart Grid and charging stations, ensuring decentralized processing, computation, and effective resource allocation. Fog nodes serve as critical intermediaries between electric vehicles, RSUs and the cloud, enabling real-time data processing, trust evaluation, and enhanced security. Positioned closer to the edge, fog nodes locally capture and clean data, significantly reducing latency and cloud communication overhead[26]. They perform multilevel trust assessments by analyzing behavior patterns, past interactions, and feedback, assigning dynamic trust scores to detect malbehaving or malicious nodes. In addition, fog nodes support the authentication of electric vehicles and messages, help detect intrusion by identifying network anomalies, and provide localized decision-making for trust-based services such as secure routing and reliable charging station selection. It gives the strength, scalability, responsiveness and resilience of the entire V2X ecosystem, making it indispensable in dynamic vehicular environments[27]. Mutual authentication is a security mechanism that ensures that both parties in a communication, typically the EV and the charging station or RSU, verify each other's identity before any data or energy exchange occurs, the fog nodes handle the local trust process, using trust scores to verify both ends. This ensures that an electric vehicle connects only to trusted charging stations and vice versa, preventing Sybil and DDoS attacks. It forwards the request for electricity demand to the Smart Grid after confirming that it is authentic and trustworthy[28].

The smart grid is an intelligent and responsive electricity distribution network that supports two-way communication between power producers and consumers[25]. In the grid trustworthiness refers to the confidence that an entity has in another based on its past behavior, security compliance and network feedback. The architecture applies CNN-LSTM combined with multilevel trust, allowing for gradual trust scoring. A higher trust score means that the node is more reliable and less likely to be malicious [29].

3.2.1 Trust evaluation:

The Smart Grid ensures that electricity is distributed and recorded safely to charge devices based on trust levels. In the trust computations, it is classified into two-way local and global trust[30] : Local trust or total trust score, vehicle per-vehicle trust score, calculated as a weighted fusion of three real-time metrics: security score,

feedback score, and behavior score, as shown in equation 1, and global trust is defined as the V2X network-wide average of local trust score, shown in equations 2 and 3, respectively.[31].

3.3 Trust computation:

In this model, the trust score is calculated with the help of total trust and global trust to detect and identify large-scale attacks in the V2X infrastructure[32]. The total and global trust are shown in equations 2 and 3.

$$\text{Trust_score} = \frac{\text{behavior_score} + \text{feedback_score} + \text{security_score}}{3} \quad (1)$$

$$\text{Global_trust} = \frac{\text{total_trust}}{\text{len}(\text{road_entities})} \quad (2)$$

$$\text{Total Trust} = \sum_{i=1}^n \text{Trust Value}_i \quad (3)$$

- **Definition:** Total trust is the aggregated trust score for electric vehicles, charging stations, and smart grids based on direct interactions.
- **Scope:** It is limited to direct interactions or transactions between entities such as electric vehicles, charging stations, and smart grid connections.
- **Data Sources:** Derive behavior score, feedback score, and security score from the dataset "Electric Vehicle Trip Energy Consumption Data".
- **Definition:** Global trust is defined as the overall trustworthiness of electric vehicles, charging stations, and smart grids perceived by the entire V2X network, including direct and indirect interactions.
- **Scope:** Both direct trust scores and indirect feedback from other entities, such as vehicle and charging station connection.
- **Calculation:** Trust computation based on the parameters used in the dataset, such as Trip energy consumption, speed, maximum and minimum cell temperature of the battery, and other parameters driving the simulation, including messages sent and received by the electric vehicles, authentication failures, and IDS alerts.

The system uses behavior, feedback, and security scores in the V2X infrastructure to determine local and global trust scores, as explained below[27].

3.3.1 Behavior Score:

The behavior score is the communication protocol, reliability, and consistency during the electric vehicles' interaction with each other.

- **Trip Energy Consumption(kWh):** Represents the electrical energy consumed by an electric vehicle (EV) during a single trip, from departure to arrival. It is a critical input feature in our V2X simulation taken from the "Electric Vehicle Trip Energy Consumption Dataset".

- **Speed:** In the electric vehicle's (EV) "Speed" (km/h), which is calculated using timestamps and longitude and latitude for a single trip. In our V2X simulation, it is a crucial behavioral and energy-related feature that has a direct impact on trust score, attack detection, and energy consumption.

$$\text{behavior_score} = \begin{cases} \min(1, \text{base} \times 1.1), & \text{benign} \\ \text{base} \times 0.85, & \text{attacker} \end{cases} \quad (4)$$

where:

$$e = 1 - \min(1, |E - 1|), \quad // E = \text{Trip Energy Consumption} \quad (5)$$

$$s = 1 - \min\left(1, \frac{|S - 200|}{400}\right), \quad // S = \text{Speed} \quad (6)$$

$$\text{base} = \frac{e + s}{2} \quad (7)$$

3.3.2 Feedback Score:

The feedback score based on the subjective trust merit assigned to each electric vehicle on historical interaction from neighboring vehicles and Road Side Units (RSUs). It reflects the perceived reliability of vehicles' messages, such as position, speed, and energy request, and is crucial for secure energy allocation and attack detection in V2X networks[33]

$$\text{feedback_score} = \begin{cases} \mathcal{U}(0.7, 1.0) & \text{if vehicle is benign} \\ \mathcal{U}(0.3, 0.6) & \text{if vehicle is under attack} \end{cases} \quad (8)$$

where $\mathcal{U}(a, b)$ denotes a uniform distribution.

3.3.3 Security Score:

Using the authentication failure rate, the IDS alert frequency and the battery temperature, calculate the dynamic security score, a combined trust metric that measures the communication integrity of vehicles. Throughout the simulation, it is updated in real time to reflect the changing security posture. Let:

- $M_t = \text{messages_sent}$
- $F_t = \text{auth_failures}$
- $A_t = \text{ids_alerts}$
- $\text{weights} = w_1, w_2$, and w_3 define as weights ($w_1 + w_2 + w_3 = 1$)
- $\text{Temp_threshold} = 20^\circ\text{C}$
- $\varepsilon = 10^{-6}$

$$\text{security_score}_t = w1 \left(1 - \frac{F_t}{M_t + \varepsilon} \right) + w2 \left(1 - \min \left(\frac{A_t}{10}, 1 \right) \right) + w3 \underbrace{\left(1 - \min \left(\frac{\Delta T}{20}, 1 \right) \right)}_{\text{Temp}} \quad (9)$$

$$\text{security_score}_t \leftarrow \text{clip}(\text{security_score}_t, 0, 1) \quad (10)$$

Before applying the deep learning model on the dataset, we add some extra features calculated based on the trust computation. The features of computing the following equations are shown below.

- **Security Score Difference:**

$$\Delta s_{i,t} = s_{i,t} - s_{i,t-1} \quad (11)$$

Captures rapid changes in trust, indicative of attacks.

- **Energy Consumption Rate:**

$$r_{e,i,t} = \frac{e_{i,t} - e_{i,t-1}}{\Delta t_i + \epsilon}, \quad \epsilon = 10^{-6} \quad (12)$$

Highlights abnormal energy usage patterns.

- **RFE:** Uses feature importance from Random Forest, based on Gini impurity reduction:

$$\text{Importance}_j = \sum_{\text{node } n \text{ splitting on feature } j} \Delta \text{Gini}_n \quad (13)$$

Iteratively removes the least important features until the desired number remains.

This MTLSTM model is designed to process the time series data of vehicle features to detect malicious behavior. In the time series function, the function takes the list of simulated vehicles and prepares the data for training and testing. Simulates vehicles for a specified number of steps, collects their feature vectors at each step, and creates sequences of these features. It also assigns a label (attack type) to each sequence based on the vehicle's simulated attack status. In trust evaluation, the CNN-LSTM model is used to assess the trustworthiness of each vehicle during the main simulation function. Processes sequences of features for each vehicle through the model to get predictions on whether the vehicle is malicious and what type of attack it might be performing. It also calculates local and global trust scores. The main simulation function. Initializes vehicles, RSU, charging station, and smart grid. Before starting the main simulation loop, it prepares the data and trains the CNN-LSTM model. The simulation then proceeds step by step, with the RSU processing vehicles, handling energy requests, and the charging station interacting with the smart grid. At each step, the trained CNN-LSTM model is used to evaluate the trustworthiness of the vehicles and detect malicious ones. The simulation collects data on various metrics, including SoC, battery lifespan, trust score, and attack detection status show in the Figure 4.

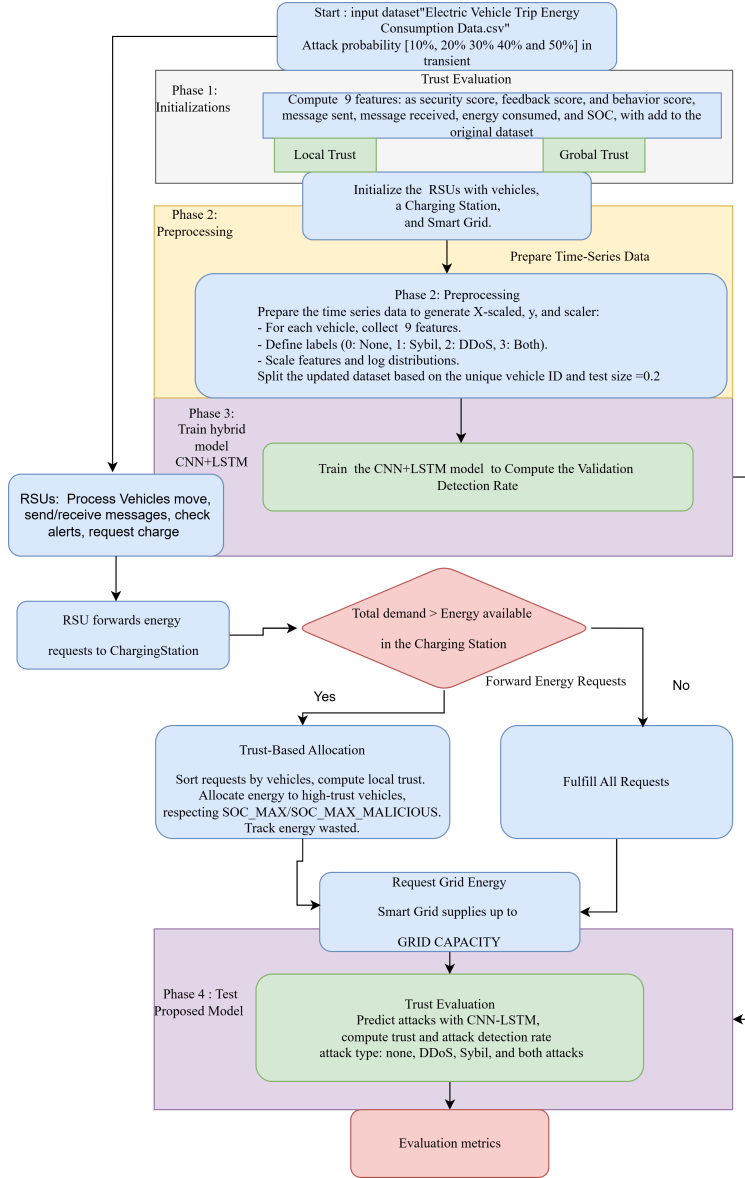


Fig. 4 Proposed MTCNN-LSTM model work flow for V2X.

The battery lifetime factor $L_i \in [0, 1]$ is calculated per time step as

$$L_i(t) = L_i(t-1) - \begin{cases} 0.005 \times \left(\frac{\text{SoC}_i(t) - \text{MAX_SOC}}{\text{MAX_SOC}} \right), & \text{if } \text{SoC}_i(t) > \text{MAX_SOC} \\ 0, & \text{otherwise} \end{cases} \quad (14)$$

Equation 14 use with MAX SOC = 0.9 to prevent battery[34]. This penalty is applied during energy allocation when overcharging occurs, directly linking it with malicious charging behavior during Sybil-induced full-charge requests, which can lead to physical battery degradation.

In the MTCNN-LSTM model, energy allocation, energy waste and battery optimization during attacks computing the following equation 15.

$$E_{\text{waste}} = \underbrace{\sum_{\substack{(v_i, r_i) \in \mathcal{R}_{\text{sorted}} \\ E_{\text{dist}} + r_i > E_{\text{avail}}}} r_i}_{\text{Capacity overflow}} + \underbrace{\sum_{\substack{v_i \in \mathcal{M} \\ \tau_i \leq 0.5}} r_i}_{\text{Malicious denied}} \quad (15)$$

Where the first term captures capacity overflow due to high legitimate demand (DDoS request flooding), and the second term represents energy denied to malicious vehicles(sybil) identified by a MTCNN-LSTM and low trust score value, unlike previous works that detect misbehavior in isolation without resource impact. In this model, it also performs real-time trust-based charging requests, applies battery lifespan penalties for overcharging, and dynamically requests grid support, ensuring secure, efficient, and battery-aware V2X charging in real-world electric vehicle environments. shown in Algorithm 1.

Algorithm 1 MTCNN-LSTM model based Trust for Secure V2X with Energy Allocation

- 1: **Input:** N vehicles, T steps, p_{attack} , real EV dataset
 - 2: **Output:** ADR, E_{waste} , L_i , T
 - 3: Initialize $L_i = 1.0$, $\tau_i = 1.0$, station energy = 2000 kWh
 - 4: Preprocess: 9 features $\rightarrow$ time-series $\rightarrow$ scale $\rightarrow$ split
 - 5: Train CNN-LSTM (128 $\rightarrow$ 100 $\rightarrow$ 50) $\rightarrow$ 94.73% accuracy
 - 6: **for** $t = 1$ to T **do**
 - 7: **for** each vehicle i **do**
 - 8: Simulate attack with p_{attack} , transition prob 0.3
 - 9: Update telemetry and request r_i
 - 10: Predict attack $\hat{y}_i \leftarrow \text{model}(X_i)$
 - 11: Compute $\tau_i = 0.4s_i + 0.3f_i + 0.3b_i$
 - 12: **end for**
 - 13: $T \leftarrow \frac{1}{N} \sum \tau_i$
 - 14: **Trust-Based Allocation:**
 - 15: **if** total demand > available **then**
 - 16: Sort by τ_i descending
 - 17: Allocate to $\tau_i > 0.5$, deny others $\rightarrow E_{\text{waste}} += r_i$
 - 18: Apply overcharge: $L_i \leftarrow L_i - 0.005 \times \frac{\text{SoC} - 0.9}{0.9}$
 - 19: **end if**
 - 20: Request grid if shortfall > 2000 kWh
 - 21: **end for**
 - 22: Compute ADR, F1, E_{waste} , T
-

4 Results and Discussion

4.1 Experimental setting

To assess the robustness of our approach, we used different evaluation metrics as presented in Section 4.2. To ensure an unbiased performance estimate, we adopted a split-test strategy to divide the data set. In this process, the dataset is divided into a 80:20 ratio, with 80% of the data used for training and the remaining 20% for testing. The number of instances in the training is 39920, while the number in the test is 9980. The generalizability of the model is further tested using multiple case studies. The proposed model operates in real time with inference on edge RSUs. The model processes a sequence length of 50 with nine features in <18 ms on a standard CPU (Intel i7-12700H), 16 GB RAM and 1TB SSD. The simulation takes the 1000-plus vehicles in an extensive network with 175.6 ms inference time (ms) for 100 vehicles requires 17.8 ms pr vehicle. This model required 68 MB of RAM during inference, including the input buffer.

4.2 Evaluation metrics

To evaluate the performance of the MTCNN-LSTM, we use various evaluation metrics.

4.2.1 Accuracy

Accuracy is used to classify the attack in V2X with sequences over the total number of test samples, computed directly from the predictions of the MTCNN-LSTM model using Equation 15.

$$\text{Accuracy} = \frac{1}{N} \sum_{i=1}^N \mathbb{I}(\hat{y}_i = y_i) \quad (16)$$

where N is the total number of test samples, $\hat{y}_i$ is the predicted attack class, y_i is the true label and $\mathbb{I}(\cdot)$ is the indicator function.

4.2.2 Precision

Precision measures the proportion of correctly predicted malicious instances out of all cases predicted as malicious for a given class k . It is defined in Equation 16.

$$\text{Precision}_k = \frac{\text{TP}_k}{\text{TP}_k + \text{FP}_k}, \quad \text{Recall}_k = \frac{\text{TP}_k}{\text{TP}_k + \text{FN}_k} \quad (17)$$

4.2.3 F1-score

The F1-score is used to normalize the mean precision and recall for a given class k , balancing false positives and false negatives. It is defined in Equation 17.

$$\text{F1-score}_k = 2 \cdot \frac{\text{Precision}_k \cdot \text{Recall}_k}{\text{Precision}_k + \text{Recall}_k}, \quad \text{F1}_{\text{weighted}} = \sum_{k=0}^3 w_k \cdot \text{F1}_k \quad (18)$$

4.2.4 Attack Detection Rate

Attack detection rate (ADR) is the percentage of actual malicious V2X sequences that are correctly identified by the MTCNN-LSTM model, regardless of the specific attack type (Sybil, DDoS, or Both). It is equivalent to the recall over non-benign classes shown in Equation 18.

$$\text{Attack Detection Rate} = \frac{\text{TP}_{\text{attack}}}{\text{TP}_{\text{attack}} + \text{FN}_{\text{attack}}} \times 100\% = \text{Recall}_{\text{non-benign}} \times 100\% \quad (19)$$

4.3 Performance evaluation

4.3.1 Case I: Taking the dynamic attacks on V2X

In the initial phase 1 of the simulation, 100 vehicle data is collected from the dataset "Electric Vehicle Trip Energy Consumption Data" including metrics such as Trip Energy Consumption, Vehicle ID Trip Distance, Time of Day, Day of Week, Longitude, Latitude, Speed, Current, Total voltage, Maximum cell Temperature of Battery, minimum cell temperature of Battery, and Trip Time Length show in Figure 5.

	Trip Energy Consumption	Vehicle ID	Trip Distance	Time of Day	Day of the Week	Longitude	Latitude	Speed	Current	Total Voltage	Maximum Cell Temperature of Battery	Minimum Cell Temperature of Battery	Trip Time Length
0	0.672	1	6.0	275	4	121.497948	31.281574	152.136056	2.583348	308.283333	31.000000	30.833333	13
1	0.896	1	6.0	2252	4	121.587564	31.256070	152.136056	2.985729	304.485714	29.000000	28.000000	18
2	1.344	1	7.0	2281	2	121.576968	31.262034	152.136056	2.354560	308.463636	31.272727	30.000000	21
3	1.344	1	8.0	3356	5	121.549709	31.257796	152.136056	1.540015	308.060000	30.000000	30.000000	16
4	0.896	1	6.0	1536	6	121.582280	31.215030	152.136056	9.028040	304.473457	28.000000	28.000000	129

Fig. 5 Electric Vehicle Trip Energy Consumption Data use in MTCNN-LSTM model.

In the phase 2 of the simulation, data preprocessing and feature engineering are conducted to prepare the dataset by cleaning numeric columns through median imputation for missing values and capping outliers using the IQR method, encoding categorical columns, and creating time-series sequences with the prepare time series data function, which extracts 'security score', 'feedback score', 'behavior score', 'message freq', 'messages received', 'energy consumed', 'soc', 'security score diff', 'energy consumed rate' over a maximum of 10 steps, while assigning labels (y) based on attack types (None, Sybil, DDoS, Both) Shown in the Table 1, and for balancing using the class weight technique to address class imbalances between benign and malicious vehicles, and data scaling is applied to ensure compatibility with a deep learning approach. This phase ensures that the data are clean and properly used for model training. In Phase 3, the script trains a CNN-LSTM model to classify vehicles by selecting all nine features, identifying whether they are benign or under attack (Sybil, DDoS, or both). This phase is critical to ensure that the system can detect malicious vehicles and prioritize energy sharing for trustworthy ones. Building the MTCNN-LSTM hybrid model, taking the hyperparameter values shown in Table 2.

In this simulation if there are no malicious nodes (0%) the international trust is stable and high, around 0.54. In addition to increasing malicious nodes such as 10%, 20%,

Table 1 Features mapping with attacks impact

Attack label	High features impact	Low features impact
Sybil	energy rate ,speed	SoC
DDoS	message rate, auth fail,ids alert rate	-
Both	all above	all above
None	normal value	normal value

Table 2 MTCNN-LSTM design and hyper parameter tuning

Hyper parameter	Values
No of CNN Layers	2
filters size	128,64
kernel size	3,3
activation	relu
output activation	softmax
No of neurons in LSTM layer 1,2,3	100,100,50
Dropout	0.4
optimizer	Adam
learning rate	0.0008
Batch size	128
No of Epoch	20

30%, 40% and 50% with transient malicious node, the global trust value drops incrementally with the increase in malicious node percentages. Because malicious nodes negatively affect the network performance to maintain trust between them afterward, if 50% of malicious nodes in V2X, the trust value is the lowest (around 0.68), indicating a significant deterioration in global trust when half of the network is composed of malicious nodes. In V2X stability across all percentages, trust values remain relatively stable within each scenario, suggesting that the network quickly adapts to malicious nodes without dramatic fluctuations, if further increase the more than 50% global trust high around 0.54 shown in Table 3, Global trust computed based on the behavior score, feedback score and security score In global trust, it is computed based on the

Table 3 Malicious percentage and global trust values

Transit malicious percentage	Global Trust
10%	0.88
20%	0.82
30%	0.79
40%	0.75
50%	0.68

behavior score calculated using Equations 4, 5, and 6, which depend on trip energy consumption and speed. The feedback score was calculated using Equation 8, and the security score depended on authentication failures, IDs, and the maximum and minimum battery temperatures to compute Equations 9 and 10. Our MTCNN-LSTM with feature selection is done explicitly by defining a list of relevant features rather than through an automated selection process. Updated datasets with nine features: 'behavior score', 'feedback score', and 'security score', with six additional features such as 'message frequency', 'received messages', 'energy consumed', 'soc', 'security score diff' and 'energy consumed rate'. The updated data set now contains 49,900 records 4.1. The class distribution is shown in Table 4. The result of MTCNN-LSTM, with the aid of a

Table 4 Class distributions for training and testing data

Class distribution	None	Sybil	DDoS	Both
Before balancing	28618	4885	10134	6263
Training	22873	3941	8049	5057
Testing	5745	944	2085	1206
Class weight	0.436	2.533	1.239	1.973

confusion matrix, displayed in Figure 6, was determined while assessing the MTCNN-LSTM model’s performance in recognizing None, Sybil, DDOS, and Both attacks. This confusion matrix provides an overview of the model’s classification accuracy, displaying both the actual and predicted results. The diagonal values in the matrix represent correctly classified instances for each class, highlighting the model’s accuracy.

- **None:**The model classifies 5501 none instances correctly, with minimal misclassification of 62 instances as sybil, 105 instances as DDoS, and 77 instances as both attacks.
- **Sybil:**We observe that the model accurately identifies 831 instances of Sybil attack with only minor misclassifications of 9 instances as none, 20 instances of DDoS, and 84 instances as both attacks.
- **DDoS:**The model now identifies 1971 DDoS instances correctly, with minimal misclassification: 8 instances are classified as none, 62 instances as Sybil, and 44 instances as both attack.
- **Both:**For both attacks, the model correctly predicts 1152 instances while misclassifying 10 as none, 31 instances as sybil, and 13 instances as a DDoS attack.

It is helpful to highlight the strengths and weaknesses of the model in more detail.

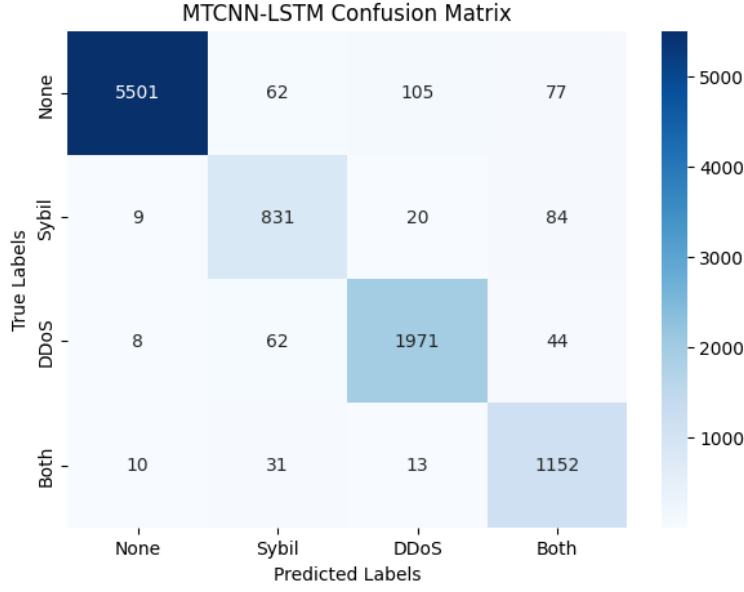


Fig. 6 Confusion matrix of MTCNN-LSTM model

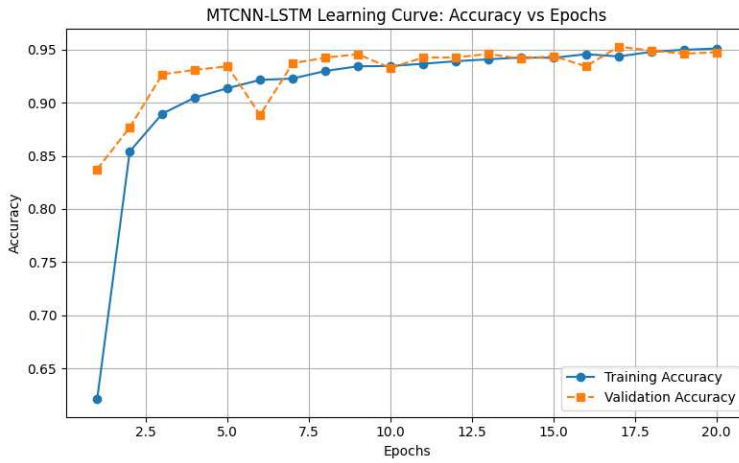


Fig. 7 Learning Curve of MTCNN-LSTM model

Figure 7 illustrates the training and validation accuracy of the MTCNN-LSTM model for the number of epochs applied. The plot above shows both curves, showing that the learning process is progressive throughout the training. The training and validation curves align closely, suggesting that they did not overfit and generalize effectively. In the last epoch, the training and validation accuracy stands at nearly 95%,

thus the model effectively identifies sybil and DDoS attacks. These results validate the model's functioning in intrusion detection for the V2X network.

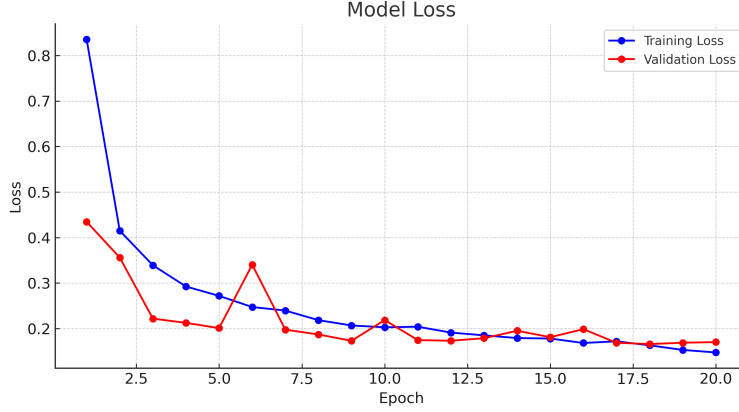


Fig. 8 Learning Curve of MTCNN-LSTM model

Figure 8 illustrates the training and validation losses of the MTCNN-LSTM model for the specified number of epochs. The plot above shows both curves, indicating that losses decline and stabilize, with no indication of overfitting or data leakage.

In Table 5, presents the results of various deep-learning models that identify none,

Table 5 Performance metrics for MTCNN-LSTM and different classifiers

Classifier	Class	Precision	Recall	F1 Score
GRU	None	0.99	0.95	0.97
	Sybil	0.84	0.92	0.88
	DDoS	0.93	0.99	0.96
	Both	0.89	0.92	0.91
LSTM	None	0.99	0.94	0.97
	Sybil	0.85	0.91	0.88
	DDoS	0.93	0.98	0.95
	Both	0.87	0.92	0.89
MTCNN-LSTM	None	1.00	0.960	0.98
	Sybil	0.84	0.88	0.86
	DDoS	0.93	0.95	0.94
	Both	0.85	0.96	0.90

Sybil, and DDoS attacks in V2X. It focuses on the recall precision and F1 score, attack detection rate, and false positive rate for every classifier. The summary of the performance metrics of GRU, LSTM, and the proposed MTCNN-LSTM has revealed model efficiency in identifying sybil and DDoS attacks in V2X. The proposed MTCNN-LSTM model and its application in selecting nine features computed through trust

Table 6 performance comparsion with GRU and LSTM model

Classifier	Accuracy	Attack Detection Rate	False Postive Rate
GRU	94.96%	98.72%	5.36%
LSTM	94.58%	97.68%	6.35%
Proposed MTCNN-LSTM	94.73%	99.36%	4.24%

metrics aim to enhance the classification power of these models. In Table 6, the GRU demonstrates the best overall classification performance. It has a strong ability to identify and classify attacks accurately. However, the MTCNN-LSTM model achieves the best results in security-specific metrics, showing a higher attack detection rate and a lower false positive rate, making it more effective in accurately detecting attacks with fewer false alarms, so that our MTCNN-LSTM model is more robust and reliable for applications where accurate attack detection and minimizing false positives are critical.

4.3.2 Case II: Energy allocation for battery optimization based on MTCNN-LSTM model

In this case, II ensures efficient energy allocation through trust-based decisions, extending battery lifespan while reducing energy wastage in smart grid interactions. The simulated energy allocation function models a Vehicle-to-Everything (V2X) environment to simulate secure and energy-aware operations among vehicles, charging stations, and a smart grid. It begins by loading or generating the dataset, and it across 100 virtual vehicles, and initializing system components like Road Side Units (RSUs), charging stations, and a smart grid with fixed capacity. Prepare time series data shown in Algorithm 1, balance them using the Class weighted technique, and split them into training and testing sets. The system trains a MTCNN-LSTM model to detect malicious behaviors based on selected and scaled features. The simulation then runs for a defined number of steps during which the vehicles interact with the RSU, request energy, and receive grid support if needed. Trust evaluations use the trained model and record key metrics, such as SoC (State of Charge), trust scores, and attack types. Finally, the system compiles the data into a DataFrame, saves it to a CSV file, computes performance metrics such as attack detection rate, false positive rate, and average battery lifespan, and generates visualizations to analyze system behavior. Figure 9, shows the "Security Score Evolution", which displays the security scores of 100 vehicles over 10 simulation steps; the x-axis shows the number of steps and the y-axis shows the security score range from (0.3-1.0) in the MTLSTM model , attack detection simulation. Each line represents a vehicle, with its color corresponding to the legend on the right, which labels vehicles as "Vehicle 1" to "Vehicle 100" and indicates their attack type (none, Sybil, DDoS, or Both) generally maintains higher, more stable scores (0.7-1.0) throughout, reflecting fewer authentication failures and IDS alerts. In contrast, vehicles under attack (Sybil, DDoS, or both) exhibit lower and more volatile scores (0.3-0.6), with noticeable dips around steps 2, 4, and 6, likely due to spikes in message frequency or IDS triggers. Initially, security score between 0.4

and 1.0, attacked vehicle scores trend downward over time, clustering at the lower end by Step 10, while benign vehicles remain consistently higher, highlighting the impact of attack-related behaviors on security metrics in the V2X system.

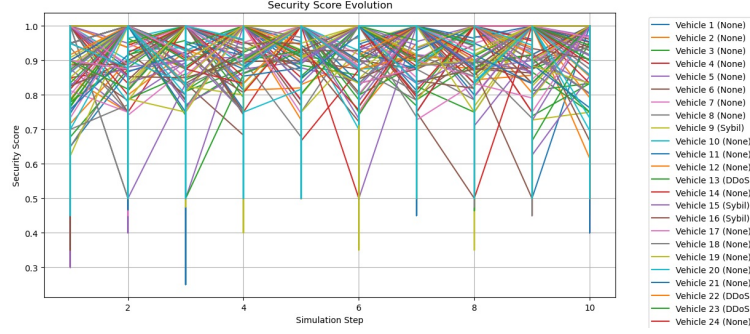


Fig. 9 Security Score Evolution.

Figure 10, showing the "Battery Lifespan Factor Evolution" plot, illustrates the battery lifespan factor of 100 vehicles over 10 simulation steps in a proposed CNN-LSTM Trust system, with each line representing a vehicle labeled by ID and attack type (no, Sybil, DDoS or Both). Starting at 1.0, the battery lifespan factor decreases over time for many vehicles, particularly those under attack, due to a low state of charge (SoC < 0.2) during movement, reduces the factor by 0.01, and overcharging (SoC > 0.9) during energy requests at the charging station deducts 0.005. By step 10, most vehicles' lifespan factors drop to around 0.4-0.6, with attacked vehicles (Sybil, DDoS, or Both) often showing steeper declines due to more frequent energy demands and malicious behavior. In contrast, benign vehicles ("None") exhibit slightly less degradation, reflecting the cumulative impact of energy management and attack-related stressors on battery health.

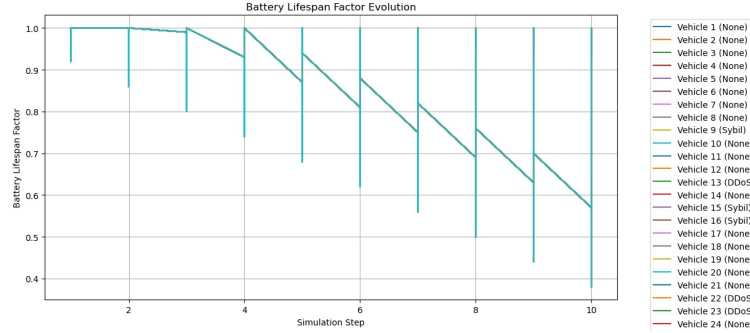


Fig. 10 Battery Lifespan Factor Evolution

The figure 11 "Total energy wasted and supplied vs. attack probability" plot shows how energy wasted and supplied vary with attack probability in the x-axis range (0.10 to 0.50) in the MTCNN-LSTM model, energy wasted increases linearly from about 250 kWh at 0.10 to 550 kWh at 0.50, reflecting the charging station higher

attack probabilities result in more malicious vehicles, increasing energy demands via request charge, and when demand exceeds the initial 500 kWh (energy available), excess requests are wasted. Conversely, energy supplied fluctuates between 1500 and 2000 kWh, peaking at 0.25 and 0.35, as the Smart Grid supplies energy to cover shortfalls, capped by grid capacity = 2000.0 per request, with variations likely due to the number of vehicles requesting charge and their trust-based prioritization receive requests sort by local trust, showing that supply dynamics are less predictable than waste in this simulation.

When the probability of attack is low (0.10-0.15), only a few malicious electric vehicles are active, resulting in minimal denial and low energy waste (250 kWh) while the grid continues to supply around 2000 kWh efficiently. As the attack rate increases to 0.15–0.25, a linear increase in wasted energy (300–500 kWh) is observed due to the emergence of more Sybil and DDoS attacks, causing partial denial for low-trust vehicles and reducing the effective supply to 1700 kWh. At an attack probability of (0.30-0.35) experiences maximum degradation, with nearly 30% of EVs compromised, leading to 550 kWh of energy waste and substantial denial and overflow in the allocation of the network. However, when the intensity of the attack reaches 0.35 to 0.50, the waste begins to saturate (600 to 650 kWh) as MTCNN-LSTM dynamically learns from historical misbehavior, blocks low-trust EVs, and restores energy balance by maintaining the supplied energy between 1500 and 1800 kWh. This behavior justifies that the model effectively self-regulates under heavy attack loads, minimizing long-term grid instability and supporting resilient, energy-efficient V2G operation.

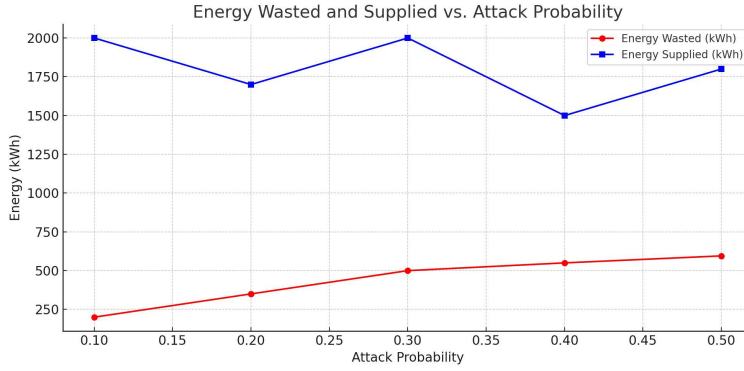


Fig. 11 Total energy wasted and supplied vs. attack probability

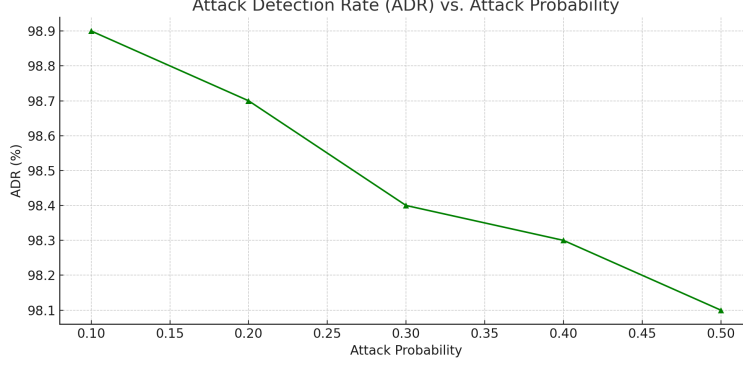


Fig. 12 Attack Detection Rate (ADR) vs. Attack Probability

In Figure 12, showing the plot of the "Attack Detection Rate (ADR) vs. Attack Probability" illustrates the relationship between attack probability in the x-axis range from 0.10 to 0.50 and the attack detection rate in the y-axis in the proposed model. The ADR decreases from 98.9% at an attack probability of 0.10 to 98.1% at 0.50, showing a slight downward trend. ADR estimates the ratio of true positives, vehicles the system correctly identifies as malicious, to the total number of attacks, increasing as the attack probability rises. The MTCNN-LSTM model detects attacks (Sybil, DDoS, or Both) based on features such as security score and message freq. However, as the probability of an attack increases, the performance of the model slightly degrades, possibly due to increased noise or overlapping behaviors between benign and malicious vehicles. If the MTCNN-LSTM work under extreme attack loads, maintaining >98% attack detection rate (ADR) when 80% of vehicles are malicious, As the malicious vehicles ratio increases from 10% to 80%, energy waste rises from 250 kWh to a saturation point of 910 kWh, reflecting denial of low-trust requests. MTCNN-LSTM-driven trust is shown in Figure 10. In the global trust declines linearly from 0.88 to 0.54, accurately reflecting the degradation of network health.

4.4 Performance comparison of our proposed model MTCNN-LSTM with state-of-the-art method

In Table 7, MTCNN-LSTM model compares with existing techniques in terms of context, trust model, attack detection rate, average battery lifespan factor, and average battery lifetime during attacks. Our MTCNN-LSTM Trust model gives an highest attack detection rate of 99.36%, an average battery life factor of 98.23% and an average battery life during attacks of 97.56%.

Table 7 Comparison of existing studies With our proposed MTCNN-LSTM model study.

line	Approach	Context	Trust Model	ADR	ABLF,ABLF/DA
	El-Sayed et.al.[35]	VANETs	Machine Learning	85%	No,No
	Atwah, R.et.al.[36]	VANETs	Smart Trust	87%	No,No
	Zhang, H et.al. [37]	V2V	Blockchain Trust	92%	No,No
	Ayobi, S et.al. [38]	VANETs	blockchain	90%	No,No
	Wang, Y et.al. [30]	V2V	Fog computing	95%	No,No
	Proposed MTCNN-LSTMModel	V2X	Multi level Trust Deep learning	99.36%	98.23&,97.56%

5 Conclusion

In this paper introduces a closed-loop V2X security and energy management A framework that fundamentally bridges the long-standing gap between intrusion detection and resource allocation in Intelligent Transportation Systems by leveraging real-world EV trip energy consumption data,the proposed MTCNN-LSTM model classifier achieves 94.7% accuracy, 94.83% weighted F1-score, and 99.36% attack detection rate (ADR) across four attack classes (None, Sybil, DDoS, Both) outperforming. Our Case II is based on a trust-energy feedback loop, where local and global trust are maintained under a 30% attack probability, dynamically prioritizing legitimate vehicles. This results in 500 kWh of energy waste at peak attack. load quantified as equation 14 ,with systematic denial of malicious requests and adaptive grid fallback ensuring supply recovery beyond 35% attack probability.

Future work includes edge deployment on 5G-V2X RSUs, extending the framework to address more diverse attack scenarios, integrating lightweight architectures for deployment on resource-constrained vehicular devices, and incorporating federated learning, blockchain-enhanced immutable trust logs, real-world field trials in urban mobility networks, and scalability analysis with thousands of vehicles. This framework paves the way for secure, sustainable, and intelligent energy ecosystems in next-generation smart cities.

6 Abbreviations

The following abbreviations are used in this manuscript:

ADR	Attacks Detection Rate
ABLF	Average battery lifespan factor
ABLDA	Average battery lifespan during attacks
V2X	Vehicle-to-everything
DDoS	Distributed Denial-of-Service
SoC	State of Charge

7 Authorship Contributions

Sanjay Kumar Sonker contributed to Conceptualization, Methodology Design, Data Curation, Investigation, and Writing-Original Draft. Vibha Kaw Raina contributed to Conceptualization, Methodology, Supervision, Review and Editing, Validation, and

Resources. Bharat Bhushan Sagar contributed to Formal Analysis and Methodology. Md Khalid Jamal contributed to Formal Analysis, Visualization, and Investigation. All authors have read, revised, and approved the final manuscript for publication.

8 Declarations

- **Data Availability:** The Electric Vehicle Trip Energy Consumption Data dataset used in this study is publicly available through ETS-Data Sharing to Advance Mobility. The dataset comprises real-world electric vehicle trip records, providing information relevant to the analysis of EV energy consumption. The dataset was published by Yang Liu in 2023 and is openly accessible through the ETS-Data repository. Dataset: Yang Liu, Electric Vehicle Trip Energy Consumption Data, ETS-Data, 2023.DOI: 10.26599/ETSD.2023.9190020.
- **Funding :** The authors gratefully acknowledge Sharda University, Greater Noida, India, for providing financial support for this research.
- **Ethics approval:** Not applicable.
- **Consent to participate:** Not applicable.
- **Consent to publish:** Not applicable.
- **Competing interests:** The authors declare no competing interests

If any of the sections are not relevant to your manuscript, please include the heading and write ‘Not applicable’ for that section.

Editorial Policies for:

Springer journals and proceedings: <https://www.springer.com/gp/editorial-policies>

Nature Portfolio journals: <https://www.nature.com/nature-research/editorial-policies>

Scientific Reports: <https://www.nature.com/srep/journal-policies/editorial-policies>

BMC journals: <https://www.biomedcentral.com/getpublished/editorial-policies>

References

- [1] Pavithra, T., Nagabhushana, B.: Intrusion detection using sa-bilstm and enhanced deep rl routing with modular homomorphic encryption for secure data transmission in vanet. *Optical Memory and Neural Networks* **34**(2), 188–205 (2025)
- [2] Hbaieb, A., Ayed, S., Chaari, L.: A survey of trust management in the internet of vehicles. *Computer Networks* **203**, 108558 (2022)
- [3] Fadhil, J.A., Sarhan, Q.I.: Internet of vehicles (ioV): A survey of challenges and solutions. In: 2020 21st International Arab Conference on Information Technology (ACIT), pp. 1–10 (2020). IEEE

- [4] Yanmin, C., Sarkar, A., Zain, J.M., Bhar, A., Noorwali, A., Othman, K.M.: Leveraging lstm and gru-based deep neural coordination in intelligent transportation to strengthen security in the internet of vehicles. *International Journal of Machine Learning and Cybernetics* **16**(4), 2431–2467 (2025)
- [5] Sonker, S.K., Raina, V.K., Sagar, B.B., Bansal, R.C.: Fog computing-based iot-enabled system security for electrical vehicles in the smart grid. *Electrical Engineering* **106**(2), 1339–1355 (2024)
- [6] Gupta, C., Singh, L., Tiwari, R.: Malicious node detection in vehicular ad-hoc network (vanet) using enhanced beacon trust management with clustering protocol (ebtm-cp). *Wireless Personal Communications* **130**(1), 321–346 (2023)
- [7] Tulay, H.B., Koksall, C.E.: Sybil attack detection based on signal clustering in vehicular networks. *IEEE Transactions on Machine Learning in Communications and Networking* **2**, 753–765 (2024)
- [8] ETSI, T.: Intelligent transport systems (its); security; trust and privacy management. *Intelligent Transport Systems (ITS)* (2018)
- [9] Hussain, R., Lee, J., Zeadally, S.: Trust in vanet: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems* **22**(5), 2553–2571 (2020)
- [10] Malhi, A.K., Batra, S., Pannu, H.S.: Security of vehicular ad-hoc networks: A comprehensive survey. *Computers & Security* **89**, 101664 (2020)
- [11] Alnasser, A., Sun, H.: Global roaming trust-based model for v2x communications. In: *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–6 (2019). IEEE
- [12] Nayak, R.P., Sethi, S., Bhoi, S.K., Sahoo, K.S., Tabbakh, T.A., Almusaylim, Z.A., et al.: Tbddosa-md: Trust-based ddos misbehave detection approach in software-defined vehicular network (sdvn). *Computers, Materials & Continua* **69**(3) (2021)
- [13] Zhang, Y.-Y., Shang, J., Chen, X., Liang, K.: A self-learning detection method of sybil attack based on lstm for electric vehicles. *Energies* **13**(6), 1382 (2020)
- [14] Xu, Q., Zhang, L., Qin, X., Zhou, Y.: A novel machine learning-based trust management against multiple misbehaviors for connected and automated vehicles. *IEEE Transactions on Intelligent Transportation Systems* (2024)
- [15] Ullah, F., Salam, A., Amin, F., Khan, I.A., Ahmed, J., Zaib, S.A., Choi, G.S.: Deep trust: A novel framework for dynamic trust and reputation management in the internet of things (iot) based networks. *IEEE Access* (2024)
- [16] Moghadasi, N., Collier, Z.A., Koch, A., Slutzky, D.L., Polmateer, T.L., Manasco,

- M.C., Lambert, J.H.: Trust and security of electric vehicle-to-grid systems and hardware supply chains. *Reliability Engineering & System Safety* **225**, 108565 (2022)
- [17] Muhammad, G., Alhussein, M.: Security, trust, and privacy for the internet of vehicles: A deep learning approach. *IEEE Consumer Electronics Magazine* **11**(6), 49–55 (2021)
 - [18] Kwon, S.K., Seo, J.H., Yun, J.Y., Kim, K.-D.: Driving behavior classification and sharing system using cnn-lstm approaches and v2x communication. *Applied Sciences* **11**(21), 10420 (2021)
 - [19] Yanmin, C., Sarkar, A., Zain, J.M., Bhar, A., Noorwali, A., Othman, K.M.: Leveraging lstm and gru-based deep neural coordination in intelligent transportation to strengthen security in the internet of vehicles. *International Journal of Machine Learning and Cybernetics*, 1–37 (2024)
 - [20] Alladi, T., Kohli, V., Chamola, V., Yu, F.R.: A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. *Digital Communications and Networks* **9**(5), 1113–1122 (2023)
 - [21] Azam, S., Bibi, M., Riaz, R., Rizvi, S.S., Kwon, S.J.: Collaborative learning based sybil attack detection in vehicular ad-hoc networks (vanets). *Sensors* **22**(18), 6934 (2022)
 - [22] Xu, Y., Zheng, L., Wu, X., Tang, Y., Liu, W., Sun, D.: Energy-efficient resource allocation for v2x communications. *IEEE Internet of Things Journal* **11**(18), 30014–30026 (2024)
 - [23] Gong, J., Wasyłowski, D., Figgenger, J., Bihn, S., Rücker, F., Ringbeck, F., Sauer, D.U.: Quantifying the impact of v2x operation on electric vehicle battery degradation: An experimental evaluation. *Etransportation* **20**, 100316 (2024)
 - [24] Zhu, Q., Huang, Y., Lee, C.F., Liu, P., Zhang, J., Wik, T.: Predicting electric vehicle energy consumption from field data using machine learning. *IEEE Transactions on Transportation Electrification* (2024)
 - [25] Abir, S.A.A., Anwar, A., Choi, J., Kayes, A.: Iot-enabled smart energy grid: Applications and challenges. *IEEE access* **9**, 50961–50981 (2021)
 - [26] Taslimasa, H., Dadkhah, S., Neto, E.C.P., Xiong, P., Ray, S., Ghorbani, A.A.: Security issues in internet of vehicles (ioV): A comprehensive survey. *Internet of Things* **22**, 100809 (2023)
 - [27] Siddiqui, S.A., Mahmood, A., Sheng, Q.Z., Suzuki, H., Ni, W.: A survey of trust management in the internet of vehicles. *Electronics* **10**(18), 2223 (2021)

- [28] Awais, S.M., Yucheng, W., Mahmood, K., Badar, H.M.S., Kharel, R., Das, A.K.: Provably secure fog-based authentication protocol for vanets. *Computer Networks* **246**, 110391 (2024)
- [29] Ranjith Kumar, K., Vallimurugan, E.: A hybrid technique for optimal placement of fast-charging stations of electric vehicles for the reliability of distribution network. *Energy Technology* **12**(4), 2300874 (2024)
- [30] Wang, Y., Sun, X., Zheng, G., Rashid, A., Ullah, S., Alasmay, H., Waqas, M.: Enhancing energy efficiency with a dynamic trust measurement scheme in power distribution network. *Computers, Materials and Continua* (2024)
- [31] Wolsink, M.: Conceptualizations of smart grids—anomalous and contradictory expert paradigms in transitions of the electricity system. *Energy Research & Social Science* **109**, 103392 (2024)
- [32] Mwanje, M.D., Kaiwartya, O., Jha, D.N., Khasawneh, A.M., Sadiq, A., Cao, Y.: Misbehaviour prediction in cav network using aggregated trust analysis: M. drolence mwanje et al. *International Journal of Intelligent Transportation Systems Research*, 1–17 (2025)
- [33] Balasubramaniam, S., Syed, M.H., More, N.S., Polepally, V.: Deep learning-based power prediction aware charge scheduling approach in cloud based electric vehicular network. *Engineering Applications of Artificial Intelligence* **121**, 105869 (2023)
- [34] Severson, K.A., Attia, P.M., Jin, N., Perkins, N., Jiang, B., Yang, Z., Chen, M.H., Aykol, M., Herring, P.K., Fraggadakis, D., *et al.*: Data-driven prediction of battery cycle life before capacity degradation. *Nature Energy* **4**(5), 383–391 (2019)
- [35] El-Sayed, H., Ignatious, H.A., Kulkarni, P., Bouktif, S.: Machine learning based trust management framework for vehicular networks. *Vehicular Communications* **25**, 100256 (2020)
- [36] Atwah, R.J., Flocchini, P., Nayak, A.: Towards smart trust management of vanets. In: 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1–5 (2020). IEEE
- [37] Zhang, H., Liu, J., Zhao, H., Wang, P., Kato, N.: Blockchain-based trust management for internet of vehicles. *IEEE Transactions on Emerging Topics in Computing* **9**(3), 1397–1409 (2020)
- [38] Ayobi, S., Wang, Y., Rabbani, M., Dorri, A., Jelodar, H., Huang, H., Yarmohammadi, S.: A lightweight blockchain-based trust model for smart vehicles in vanets. In: Security, Privacy, and Anonymity in Computation, Communication, and Storage: 13th International Conference, SpaCCS 2020, Nanjing, China, December 18–20, 2020, Proceedings 13, pp. 276–289 (2021). Springer