Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

A hybrid deep learning-based intrusion detection system for EV and UAV charging stations

Rosebell Paul & Mercy Paul Selvan

To cite this article: Rosebell Paul & Mercy Paul Selvan (2024) A hybrid deep learning-based intrusion detection system for EV and UAV charging stations, Automatika, 65:4, 1558-1578, DOI: 10.1080/00051144.2024.2405787

To link to this article: https://doi.org/10.1080/00051144.2024.2405787

Published online: 23 Sep 2024.

AUTOMATIKA
2024, VOL. 65, NO. 4, 1558–1578
https://doi.org/10.1080/00051144.2024.2405787

OPEN ACCESS Check for updates

A hybrid deep learning-based intrusion detection system for EV and UAV charging stations

Rosebell Paul and Mercy Paul Selvan

Department of Computer Science and Engineering, School of Computing, Sathyabhama Institute of Science and Technology, Chennai, India

ABSTRACT

This paper proposes a novel approach that leverages a hybrid deep learning framework called the Squirrel Search-optimized Attention-Deep Recurrent Neural Network (SS-ADRNN) to optimize the management of charging stations, ensuring efficient resource allocation while safeguarding user data and minimizing operational costs. The SS-ADRNN model incorporates squirrel search optimization, which is inspired by the foraging behaviour of squirrels, to dynamically adjust charging station operations based on environmental conditions and demand patterns. Additionally, attention mechanisms are employed to prioritize relevant input features, enabling the model to focus on critical information during decision-making processes. Deep recurrent neural networks (RNNs) are utilized to capture temporal dependencies in charging station data, allowing for more accurate predictions and adaptive control strategies. Experimental evaluations demonstrate the effectiveness and feasibility of the proposed SS-ADRNN-based approach in real-world scenarios. The results showcase significant improvements in the detection of malicious traffic and cost minimization compared to traditional charging station management methods. Overall, this research contributes to advancing the field of intelligent charging station optimization, offering a robust and adaptable solution for EV and UAV charging infrastructures that prioritize both security and operational efficiency.

ARTICLE HISTORY
Received 27 May 2024
Accepted 6 September 2024

KEYWORDS
Squirrel Search Algorithm; attention network; deep recurrent neural network; electric vehicle; unmanned aerial vehicle

1. Introduction

The world is facing a fuel crisis, and the global community is looking for an alternate option to utilize renewable energy sources to meet the energy demands. The rise of Electric Vehicles (EVs) presents a transformative shift towards cleaner and more sustainable transportation solutions [1,2]. However, as the demand for EV escalates [3], it is essential that secure and cost-effective EV charging infrastructures are developed. The pandemic lockdown led to the rapid proliferation of Unmanned Aerial Vehicles (UAVs) which is yet another intelligent sustainable transportation solution for all industrial sectors [4]. UAV technology has been used for diverse applications in multiple domains such as military, medical services, surveillance and agriculture. These two technologies make transportation more productive, eco-friendly and reliable. This transition led to the pressing need for robust and secure electric charging infrastructure capable of accommodating the burgeoning demand. The two critical challenges that hinder the faster EV and UAV market growth in its nascent stage are security and charging cost optimization.

Generally, EVs and UAV charging station comprises of four essential elements: sensing, communication, net working and computational [5]. The first component consists of a sequence of wired or wireless sensors to determine the safety and health of different electrical parts in the EV and UAV charging stations [6]. The second component interconnects with the local grid system, Supervisory Control And Data Acquisition (SCADA) module, EVs, UAVs and other internal sensors using the internet connection to confirm the availability and energy efficiency [7]. The internet connection can be any wireless technology like Wi-Fi, Bluetooth, mobile networks, etc. Finally, the computational element performs arithmetic, logic and control operations. EV and UAV holders must schedule the charging through the Internet, integrating the maximum number of EV and UAV users into the grids [8]. Before the charging process, the EV and UAV charging stations typically request user authorization, enabling financial and personal data to be shared through platforms like Bluetooth, Radio Frequency Identification (RFID), etc. However, transmitting information through wireless technology imposes vulnerabilities in EV and UAV charging systems [9,10]. These vulnerabilities in charging infrastructure impose significant challenges in terms of security and data privacy. Hence, a robust and effective threat detection and privacy preservation model is necessary to ensure the security and integrity of EV and UAV charging stations

CONTACT Rosebell Paul rosebellabin@gmail.com

[11]. The security of the EV and UAV charging infrastructure can be enhanced by introducing Intrusion Detection Systems (IDS).

While IDS safeguards the EV users and energy providers, efficient resource allocation for this energy trading is ensured with the optimum cost of charging. The proposed intelligent IDS leverages cutting-edge technologies that provide way to bridge this divide to achieve efficient and sustainable charging station operations.

Numerous studies have been developed for security and privacy preservation of EV and UAV charging stations using IDSs. These studies used techniques such as Support Vector Machine (SVM) [46] Random Forest (RF) [13], Deep Neural Network (DNN) [14] and so on. These techniques leverage their learning efficiency to distinguish between normal and malicious data. Typically, these models are trained in either supervised or unsupervised ways and accurately detect cyber threats and other vulnerabilities. Despite their advantages, these methods face significant challenges. One of the most common challenges is the lack of generalization. Generally, deep learning and machine learning techniques are overtrained on the training samples, inducing overfitting. This problem causes the system not to generalize well on unseen or real-world scenarios. In addition, these models face issues like limited scalability, high computational time, lower adaptability, etc. One of the other main challenges is to guarantee optimized charging operations that meet fluctuating demand with minimum operational costs and ensure data privacy and security for EV users. The proposed system aims to balance these objectives by integrating hybrid deep learning with optimization algorithms. The hybrid deep learning approach employed in the proposed algorithm ensures the security of the user data by detecting malicious data from the network. Consequently, a squirrel search algorithm was deployed to optimize the functioning of the charging station considering the demand, available energy and real-time environmental conditions, thereby reducing the energy cost and waiting time for the users. Through this research, we intend to support the advanced transportation sector by providing reliable and promising solutions for securing charging infrastructure.

1.1. Case studies revealing the significance of the proposed system

According to the recent announcements made by the government of India Indian Computer Emergency Response Team (CERT-In), which is assigned the responsibility to keep record of the cybersecurity incidents in India, have reported vulnerabilities in the Electric Vehicle Charging station applications. CERT-In raised alerts and vulnerability notes seeking reformative measures.

A white hat attack on German Tesla charging stations was made in January 2023 which revealed that Tesla vehicles were getting hacked and were performing the vehicle operations such as unlocking doors, honk horns and even drive the car [15].

As per the statistics provided by CERT-In, the number of cyberattacks against EV charging from 2018 to 2022 has drastically increased from 2 lakhs to almost 14 lakhs.

Several charging stations in Russia were disabled while the stations' video displays showed annoying words on Russian President, as well as denying charge to EV users [12].

The studies made at SaiFlow, an Israel-based company, states that the vulnerabilities in the EV charging infrastructure can be exploited for DoS Attacks [16].

All the above-mentioned recent case studies from different parts of the world reveal the necessity of the deployment of an efficient IDS to detect the malicious traffic and protect the system. As described in the objectives of the proposed system ensures security and privacy to the user information by accurately detecting and classifying the intrusions or malicious traffic entering the charging infrastructure. The proposed methodology is trained using the dataset containing normal and malicious traffic for attack detection and classification and provides solution for the above security breaches which is elaborated in Section 5.3. In this scenario, using IoT devices, we collect the information of the vehicle and the users. After detection, the identified attacks are neglected from the charging infrastructure, while the normal data are allowed to enter in the network. Consequently, the system offers cost minimization by optimally selecting the charging unit.

The major contributions of the study are described below.

- The presented study introduces a multi-objective framework using deep learning and metaheuristic optimization algorithms to preserve security and minimize charging costs in the EV and UAV charging stations.
- The study developed the ADRNN module, which combines the efficiency of the Attention mechanism with a deep recurrent neural network for accurate and reliable attack prediction in charging infrastructure.
- Further, we employ the Squirrel Search Algorithm to optimize users' charging costs by selecting the appropriate charging unit, enhancing both cost and resource utilization efficiency.
- Finally, the study's results were determined and validated with conventional algorithms in terms of accuracy, precision, recall, f-measure and computational time.

The following parts of the article are described as follows: Section 2 provides the detailed review of the current IDS frameworks, Section 3 presents the problem statement, Section 4 details the working of the proposed strategy, Section 5 provides the detailed discussion of the results, and Section 6 presents the article conclusion.

2. Related works

The EV and UAV charging infrastructure comprises the sensing, communication, and networking components. The sensing part is mainly prone to physical attacks which are small scale. The installation of surveillance systems and tamper proof hardware units may primarily resolve these issues. The large-scale attack mainly occurs at the networking and internet connection side where all the communication occur between the energy requestors and providers. In the grids, the incorporation of open communication layer into the physical layer offers various facilities such as automation, intelligence resource management and bidirectional communication. However, this layer is prone to cybersecurity threats and reduces the integrity and confidentiality of the grid resources. The Confidentiality Integrity Availability (CIA) Triad when compromised leads to security breaches. Figure 1 depicts the systematic architecture of EV and UAV charging infrastructure with the major category of attacks.

The major category of attacks are Denial of Service (DOS) Attacks, Man-in-Middle attacks, False Data Injection as well as Malware Injection [17]. The DOS attacks mainly occur by flooding the EVCS with large amount of request which leads to blocking of the system's normal function. These attacks are critical as the EV users might approach CS when in emergency and being denied of the service leads to fatal situation. Man-in-Middle is an active kind of attack in which the intruder intercepts the communication between the EV users and this may lead to misinterpretations in the

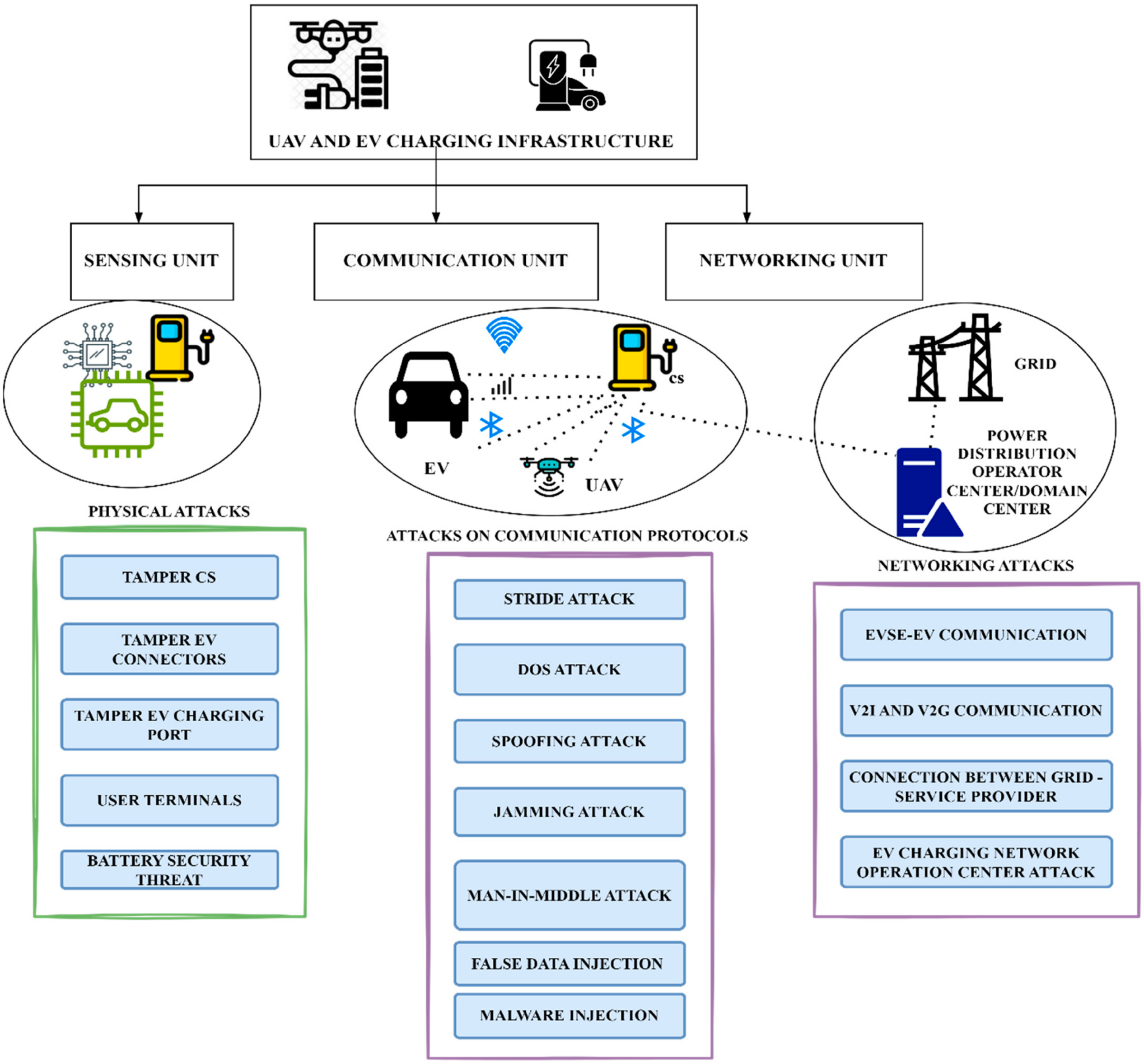


Figure 1. Systematic architecture of EV charging infrastructure and major attacks.

energy trading. The charging request can be altered leading to excessive charging or discharging as well as sensitive information of the users can be leaked. The False Data Injection attacks cause unauthorized access in the communication protocols which may result in varying the battery status information or charging rates. In an STRIDE attack, the attackers send forged de-authentication packets to disconnect legitimate users from the network. In a jamming attack, the attackers flood the network with radio signals to disturb the communication. The GPS attacks include GPS jamming and GPS spoofing. In the case of GPS jamming, the attacker emits a signal at an identical frequency as the authentic GPS signal, aiming to interfere with and disrupt the communication of GPS signals. On the other hand, GPS spoofing involves the attacker transmitting fabricated GPS signals to mislead UAVs by providing false location information.

Malware injection attacks mainly occur when malicious scripts are injected to the publicly available Electric Vehicle Supplier Equipment (EVSE) from where it stretches out to the other units of EV charging infrastructure. These types of phishing attacks can pose a major threat to EV charging as the web applications may contain malicious script which led to bogus website. It may cause theft of sensitive data of the users and regular security checking is to be maintained to protect the system from these attacks. It is crucial to identify these attacks in prior [18]. A study on detection of whether an URL is benign or not using machine learning algorithm is described in [19]. Among the several machine learning algorithms, Random Forest provided a higher accuracy rate of 97% in identification of malicious URL [20]. Further study using ensemble model reveals the outstanding performance of Catboost model for identifying an URL is benign or not [21]. These attacks mainly occurs via web applications and hence the identification of the malicious network traffic prior to usage of the application will help to safeguard the energy trading infrastructure of EV and UAVs from these kind of attacks. A constant watch on the incoming traffic for the identification of all potential threats is the main goal of IDSs.

The conventional intrusion detection models use signature-based and anomaly-based detection methods to identify and mitigate cybersecurity threats, ensuring data security in the charging infrastructure [22]. These models scan unusual activities and send instant alerts to system administrators, assisting them in responding to security threats quickly. The most common types of intrusion detection models include Signature-based detection (SD), Anomaly-based detection (AD) and Stateful protocol analysis (SPA).

In SD approach, the attack patterns are compared with the incoming data patterns, making the system to identify the malicious data entry. However, this approach cannot learn or capture the new or unknown attacks. In addition, the system operator must upgrade the fingerprint (patterns) of the unknown or new attacks manually. The AD-based IDS approach identifies the malicious data entry by examining whether the incoming packet varies from the normal network characteristics or not, and this is the most employed IDS framework. Despite its widespread use, the AD approach has limitations, such as a higher rate of false positives and minimum accuracy than the SD technique. Some studies focused on developing hybrid models combining SD and AD to mitigate these limitations. By leveraging the strengths of both methods, they intended to enhance detection accuracy and reduce false positives.

Another approach is SPA, which can monitor the state and behaviour of network protocols, identifying deviations from expected communication patterns. Unlike SD and AD, which focus primarily on data patterns and statistical anomalies, SPA delves into protocol-level interactions, making it reliable for detecting attacks and preserving privacy [23]. The primary difference between the AD and SPA approaches is that the SPA equates the actual network characteristics against standard security protocols, while the AD equates it against the observed network characteristics. The SPA approach is resource intensive, as it must track and analyse the protocol states. In addition, it cannot examine the normal protocol characteristics, making it not suitable for real-world applications. Hence the studies on the IDS types concluded that the AD-based approach is more effective and reliable than others and is widely used in current applications. Through a comprehensive exploration of several AD-based IDS approaches using different Deep Learning (DL) and Machine Learning (ML) algorithms such as Support Vector Machine (SVM), Random Forest (RF), Principal Component analysis (PCA) and KNN Classifier, Convolutional Neural Network (CNN), ML-based IDS, Embedding Feature Selection and ensemble learning-based IDS, Voting based on Negative Selection Algorithm based ID, etc., we analysed. The key issues like limited generalizability, computational time, overfitting, complexity, etc. are yet to be addressed precisely. Some of the recent works associated with the IDS for EV are summarized in Table 1.

In addition to threat detection, ensuring privacy is significant in charging infrastructure to ensure the confidentiality and integrity of user data. Since the communication between EVs and UAVs is established in a dynamic environment, a stable and effective connection needs to be established among the entities. One common approach to establishing stable connections is content-centric networking. This approach improves communication by focusing on the transmitted content rather than the endpoints [34]. Other preserving techniques involve using cryptographic approaches and

Table 1. Summary of recent works in intrusion detection mechanisms for EV.

Author	Title	Algorithm/Model	Dataset	Performance Metrics	Inference	Limitations
Manoj Basnet et al.	Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station [24]	LSTM + DNN	CICIDS 2018	Accuracy	LSTM is a highly efficient algorithm with high accuracy rate of approximately 97.6%	This method lacks generalizability and faces higher false alarm rate
Manoj Basnet et al.	Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station [25]	LSTM + DNN + CNN	Simulation Dat for ransome and normal samples	Accuracy, F1 Score, AUC	A distinct and unique ransomware identification method for the Supervisory Control and Data Acquisition (SCADA)-assisted EVCS	Although the system provides low false alarm rate, the integration of multiple DL algorithms into single approach is complex and requires knowledge expertise
Manoj Basnet et al.	Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning [26]	LSTM + NN	Dataset created from the proposed system EVSE architecture	Accuracy	False Data Injection and DDoS Attacks on the networking component of EVSE were simulated and studied	The study solely concentrates on attacks faced by the 5G enabled SCADA
ElKashlan et al.	A Machine Learning-Based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCSs) [27]	Naïve Bayes classifier, J48 classifier, attribute-select classifier, Filtered classifier	IoT-23, validated using the real IoT EVCS traffic database	Accuracy, Precision, Recall, F1 Score	Considering precision, F-1 score and Recall, the filtered classifier has the highest rank and lowest modelling time	The scope of the study is limited to low dimensional data, and hence further analysis must be done for large-scale dataset. This framework demands more resources for training, and it is costly
ElKashlan, M et al	Intrusion Detection for Electric Vehicle Charging Systems (EVCS)[28]	Decision Table and Filtered Classification Algorithm	IoT-23	Accuracy, Precision, Recall, F1 Score	filtered classifier algorithm can handle missing attribute scenarios	the performance of this approach decreases when the IoT data increases
Manoj Basnet et al.	Deep Reinforcement Learning-Driven Mitigation of Adverse Effects of Cyber-Attacks on Electric Vehicle Charging Station [29]	Twin Delayed Deep Deterministic Policy Gradient (TD3)	Simulation-based data	Hyperparameter sensitivity, convergence, stability	To alleviate the type I and type II attacks on EVCS controllers TD3-based software clones are used. The system resolves the issue of incremental bias, and hyperparameter sensitivity of the conventional EVCS controllers	5G-based applications are yet to be analysed, training this model is resource intensive and time-consuming
Manoj Basnet et al.	WCGAN-Based Cyber-Attacks Detection System in the EV Charging Infrastructure [30]	External classifier Wasserstein condition GAN (EC-WCGAN)	Synthetic data generation using GAN Network, NSL KDD Dataset	Accuracy, Recall, Precision	To identify DDoS attack in EV charging infrastructure, WCGAN provides improved performance than Deep learning algorithms	The training process is highly complex and requires more resources, it is not directly applicable for real-world EVCS, as it cannot adapt dynamic characteristics of charging station
Warraich et al.	Early detection of cyber-physical attacks on fast-charging stations using machine learning considering vehicle-to-grid operation in microgrids [31]	Discrete samples of power demand readings	Decision tree model and K Fold Validation	Classification Accuracy and F1 Score	To detect the attacks affecting the fast-charging stations which aims to allow fast charging for Evs along with frequency and voltage regulation to electricity grid	The proposed system takes into consideration power demand profile and most salient features can be extracted by computing the rank of predictors for better performance, this approach cannot identify diverse attack scenarios and different kinds of attacks
Dalal et al.	Extremely boosted neural network for more accurate multi-stage Cyber-attack prediction in cloud computing environment [32]	Multi-Step Cyber-Attack Dataset (MSCAD)	Boosted Neural Network	99.72% accuracy	The system is used to detect multi-stage cyberattacks	The system is not studied on real-time traffic
Guru Bhandari et al.	Distributed Deep Neural Network-Based Middleware for Cyber-Attacks Detection in Smart IoT Ecosystem: A Novel Framework and Performance Evaluation Approach [33]	Deep Neural Network	Aposemat IoT-23 dataset, Edge-IIoTset	Detection Accuracy and F1 Score	DNN provides better results for malware detection considering all the samples of both the datasets	The system needs to be improvised so that minimal resources are used and provide better performance. Device specific data from the hardware can be taken for study of device centric security issue

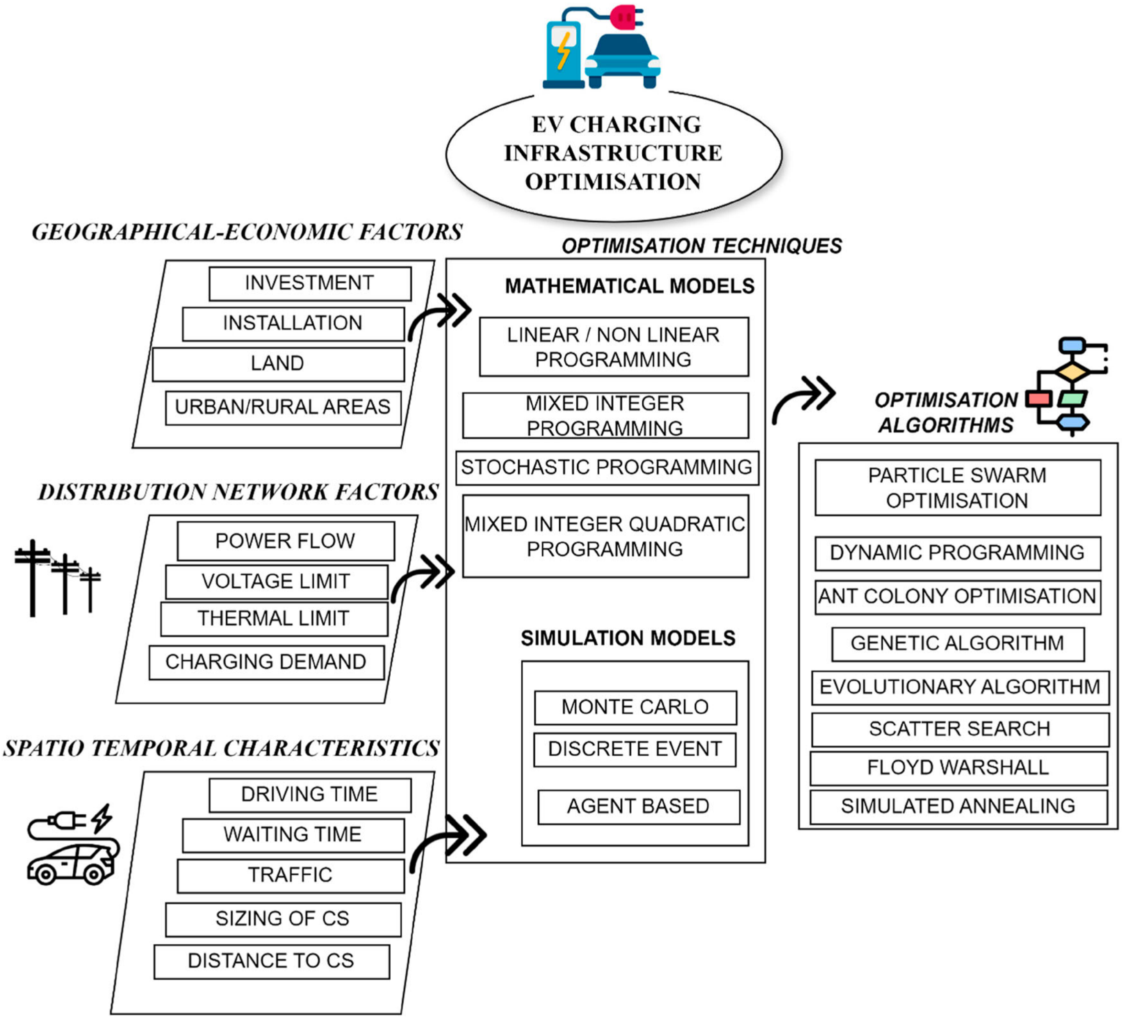


Figure 2. Summary of various parameters related to EV charging.

secure data transfer protocols to ensure the privacy and security of the data during transmission. Some of the commonly used approaches include symmetric encryption and asymmetric encryption methods. These encryption algorithms encode the data into another form, ensuring protection against threats and unauthorized data access. Symmetric encryption offers speed and efficiency, while asymmetric encryption provides stronger security through key pairs. Although the encryption techniques offer security during transmission, they face challenges, including key management complexities and computational overhead. Moreover, they cannot secure data against other security threats, such as insider attacks or system vulnerabilities [35]. These challenges make the existing approach ineffective in providing security and privacy to the data and hence intensive studies are being carried out to fill in these gaps.

Another primary concern hindering the fast adoption of EV and UAV is the charging cost optimization of energy trading. A summary of the various parameters related to energy charging discussed in the existing studies is shown in Figure 2. Based on this analysis, the vital objective function was narrowed down to minimize the charging rate taking into consideration the history of charging. The different mathematical models [36], simulation models [37] and metaheuristic algorithms [38,39] that are feasible for the system implementation were identified as in the summary figure. The recently developed Squirrel Search Algorithm (SSA) and its outstanding performance in comparison with six other optimization algorithms are discussed in [40]. The effectiveness of this SSA in terms of convergence rate and accuracy can be used to obtain more optimal solutions for the pricing mechanisms in EV energy trading.

Thus the proposed system focuses on the dual objectives of security from malicious traffic and cost minimization in the context of EV and UAV charging stations. Key components of the system design include defining privacy constraints and cost optimization metrics, identifying data sources, and preprocessing requirements, and outlining the integration of deep learning models into the charging station infrastructure. The proposed system model addresses the need for real-time decision-making based on optimized resource allocation and charging strategies to ensure efficient operation of charging stations while safeguarding user privacy and reducing operational costs.

3. Problem statement

The proposed model integrates a hybrid deep learning approach, specifically leveraging the Squirrel Search-optimized Attention-Deep Recurrent Neural Network (SS-ADRNN), to make intelligent decisions based on real-time data and constraints. The system collects data from EVs and UAVs, including charging demands, environmental conditions and historical usage patterns. This data undergoes pre-processing to clean and normalize it, preparing it for input into the SS-ADRNN model. The Squirrel Search optimization algorithm dynamically optimizes charging station operations, adjusting charging rates and schedules to minimize costs while adhering to privacy constraints. The attention mechanism within the SS-ADRNN model allows for the focusing of relevant features and inputs, enhancing interpretability and performance. The deep RNN architecture captures temporal dependencies in charging station data, enabling the model to learn from past behaviours and predict future demands. Privacy-preserving strategies are implemented throughout the charging station operations to anonymize user data and protect privacy during data handling, processing and communication.

4. Proposed methodology

The proposed methodology for privacy preservation and cost minimization in EV and UAV charging stations revolves around a Hybrid Deep Learning framework termed Squirrel Search-optimized Attention-Deep Recurrent Neural Network (SS-ADRNN). This framework integrates the strengths of deep learning with the efficiency of evolutionary algorithms, specifically tailored for privacy-sensitive and cost-efficient charging station management. SS-ADRNN employs a hierarchical architecture, where attention mechanisms focus on relevant features while deep recurrent neural networks capture temporal dependencies in charging station operations. Furthermore, Squirrel Search optimization ensures robustness against local optima, enhancing the model's ability to find globally optimal solutions. The architecture of the proposed framework is shown in Figure 3.

By leveraging SS-ADRNN, the methodology addresses critical challenges in EV and UAV charging station management. Privacy preservation is ensured through advanced encryption techniques and data anonymization strategies embedded within the deep learning framework. Moreover, the optimization objectives encompass both cost minimization and operational efficiency, enabling charging stations to adapt dynamically to fluctuating demand and energy prices. Through extensive simulations and real-world deployment, the proposed methodology demonstrates superior performance in balancing the competing goals of privacy preservation and cost efficiency, thereby offering a scalable solution for sustainable and secure charging infrastructure in the era of electric and unmanned mobility.

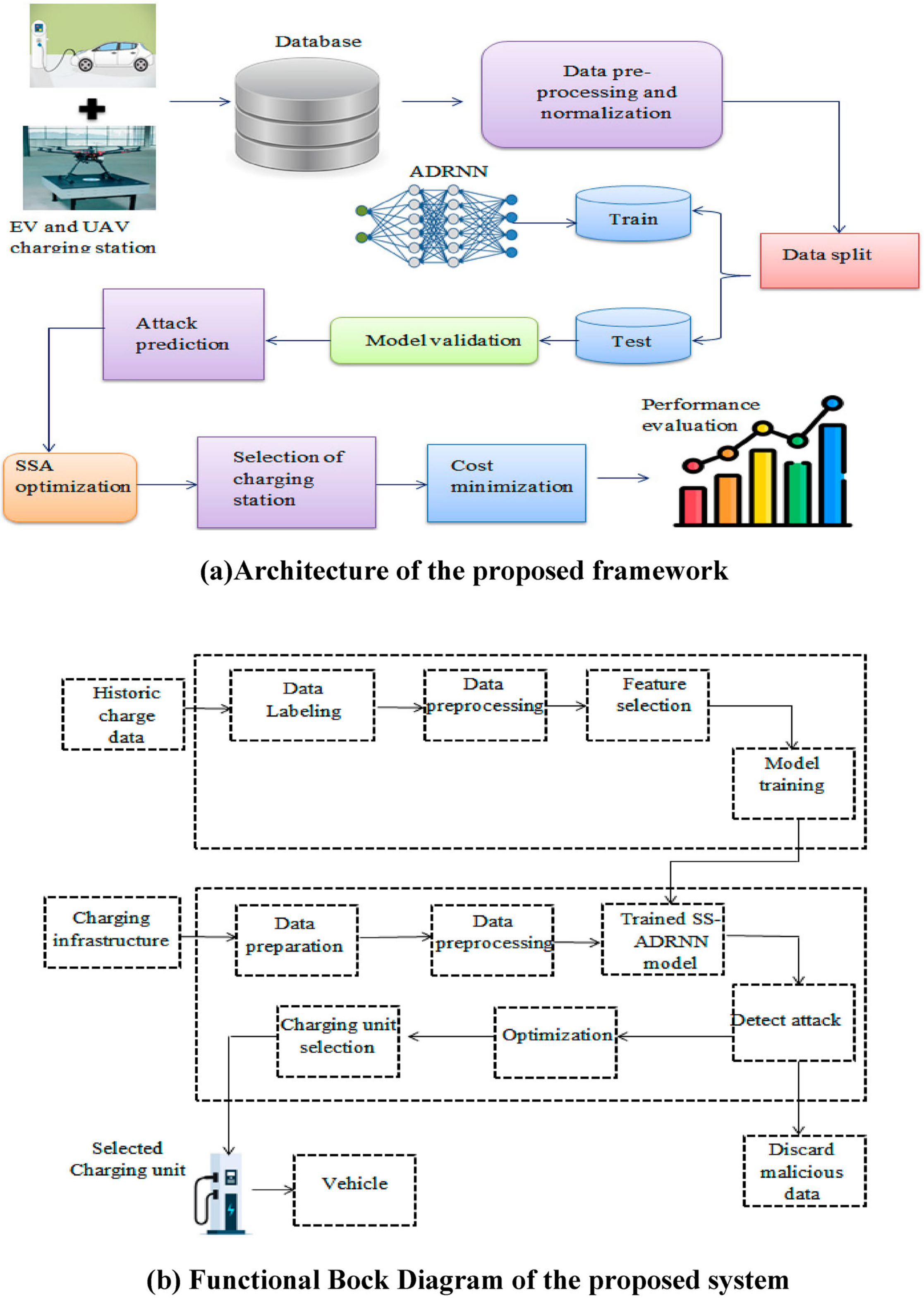
4.1. Data collection

The proposed mechanism commences with the collection of datasets. This study utilizes a publically available UAV network communication dataset from the GitHub site, available at https://github.com/naiksrinu/UAV_DataSet_NetworkCommunication. The UAV Network Communication Experimental dataset collects traffic captured from a wireless network used by UAVs during a simulated search and rescue mission. The dataset includes both legitimate network traffic and traffic generated by WiFi and GPS attacks. The WiFi attacks include different STRIDE and jamming attacks. This study also utilizes the EV network communication dataset named CICEV2023, and it is available at https://www.unb.ca/cic/datasets/cicev2023.html. This database contains four distinct attack scenarios based on Correct EV ID, incorrect EV, incorrect EV Timestamp and incorrect CS Timestamp. The features present in this dataset are described in Table 2.

4.2. Data pre-processing

Data pre-processing plays a pivotal role in ensuring privacy preservation and cost minimization in EV and UAV charging station management using the proposed SS-ADRNN framework. In this methodology, pre-processing involves several key steps. First, sensitive information such as user identities and charging patterns is anonymized using encryption techniques to protect individual privacy. Additionally, data is cleaned and normalized to ensure consistency and reliability in model training. Moreover, feature selection techniques are employed to identify relevant charging station parameters while mitigating the risk of data leakage. Furthermore, outlier detection and removal procedures are applied to enhance the robustness of the model against potential attacks or anomalies. By meticulously pre-processing the data, the SS-ADRNN framework ensures that the subsequent deep learning algorithms operate on sanitized inputs, thereby balancing the imperatives of privacy preservation and cost minimization effectively in the context of EV and UAV charging station management. Here, we used z-score normalization was employed for converting the data samples into common scale, and is formulated in Equation (1).

$$Zs = \left(\frac{D_a - \mu}{\sigma}\right) \tag{1}$$



(a)Architecture of the proposed framework

(b) Functional Bock Diagram of the proposed system

Figure 3. The proposed framework: (a) architecture of the proposed framework; (b) functional block diagram of the proposed system.

where Zs denotes normalized score for the data sample D_a, μ indicates the mean and σ represents standard deviation. Similarly, for each data sample in the dataset, the normalized value was determined. These steps not only improve data quality but also increase the speed of data processing and confirm consistency and quality.

4.3. Attention-based deep recurrent neural network

The pre-processed data is passed to the ADRNN module. The ADRNN module combines the efficiency of Attention Mechanism and Deep Recurrent Neural Network. The attention mechanism integrated into the

Table 2. Dataset description.

Features	Description
Instruction overhead	It offers high-level details regarding libraries and code symbols utilized in the Linux kernel by quantifying the count of instructions employed in profiling targets, specifically either CS or GS
CPU cycle overhead	Perf computes the number of cycles utilized by profiling targets and details the overhead associated with libraries and code symbols in the Linux kernel
Time delta	It defines the duration between the immediately preceding and subsequent authentications
Branches	It indicates the number of branch commands implemented by the profiling target
Branch overhead	It offers insights into the overhead associated with libraries and code symbols utilized in the Linux kernel by tallying the count of branch instructions employed by the profiling target
Instructions	It indicates the number of instructions utilized by the profiling target
Cycles	It refers to the number of cycles consumed by the profiling target

proposed framework enables to focus on most important attributes for the attack prediction in EV and UAV charging infrastructure. On the other hand, the DRNN acts as classifier, which predicts the normal and malicious traffic by understanding the interrelationship and patterns between the input and output. Attention mechanism is a deep learning, which is employed for selecting the most informative features from the pre-processed dataset. The input of the attention mechanism is expressed in Equation (2).

$$P_R(Da) = \{da_1, da_2, da_3, \ldots, da_n\} \tag{2}$$

where $P_R(Da)$ defines the pre-processed database, da denotes the attributes present in the dataset. The attention mechanism generates the attention score A_{ts} for each feature da in the dataset using a scoring function. The attention score is determined using Equation (3)

$$A_{ts} = soft\max(w_t.da) \tag{3}$$

where w_t defines the weight function used for evaluating the attention scores. After evaluating the attention scores, the features with greater attention scores are selected for DRNN training. This feature set contains most important and relevant attributes for classifying the normal and malicious data. This feature sequence is fed as input to the DRNN module for training and attack prediction.

The DRNN is a deep learning algorithm that consists of multiple recurrent layers in the neural network architecture. Generally, the RNN contains single recurrent layer, which can process the sequential data by storing the previous inputs in the memory. In DRNN, the outcome of one recurrent layer is forwarded as input to the next recurrent layer, and the number of recurrent units depends on the complexity of the problem. These multiple recurrent layers help the system to capture, understand, and learn the intricate patterns and interconnections between the normal and malicious data. The designed DRNN mechanism contains three layers such as input layer, two or more recurrent layers, and output layers. These layers relate to each other through neurons. The connection involves feedback of weights and bias vector in between the neuron connection. In DRNN, the recurrent layer acts as the memory unit, and each memory unit contains memory cells with self-connections for storing the temporal state information. This capacity of DRNN enables to learn the long-term temporal dependencies in the sequential input data.

The presented study utilizes the LSTM architecture of DRNN. This architecture of LSTM contains various gates to control or regulate the information flow in the network. The LSTM gates includes input gate, forget gate, cell state and output gate. The LSTM's input gate is represented mathematically in Equation (4).

$$Ig_t = \sigma_i(W_{ig}Ao_t + W_{hi}hs_{t-1} + B_{ig}) \tag{4}$$

where Ig_t represents the input gate at time t, σ_i denotes the input gate activation function, W_{ig} defines the input gate weight matrix, W_{hi} indicates the weight matrix between the input gate and hidden unit, hs_{t-1} represents the hidden state at previous time sequence and B_{ig} refers to the input gate bias vector. The input gate of the LSTM helps to learn that what portion of the input sequence must be integrated into the cell state. After input gate, a forget gate was designed, which takes decision regarding what feature or data from the previous cell state should be forwarded to the next cell state, and what feature should be eliminated. It is expressed in Equation (5)

$$fg_t = \sigma_{fg}(W_{fg}Ao_t + W_{hf}hs_{t-1} + B_{fg}) \tag{5}$$

where fg_t indicates the forget gate at time step t, σ_{fg} defines the forget gate activation function, W_{hf} denotes the weight matrix interconnecting forget gate and hidden state, W_{fg} represents the forget gate's weight matrix, and B_{fg} defines the forget gate bias vector. This gate acts as the bridge between the input gate and the cell state. After forget gate, a cell state is placed, which gathers the information or feature from the input and forget gates, and update its state. This feature enables the system to learn and capture the intricate features and patterns for malicious data prediction and it is computed in Equation (6)

$$\begin{aligned} cs_t =& fg_t * cs_{t-1} \\ &+ Ig_t * \tan h(W_{csi}Ao_t + W_{csh}hs_{t-1} + B_{cs}) \end{aligned} \tag{6}$$

where cs_t represents the cell state at time t, cs_{t-1} refers to the previous cell state, $tanh$ indicates tangent activation function, W_{csi} defines the weight matrix interconnecting cell state and input gate, W_{ch} refers to the weight matrix interconnecting cell state and forget state and B_{cs} represents cell state bias vector. The updated feature sequence from the cell state is forwarded to the output gate. The updated feature sequence contains information regarding the pattern difference between the normal and malicious data. The output gate is expressed in Equation (7)

$$Og_t = \sigma_{og}(W_{ogi}Ao_t + W_{ho}hs_{t-1} + B_{og}) \quad (7)$$

where Og_t refers to the output gate at time step t, σ_{og} represents the output gate activation function, W_{ogi} denotes the weight matrix interconnecting output gate and input gate, W_{og} defines the weight matrix connecting the output gate to the hidden state, and B_{op} represents the output gate bias vector. The output gate represents the result of each LSTM layer, and the output of last LSTM (recurrent) layer is forwarded into the output layer. The DRNN's output layer is expressed in Equation (8)

$$Op_t = soft\max(W_{op}.Og_t + B_{op}) \quad (8)$$

where Op_t represents the outcome of the DRNN, *softmax* defines the activation function, W_{yo} indicates the weight matrix of the output layer and B_{yt} denotes the bias vector of the output layer. This output layer provides the probability value, which helps to classify the data as malicious or normal. The malicious activity classification is represented in Equation (9).

$$C_f = \arg\max(Opt) \quad (9)$$

where C_f indicates the classification function that determines the attack type with the highest probability. Based on the probability value, the *arg max* function returns a class (normal or attack types [STRIDE, jamming, GPS jamming, GPS spoofing]). Thus, based on the learned patterns, the proposed strategy detects the intrusion by comparing the pattern of pre-processed data with the learned malicious traffic pattern. If the input data pattern matches with the malicious data pattern, then the system predicts it as "Malicious". Then the model intends to identify the type of attack or intrusion by estimating the probability value of the traffic. After classification, the developed algorithm eliminates the data to ensure security and confidentiality of the charging infrastructure.

If the probability value range is [0, 0.1], the system classifies the traffic as "normal", if the range of probability value is [0.2, 0.3], the system classifies the traffic as "STRIDE". If the range lies in [0.3, 0.4], the system categorizes it as "Jamming", and if the range lies in [0.4, 0.5], the system predicts it as "GPS jamming". Finally, if the range of the probability value is [0.5, 0.6], then the system classifies it as "GPS spoofing".

The ADRNN framework undergoes intensive training, and the loss during training is measured using Equation (10)

$$Ls = \frac{1}{Ts}\sum_{i=1}^{Ts}(A'_s - P_s) \quad (10)$$

where Ls defines the loss function, Ts denotes the total number of training samples, A'_s represents the actual outcome and P_s refers to the predicted value. This loss can be resolved by tuning the hyperparameters of ADRNN using the random search optimization.

4.4. Squirrel Search Algorithm

Once the attacks are identified and classified using the ADRNN module, the malicious traffic is eliminated from the system to ensure security and privacy for the original users. After attack detection, Squirrel Search Optimization was employed to optimize the charging cost for users in the charging environments. A squirrel search algorithm is a nature-inspired optimization approach inspired by flying squirrels' foraging characteristics (gliding). Gliding is an effective mechanism that small mammals use to travel long distances [40]. The squirrels use this strategy to change their location during warm weather to explore food resources. After finding the food resources, they store the food for winter. Typically, these squirrels are active in warm climates and less active during winter. The mathematical formulation of these foraging characteristics is being applied to resolving unimodal, multimodal and multidimensional optimization problems. Each flying squirrel searches for food individually and optimally uses available food resources by employing dynamic foraging behaviour. Similarly, we utilized these foraging characteristics to search for charging unit with minimum cost, considering the available energy resources in EV and UAV charging stations. In the proposed work, the SSA algorithm was employed to find the charging unit with less cost in the charging environments. The first step in SSA is the initialization of algorithm parameters, which includes maximum iteration, population size, number of decision variables, gliding constant, and scaling factor. Consequently, the flying squirrel was initialized. The SSA optimization starts with the random initialization of the location of flying squirrels. Like this, we initialized the location of charging units and it is expressed in Equations (11) and (12).

$$C_u = \begin{bmatrix} ch_{11}ch_{12}ch_{13}\ldots..ch_{1n} \\ ch_{21}ch_{22}ch_{23}\ldots..ch_{2n} \\ \vdots\vdots\vdots\ldots\ldots\vdots \\ ch_{m1}ch_{m2}ch_{m3}\ldots..ch_{mn} \end{bmatrix} \quad (11)$$

$$V_{i,j} = V_l + rand() * (V_u - V_l), \quad i = 1, 2, \ldots.., s \quad (12)$$

where C_u defines the location of charging stations, ch denotes the charging unit, vehicles (EVs or UAVs),

V_u V_l the upper and lower bounds of the decision variables, and *rand*() random numbers in the range [0, 1]. Then the distance between the vehicle's location and the charging unit's location was determined. The distance calculation is expressed in Equation (13)

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)} \tag{13}$$

where $D_{i,j}$ indicates the distance between the vehicles. After initialization, the fitness of each flying squirrel is determined. In the proposed work, the fitness value of charging unit was evaluated based on the pre-defined objective function.

Thus the second step is to determine the population's value based on the defined objective function. The objective function is to reduce the charging cost of vehicles by finding the charging unit with a lower cost, considering the vehicle's location from the charging station. The objective function is defined in Equation (14).

The objective function is defined in Equation (14).

$$Objective = \min(C_{ch}) \tag{14}$$

where C_{ch} denotes the charging cost at the charging unit *ch*.

Then the fitness value of each charging unit is determined. The fitness value of the charging unit is represented in Equation (15)

$$F(C_u) = \begin{bmatrix} f(ch_{11} & ch_{12} & ch_{13} & \ldots..ch_{1n}) \\ f(ch_{21} & ch_{22} & ch_{23} & \ldots..ch_{2n}) \\ \vdots & \vdots & \vdots & \ldots\ldots\vdots \\ f(ch_{m1} & ch_{m2} & ch_{m3} & \ldots..ch_{mn}) \end{bmatrix} \tag{15}$$

where f indicates the fitness of the charging unit. The charging cost is determined by considering the available energy in the charging infrastructure, the distance between the vehicle and the charging unit and the energy demand of the user.

After fitness evaluation, the entire population was sorted in descending order, such that the charging unit with minimum cost was displayed first and the charging unit with maximum cost was displayed last. Then the SSA explores the search space to find the optimal solution (exploration). This exploration phase enables the system to provide optimal solutions irrespective of the changing conditions in the charging infrastructure. This update follows the gliding mechanism of the squirrels. The positions of the charging units are updated using Equation (16).

$$(ch_{t+1}) = (ch_t) + D_{i,j}G.(ch' - ch_t) \tag{16}$$

where (ch_{t+1}) indicates the updated solutions, ch_t the current solution and G the gliding constant. After position updating, the fitness value was determined for the updated solutions. If the fitness of the updated charging unit is high, then the system suggests the vehicle select the updated charging unit. On the other hand, if the fitness of the updated solution is low, then the system suggests the old charging unit (charging station selected before updation). The greater fitness value defines that the charging unit with minimum cost. Hence after fitness updation, the charging unit with higher fitness value is selected for charging.

```
Algorithm: SSA-ADRNN
Input: UAV network communication dataset, EV network communication
   dataset, ADRNN hyperparameters, maximum iteration of SSA ($tmax$),
   charging unit locations;
Output: Classification results (malicious or normal), optimized charging
   unit with minimal cost
Initialization: EV and UAV datasets, ADRNN hyperparameters, SSA
   parameters, charging unit locations
 1. Data pre-processing:
      For each database:
         Perform outlier detection using linear interpolation
         Handle missing values with mean imputation
         Normalize features using z-score normalization
      End for
 2. Define the ADRNN architecture (LSTM layers, attention mecha-
    nism):
      For each data point$da$ in the database$P_R(Da)$:
         Determine attention score$A_{ts}$
         Select $da$with high attention score
         Train DRNN with selected features
            For each training epoch:
 3. Compute probability$Op_t$
      if ($Op_t > 0.5$)
         Malicious
      Else
            Normal
         End for
         Compute loss using Equation (10)
         Tune hyperparameters to minimize loss $Ls$
 4. Squirrel Search Algorithm:
      while $t < tmax$ do
         For each charging unit $ch$in the population size of $n$ do
            Calculate $f$
            Sort the population in descending order
            Determine global best solution$ch$
            Update the locations of charging units $ch'$
            Calculate fitness $f'$for updated solution$ch_{t+1}$
            If ($f' > f$)
                  Select updated charging unit
            Else
                  Select initial charging unit location
            $t$++
            End for
      Check termination criteria
   End while
End
```

Thus the SSA algorithm optimizes the vehicles' charging cost by suggesting a charging station with minimal cost. This process continues until reaching the maximum iteration or maximum convergence. At each iteration, the system selects the charging unit with minimum cost for the EVs and UAVs.

A flowchart of the proposed methodology is displayed in Figure 4. The working of the proposed algorithm is presented in pseudocode format in Algorithm 1.

5. Results and discussion

In this study, we developed a hybrid SS-ADRNN mechanism for effective identification of malicious activities

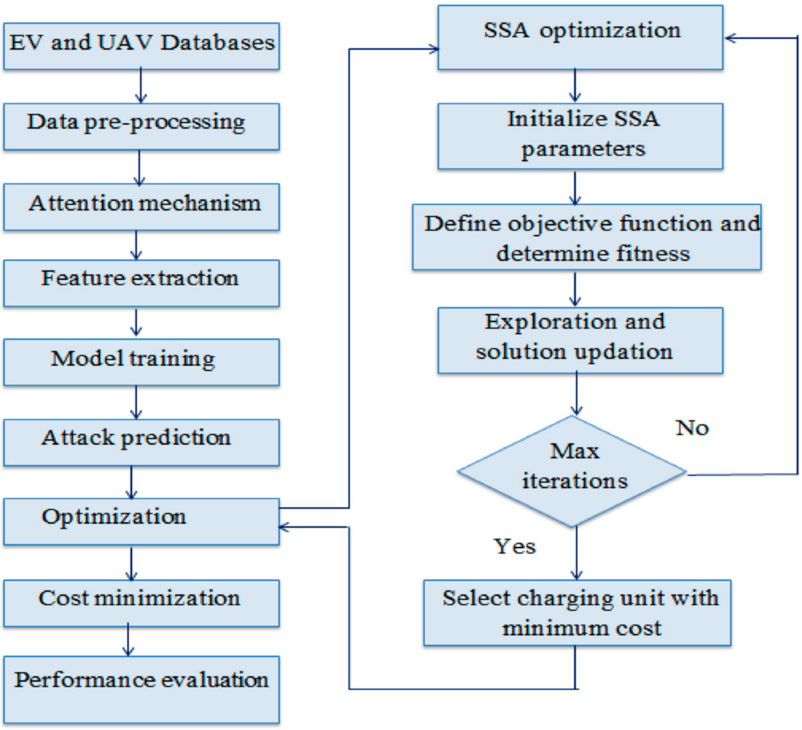


Figure 4. Flowchart of the proposed framework.

in EV and UAV charging infrastructure. The proposed methodology combines the efficiency of Squirrel Search Optimization and Attention-assisted Deep Recurrent Neural Network. The ADRNN acts as a classifier, which identifies the normal and malicious data in charging infrastructure by understanding the patterns and relations between them, while the SSA optimizes the cost of the EV and UAV charging infrastructure, ensuring improved resource utilization and charging cost minimization for EV and UAV users. The presented framework was implemented in Python software and the results of the study were evaluated in terms of accuracy, precision, recall, f-measure, resource utilization rate and cost.

5.1. Performance analysis

In this module, we examined the training and testing performances of the proposed framework in terms of accuracy and loss. In the initial phase, the dataset was split into the ratios of 75:25 for training and testing purposes. Table 3 presents the parameters of ADRNN.

Table 3. Parameters of the ADRNN model.

Parameters	Value/range
Training epochs	80, 25
Recurrent layer type	LSTM
Learning rate	0.01
Batch size	32
Optimizer	Random search optimizer
Loss function	Cross-entropy
Number of layers	2
Hidden units	128
Dropout rate	0.1
L2 Regularization	0.0001

The accuracy defines how efficiently and quickly the proposed algorithm learns the patterns and interrelations between the normal and malicious data, while the loss measures the variation between the actual and predicted outcomes. Figures 5(a, b) present the loss and accuracy of the proposed framework for EV dataset. The training accuracy measures the effectiveness of the proposed algorithm for capturing and understanding the correlation between the malicious and normal data in EV and UAV charging infrastructures. It measures how fast the developed strategy learns and predicts the malicious data. On the other hand, the testing accuracy quantifies how efficiently the proposed framework detects the malicious data on unseen data samples. It measures the presented model's generalizability to unknown samples.

The training loss defines the difference between the actual (real) and the predicted outcomes of the proposed strategy for the train data samples. The small deviation between the real and predicted results demonstrates that the designed framework correctly identifies the malicious class. On the other hand, the testing loss measures the variation between the real and evaluated results of the proposed strategy for test or unknown data samples. This measures the generalization ability of the developed mechanism for unseen data samples. Also, it quantifies how precisely the proposed system works for the unknown data. Figures 6(a, b) illustrate the loss and accuracy of the developed framework for UAV dataset.

This intensive evaluation of training and testing performances of the proposed strategy highlights that it obtained greater training and testing accuracy,

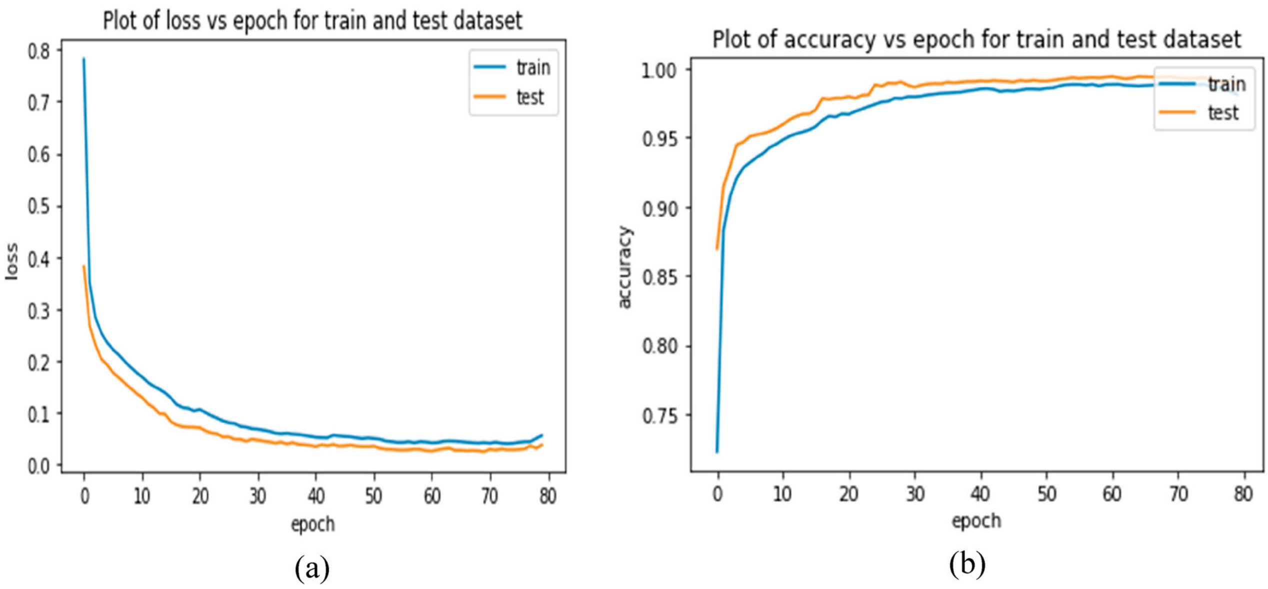


Figure 5. Performance of EV dataset: (a) loss and (b) accuracy.

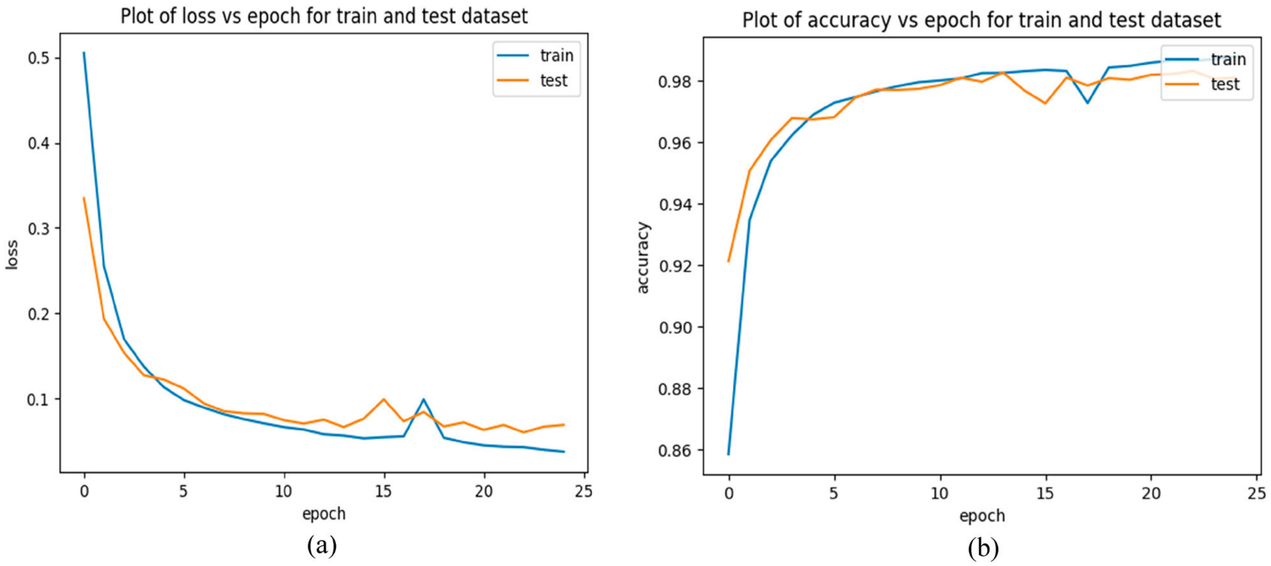


Figure 6. Performance of UAV dataset: (a) loss and (b) accuracy.

demonstrating its effectiveness in understanding the pattern and interconnection between the normal and malicious data. In addition, the minimum losses in training and testing phases evaluate that the predicted results are the same as the actual results. Figures 7(a, b) present the confusion matrix for EV and UAV datasets.

5.2. Evaluation metrics

This section discusses the metrics used to evaluate the proposed strategy's performance. The metrics include accuracy, precision, recall, f-measure, computational time, resource utilization and cost efficiency. The definitions of the above metrics are described below.

5.2.1. Accuracy

Accuracy measures how effectively the model detects and classifies the normal and malicious traffic in charging infrastructure. It is measured in percentage (%). It defines the ratio of correct classifications to the total classifications made by the system and is formulated in Equation (17).

$$Accuracy = \frac{T_{PS} + T_{NG}}{T_{PS} + T_{NG} + F_{PS} + F_{NG}} \tag{17}$$

T_{PS}, T_{NG}, F_{PS} and F_{NG} define the true-positive, true-negative, false-positive, and false-negative, respectively.

5.2.2. Precision

Precision defines the model's efficiency in correctly identifying and classifying the specific attack class among the total instances labelled as malicious. It is measured in percentage (%) and is defined in Equation (18). It defines the proportion of true-positive predictions to the total number of instances labelled as

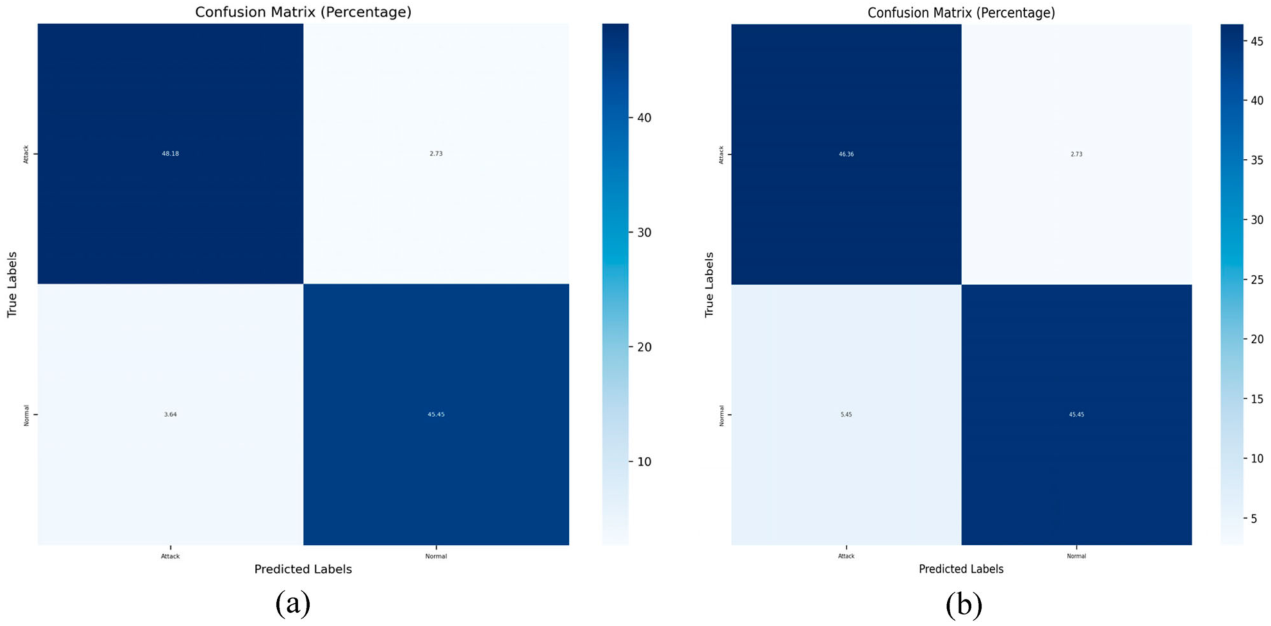


Figure 7. Confusion matrix: (a) EV dataset and (b) UAV dataset.

positive.

$$Precision = \frac{T_{PS}}{T_{PS} + F_{PS}} \tag{18}$$

5.2.3. Recall

Recall measures the proposed framework's ability to correctly detect all attack instances among the real attack cases present in the database. It is measured in percentage (%). It quantifies the proportion of the true-positive predictions to the total number of real attack cases and is formulated in Equation (19).

$$Recall = \frac{T_{PS}}{T_{PS} + F_{NG}} \tag{19}$$

5.2.4. F-measure

The F-measure metric measures the harmonic mean of precision and recall. It offers a balanced evaluation of system performances, considering both false positives and negatives. It is measured in percentage (%). The formula for F-measure is expressed in Equation (20).

$$F - measure = 2\left[\frac{recall * precision}{recall + precision}\right] \tag{20}$$

5.2.5. Computation time

Computational time defines the total time the model spends performing tasks such as data pre-processing, feature extraction, model training, attack detection and classification, and cost optimization. It is measured in seconds (s). This metric enables us to determine the computational efficiency of the proposed model; it is mathematically represented in Equation (21).

$$Computational\ rate = T_{dp} + T_{fs} + T_{mt} + T_{ad} + T_o \tag{21}$$

where T_{dp} indicates the computational time, defines the consumed for performing data pre-processing, T_{fs} represents the time taken for feature extraction, T_{mt} defines the time consumed for model training, T_{ad} denotes the time taken for attack detection and classification, and T_o defines the time consumed for cost optimization task.

5.2.6. Data confidential rate

The data confidential rate defines the rate at which the proposed strategy protects sensitive information in EV and UAV charging infrastructure from cybersecurity threats. In other words, this metric enables us to assess how effectively the developed mechanism preserves privacy in the EV and UAV charging environment, and it is represented in Equation (22).

$$Data\ confidental\ rate = \frac{Dpr}{Tp} \tag{22}$$

where Dpr indicates the number of data packets correctly received and Tp defines the total number of packets sent in the charging environment.

5.2.7. Cost efficiency

Cost efficiency measures the proposed framework's ability to minimize the overall costs associated with the charging stations for EVs and UAVs while maintaining the charging standards, and it is measured in percentages. It is formulated in Equation (23)

$$\text{Cost efficiency} = 1 - \frac{Cbs}{Cas} \tag{23}$$

where Cbs indicates the charging cost before SSA optimization and Cas denotes the charging cost after SSA optimization. It is measured in percentage. The charging cost is determined by multiplying the total energy consumed by the vehicle with the price of electricity.

5.2.8. Intrusion detection overhead

Intrusion detection overhead defines the proposed strategy's time to identify and respond to malicious traffic. This metric determines how fast the model identifies and classifies the traffic. It is expressed in Equation (24).

$$\text{Intrusion detection overhead} = \text{Td} - \text{Ts} \tag{24}$$

where Td denotes the time taken by the system for detecting malicious data/traffic and Ts indicates the time consumed by the system for responding to the malicious data. It is measured in seconds (s).

The intensive evaluation of these metrics allows us to determine the efficiency of the proposed strategy in performing intrusion detection and cost minimization. These metrics are evaluated by training and testing the presented strategy using the EV and UAV databases on the Python platform.

5.3. Comparative analysis

To validate the performance of the proposed strategy, a comprehensive comparative analysis was made with the state-of-the-art models and recently developed approaches. The techniques used for comparative assessment include Random Forest (RF), Decision Tree (DT), Logistic Regression (LR), Linear Discriminant Algorithm (LDA) [41], Long Short-Term Memory (LSTM), Deep Neural Network (DNN) [14], Continuous Wavelet transform with Convolution Neural (CWT-CN) [42], ResNet Autoencoder based Cyber-Physical Anomaly Detection (RA-CAD) [43], Self-Adaptive Intrusion Detection (SAID) [44] and Exhaustive Distributed Intrusion Detection (EDID) [45]. The performance metrics used for comparative study include accuracy, precision, recall, f-measure, cost efficiency, data confidential rate, computational time and resource utilization efficiency. The performances are measured by implementing all approaches in the Python software and validating them using both the UAV and EV datasets.

Accuracy measures the model's effectiveness in predicting and classifying the normal and malicious traffic in the EV and UAV charging infrastructure. Figure 8(a) presents the comparative evaluation of accuracy. The existing models, including RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID, achieved an average accuracy rate of 97.12%, 96.78%, 95.34%, 92.9%, 95.35%, 94.23%, 97.34%, 96.5%, 96.2% and 93.67%, respectively. In comparison, the proposed methodology achieved a higher accuracy of 99.23%. The significant improvement of accuracy by the proposed algorithm manifests that it effectively predicts and classifies the normal and malicious events in the charging infrastructure. By predicting and classifying the attacks, this strategy offers security to the charging environments.

Consequently, the precision performance of the proposed algorithm was compared with the above-stated techniques. Figure 8(b) depicts the comparison of precision. The precision metric determines the model's efficiency in predicting malicious attacks in the charging infrastructure. These above-stated techniques earned the precision of 96.89%, 95.81%, 95.07%, 91.45%, 95.2%, 94.11%, 97.5%, 96.25%, 95.0% and 93.56%, respectively. However, the developed strategy obtained a greater precision value of 98.92%. This illustrates that the proposed strategy accurately classifies the different attack instances compared to the existing models. This manifests its potential as an advanced and reliable solution for threat detection in the real-world EV and UAV charging infrastructure.

The recall metric measures the model's effectiveness in identifying all relevant instances related to the IDS in EV and UAV charging environments. Figure 8(c) presents the comparative assessment of recall. The existing models, including RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID, obtained an average recall rate of 97.30%, 95.97%, 94.89%, 92.45%, 95.12%, 94.45%, 97.19%, 96.70%, 95.35% and 93.44%, respectively. On the other hand, the developed methodology obtained an improved recall rate of 99.32%. This improvement in the recall manifests the model's efficiency and reliability in identifying all relevant instances associated with intrusion detection in the EV and UAV charging infrastructure. Moreover, this greater recall rate ensures that the proposed model identifies the maximum number of attack cases correctly, reducing the risk of potential security threats in the EV and UAV charging infrastructure.

Simultaneously, the f-measure performance was evaluated and compared with the existing methodologies to validate how the developed algorithm balances the prediction of positive and negative instances. Figure 8(d) depicts the comparison of f-measure. These existing algorithms attained f-measure of 97.12%, 95.88%, 94.92%, 91.80%, 95.17%, 94.27%, 97.26%, 96.55%, 95.16% and 93.48%, respectively, while the proposed algorithms earned higher f-measure of 99.11%. This increased f-measure demonstrates the proposed model's efficiency in balancing the prediction and classification of both normal and malicious instances. Also, the increased f-measure manifests that the proposed strategy reduces the false positives and negatives, enabling secure charging infrastructure for EV and UAV users.

The intrusion detection overhead measures the time the proposed strategy takes to respond to normal and malicious traffic. Figure 9(a) depicts the comparison of intrusion detection overhead. The existing techniques,

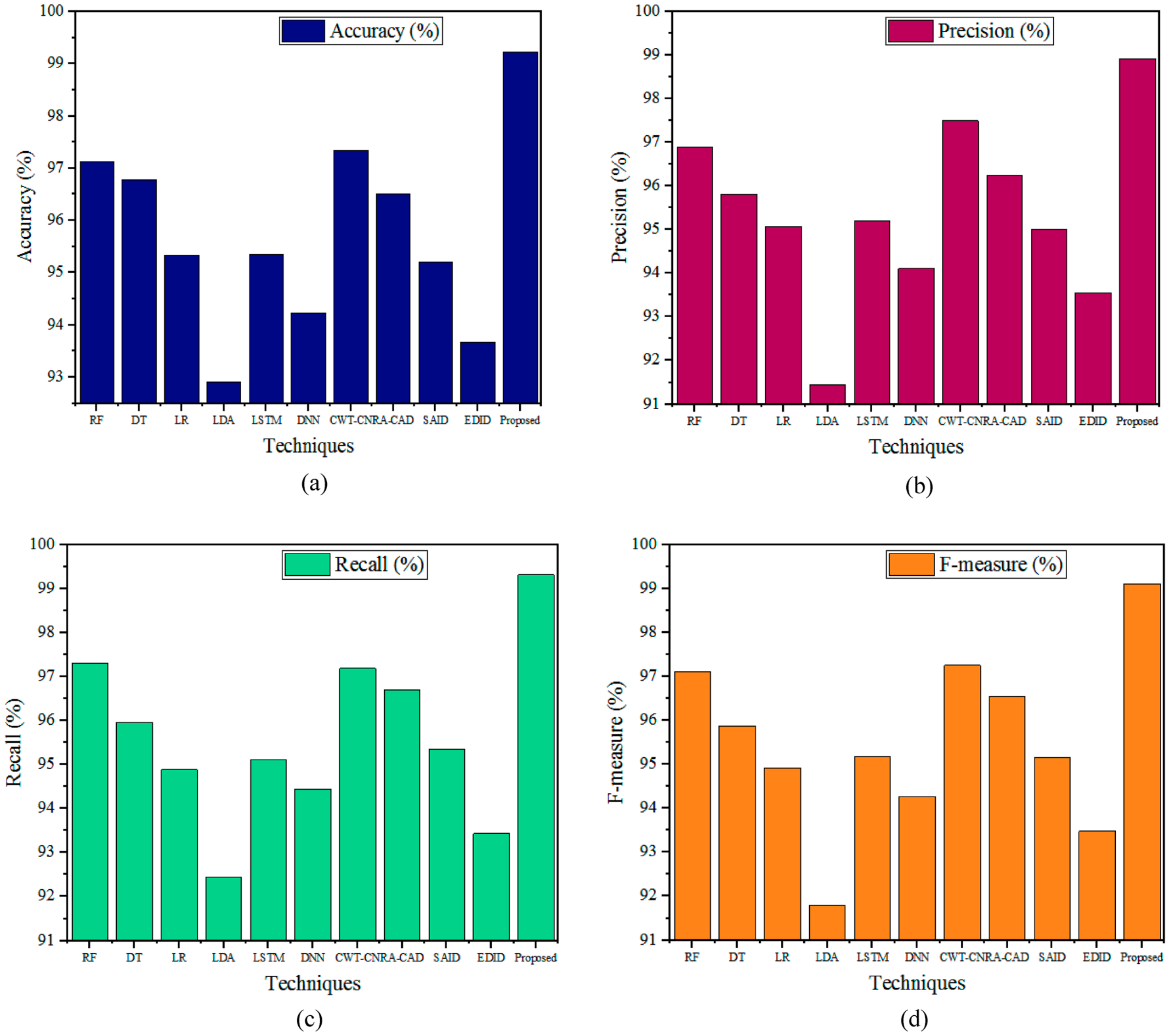


Figure 8. Comparison of intrusion detection performances: (a) accuracy, (b) precision, (c) recall and (d) f-measure.

including RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID, obtained an average detection overhead of 1.2s, 2.5s, 1.9s, 2.1s, 3.4s, 2.9s, 1.6s, 2.2s, 1.3s and 1.9s, respectively. However, the proposed algorithm achieved a minimum detection overhead of 0.5s, highlighting the model's efficiency in quickly responding to the intrusion in the charging infrastructure.

Cost efficiency determines how effectively the proposed strategy reduces the cost of charging and is measured in percentages. Figure 9(b) presents the comparison of cost efficiency. The existing models like RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID earned cost efficiency of 95.82%, 92.70%, 89.56%, 90.43%, 93.68%, 95.75%, 96.83%, 95.29%, 94.91% and 92.80%. The proposed algorithm obtained a cost efficiency of 98.56%, demonstrating that the proposed strategy delivers high-quality charging services at a lower cost than existing methods. This also ensures that the squirrel search algorithm optimizes resource allocation, ensuring that energy and charging stations are used more effectively, which helps reduce costs.

Consequently, the data confidential rate was determined to assess the security level provided by the proposed technique in the EV and UAV charging environments. This metric determines how effectively the proposed algorithm protects the user information from unauthorized access or attackers. These methodologies achieved a data confidential rate of 97.11%, 96.54%, 95.53%, 91.98%, 95.67%, 94.32%, 97.24%, 96.00%, 95.43% and 93.47%, respectively. However, the developed algorithm achieved an improved data confidential rate of 98.56%, which illustrates its efficiency in ensuring the security and privacy of user information in the charging environments.

This framework improves data protection and enhances the environment's privacy by accurately detecting and mitigating cyber threats. Figure 9(c) presents the comparison of cost efficiency.

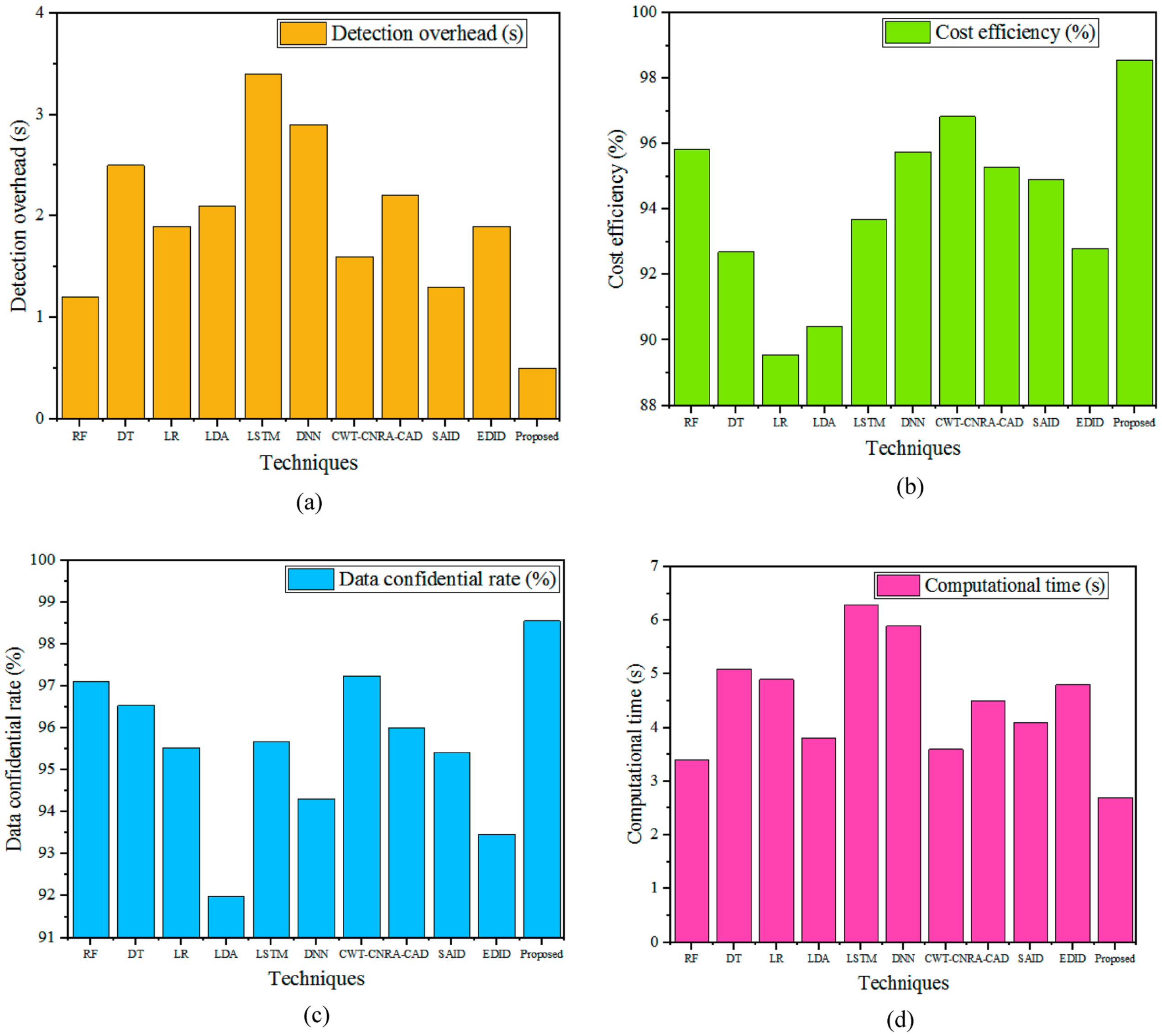


Figure 9. Comparison assessment: (a) intrusion detection overhead, (b) cost efficiency, (c) data confidential rate and (d) computational time.

Finally, the computational time was measured for all the techniques, and the validation of computational time is presented in Figure 9(d). This metric measures the time the techniques consume for all tasks, from data pre-processing to cost optimization. The existing models earned computational time of 3.4s, 5.1s, 4.9s, 3.8s, 6.3s, 5.9s, 3.6s, 4.5s, 4.1s and 4.8s, respectively, while the proposed technique earned computational time of 2.7s. The lower computational time earned by the developed method illustrates that it performs the above-stated tasks quickly. Reducing computational time emphasizes that the developed methodology processes the data quickly, illustrating its responsiveness in real-world applications. In addition, it demonstrates that the designed strategy identifies the attacks quickly, thereby reducing the adverse influence of malicious data in the charging infrastructure. Table 4 tabulates the overall comparative analysis. From the comprehensive comparative assessment, it is evident that the proposed strategy achieved superior performances in terms of accuracy, precision, recall, f-measure and data confidential rate.

Furthermore, to assess the efficiency of the proposed strategy, the model's performances are tested by launching different attacks like ransomware, Spoofing attacks, Denial of Service (DoS) attacks and distributed denial of service attacks (DDoS) in the EV charging ecosystem through data packets. Then the performance of the system was determined under these attack cases. Figure 10 and Table 5 depict the performances of the developed methodology under different attack cases. From the analysis, the proposed strategy accurately identifies and classifies above attacks with greater accuracy. These results substantiate the role of this proposed system as a solution to the case studies discussed in Section 1.1.

These improved performances manifest that the developed SS-ADRNN strategy accurately detects and classifies the intrusion in the EV and UAV charging infrastructure compared to other models. Also the

Table 4. Comparative analysis of the proposed model's performances with existing works.

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)	Computational time (s)	Detection overhead (s)	Cost efficiency (%)	Data confidential rate (%)
RF	97.12	96.89	97.30	97.12	3.4	1.2	95.82	97.11
DT	96.78	95.81	95.97	95.88	5.1	2.5	92.70	96.54
LR	95.34	95.07	94.89	94.92	4.9	1.9	89.56	95.53
LDA	92.9	91.45	92.45	91.80	3.8	2.1	90.43	91.98
LSTM	95.35	95.2	95.12	95.17	6.3	3.4	93.68	95.67
DNN	94.23	94.11	94.45	94.27	5.9	2.9	95.75	94.32
CWT-CN	97.34	97.5	97.19	97.26	3.6	1.6	96.83	97.24
RA-CAD	96.5	96.25	96.70	96.55	4.5	2.2	95.29	96.00
SAID	95.2	95.0	95.35	95.16	4.1	1.3	94.91	95.43
EDID	93.67	93.56	93.44	93.48	4.8	1.9	92.80	93.47
Proposed (SS-ADRNN)	**99.23**	**98.92**	**99.32**	**99.11**	**2.7**	**0.5**	**98.56**	98.56

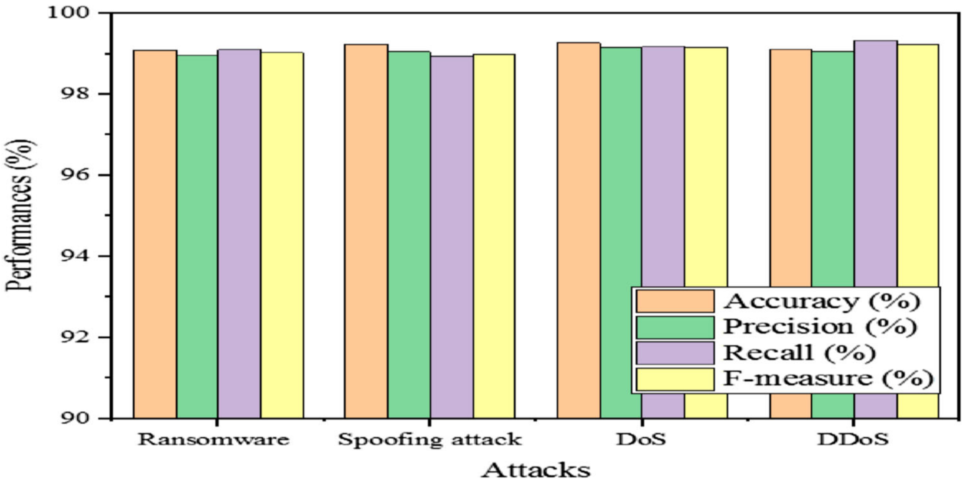


Figure 10. SS-ADRNN performance under different attack cases.

Table 5. Performances of the proposed strategy across different attack cases.

Attacks	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
Ransomeware	99.09	98.96	99.10	99.03
Spoofing attack	99.23	99.05	98.94	98.99
DoS	99.27	99.15	99.17	99.16
DDoS	99.11	99.06	99.32	99.32

improved cost efficiency manifests the model's efficiency in reducing the charging cost of the vehicles compared to the existing methods. On the other hand, the metrics like computational time, and intrusion detection overhead are reduced in the developed algorithm, which demonstrates its effectiveness and robustness in minimizing the time consumption in detecting, and classifying the attacks. This extensive assessment with the currently existing methodologies highlights that the proposed strategy is highly reliable in intrusion detection and cost optimization than others.

5.4. Discussion

In this study, we developed an innovative algorithm for securing the charging station from the malicious activities. The developed study was implemented in Python for publicly available EV and UAV network communication databases. The implementation outcomes manifest that the developed strategy obtained 99.23% accuracy, 98.92% precision, 99.32% recall and 99.11% f-measure in predicting malicious data. In addition, the developed algorithm obtained improved data confidential rate and cost efficiency of 98.56% and 98.56%, respectively.

The proposed work consumed a very low processing time and intrusion detection overhead of 2.7 s and 0.5 s, highlighting its responsiveness in real-world threat detection. Furthermore, we performed a comparative analysis with the existing models to validate the effectiveness of the proposed algorithm.

The comparison with current models like RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID demonstrates the superiority of the proposed technique in intrusion detection and cost minimization in charging infrastructure. It also demonstrates that parameters like accuracy, recall, f-measure, precision, data confidential rate, and cost efficiency are enhanced in the proposed strategy by 1.89%, 2.03%, 2.02%, 1.85%, 1.32% and 1.73% respectively, demonstrating its effectiveness over the current approaches. These greater performances incurred by the proposed algorithm make it more effective and robust for detecting the security threats in charging stations, thereby offering a reliable solution for securing the EV and UAV charging stations. Also, it highlights the model's capacity in reducing the charging cost and computational overhead. These superior performances achieved by the proposed algorithm illustrate its ability in detecting intrusions and minimizing charging cost in the charging infrastructure.

Nevertheless, the following shortcomings of the proposed system are to be explored:

- The physical EVCS as well as UAV charging infrastructure has not been installed due to the high cost of implementation. Hence the training and testing algorithms were carried out in offline manner. To make a thorough understanding of the working of the algorithm, it is crucial to analyse the working in real-time traffic.
- The proposed system is implemented solely taking CICEV2023 dataset, but for an intrinsic evaluation comparison can be made across diverse and larger datasets.

6. Conclusion and future scope

This study proposed a distinct strategy named SS-ADRNN for predicting the malicious activities in the EV and UAV charging infrastructure. The primary concern of the developed strategy is to predict the attacks and optimize the charging cost in the EV and UAV charging stations. The proposed mechanism combines the benefits of the SSA and ADRNN for attack prediction and cost optimization. The developed study was validated with the publicly available EV and UAV datasets. The implementation results manifest that the proposed framework earned 99.23% accuracy in predicting the malicious data entry. Also this approach consumed minimum computational time of 2.7 s for performing attack prediction and cost optimization. Furthermore, we made a comparative study with conventional algorithms such as RF, DT, LR, LDA, LSTM, DNN, CWT-CN, RA-CAD, SAID and EDID to validate the effectiveness of the developed framework. The comparative assessment shows that accuracy, precision, recall, f-measure, data confidential rate and cost efficiency performances are enhanced by 1.89%, 2.03%, 2.02%, 1.85%, 1.32% and 1.73% respectively.

The proposed system can be used to safeguard any critical Industrial Control System such as SCADA by the identification of the malicious traffic in prior to the attack. Although the proposed SS-ADRNN approach obtained impressive outcomes in predicting the malicious activities and optimizing charging costs in the EV and UAV charging infrastructure, it has certain limitations. First, the efficiency of the developed strategy depends on the dataset used, illustrating that the system's generalization is limited to dataset-specific characteristics. Second, the developed methodology is not tested on larger and diverse databases, which lacks the system's scalability and robustness across real-time scenarios. Hence, to resolve these issues, the future study should focus on exploring different dimensions related to the EV and UAV charging infrastructure by integrating continuous learning algorithms. Future studies should explore different dimensions, including dynamic resource allocation and demand-response strategies related to the EV and UAV charging infrastructure, by integrating continuous learning and multi-objective optimization algorithms.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

ORCID

Rosebell Paul http://orcid.org/0000-0001-8914-2432

References

[1] Obrador Rey S, Canals Casals L, Gevorkov L, et al. Critical review on the sustainability of electric vehicles: addressing challenges without interfering in market trends. Electronics. 2024;13:860. doi:10.3390/electronics13050860

[2] Teimoori, Z., Yassine, A. and Hossain, M.S., 2024. Smart vehicles recommendation system for artificial intelligence-enabled communication. IEEE Trans Consum Electron.

[3] Bharat M, Dash R, Jyotheeswara Reddy K, et al. Secure and efficient prediction of electric vehicle charging demand using α2-LSTM and AES-128 cryptography. Energy and AI. 2024;16:100307. doi:10.1016/j.egyai.2023.100307

[4] Kunovjanek M, Wankmüller C. Containing the COVID-19 pandemic with drones – feasibility of a drone enabled back-up transport system. Transport Policy. 2021;106:141–152. doi:10.1016/j.tranpol.2021.03.015

[5] Mastoi MS, Zhuang S, Munir HM, et al. An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends. Energy Reports. 2022;8:11504–11529. doi:10.1016/j.egyr.2022.09.011

[6] Tarafdar-Hagh M, Taghizad-Tavana K, Ghanbari-Ghalehjoughi M, et al. Optimizing electric vehicle operations for a smart environment: a comprehensive review. Energies. 2023;16:4302. doi:10.3390/en16114302

[7] Acharya S, Dvorkin Y, Pandžić H, et al. Cybersecurity of smart electric vehicle charging: a power grid perspective. IEEE Access. 2020;8:214434–214453. doi:10.1109/ACCESS.2020.3041074

[8] Johnson J, Berg T, Anderson B, et al. Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. Energies. 2022;15:3931. doi:10.3390/en15113931

[9] Hamdare S, Kaiwartya O, Aljaidi M, et al. Cybersecurity risk analysis of electric vehicles charging stations. Sensors. 2023;23:6716. doi:10.3390/s23156716

[10] Bazazi U, Ravadanegh SN. Evaluation of cyberattacks in distribution network with electric vehicle charging

infrastructure. In: Vahidinasab V., Mohammadi-Ivatloo B., editors. Electric vehicle integration via smart charging: technology, standards, implementation, and applications. Cham: Springer International Publishing; 2022, 111–128.

[11] Girdhar M, Hong J, You Y, et al. Cyber-attack event analysis for EV charging stations. 2023 IEEE Power & Energy Society General Meeting (PESGM). 2023, IEEE.

[12] Lambert F. “Hacked electric car charging stations in Russia display ‘Putin is a d∗ckhead’ and ‘glory to Ukraine’”, Feb 28 2022. https://electrek.co/2022/02/28/hacked-electric-car-charging-stations-russia-displays-putin-dckhead-glory-to-ukraine/.

[13] Datir H, Jawandhiya P. Random forest based hybrid model for intrusion detection system. Int J Recent Technol Eng. 2019;8:5054–5058. doi:10.35940/ijrte.D8274.118419

[14] Lee S-W, Mohammed sidqi H, Mohammadi M, et al. Towards secure intrusion detection systems using deep learning techniques: comprehensive analysis and review. J Netw Comput Appl. 2021;187:103111. doi:10.1016/j.jnca.2021.103111

[15] EV Update Media. EV charging stations susceptible to cyber-attacks and cyber security incidents. March 19, 2023. https://evupdatemedia.com/ev-charging-stations-susceptible-to-cyber-attacks-and-cyber-security-incidents/.

[16] Kovacs E. EV charging management system vulnerabilities allow disruption, energy theft. February 2, 2023. https://www.securityweek.com/ev-charging-management-system-vulnerabilities-allow-disruption-energy-theft/.

[17] Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur. 2021;4:18. doi:10.1186/s42400-021-00077-7

[18] Abu Al-Haija Q, Al-Fayoumi M. An intelligent identification and classification system for malicious uniform resource locators (URLs). Neural Comput Appl. 2023;35:16995–17011. doi:10.1007/s00521-023-08592-z

[19] Al-Haija QA, Badawi AA. URL-based phishing websites detection via machine learning. 2021 International Conference on Data Analytics for Business and Industry (ICDABI); 2021; Sakheer, Bahrain, p. 644–649, doi:10.1109/ICDABI53623.2021.9655851

[20] Elqasass A, Aljundi I, Al-Fayoumi M, et al. Facilitating secure web browsing by utilizing supervised filtration of malicious URLs. In: Joby PP, Alencar MS, Falkowski-Gilski P, editors. Iot based control networks and intelligent systems. ICICNIS 2023. Lecture notes in networks and systems. Singapore: Springer, 2024. p. 459–468, doi:10.1007/978-981-99-6586-1_31

[21] Odeh A, Abu Al-Haija Q, Aref A, et al. Comparative study of CatBoost, XGBoost, and LightGBM for enhanced URL phishing detection: a performance assessment. J Internet Services Inf Sec. 2023;13:1–11. doi:10.58346/JISIS.2023.I4.001

[22] Ali M, Haque M, Durad MH, et al. Effective network intrusion detection using stacking-based ensemble approach. Int J Inf Secur 2023;22:1781–1798. doi:10.1007/s10207-023-00718-7

[23] S. Seng, Joaquin Garcia-alfaro, Y. Laarouci. Implementation of a stateful network protocol intrusion detection systems. SECRYPT 2022: 19th International Conference on Security and Cryptography, Jul 2022, Lisbon, Portugal. p. 398–405.

[24] Basnet M, Ali MH. Deep learning-based intrusion detection system for electric vehicle charging station. 2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES); 2020. IEEE.

[25] Basnet M, Poudyal S, Hasan Ali M, et al. Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America); 2021. IEEE.

[26] Basnet M, Ali MH. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. IET Gener Transm Distrib. 2021;15:3435–3449. doi:10.1049/gtd2.12275

[27] ElKashlan M, Elsayed MS, Jurcut AD, et al. A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). Electronics. 2023;12:1044. doi:10.3390/electronics12041044

[28] ElKashlan M, Aslan H, Said Elsayed M, et al. Intrusion detection for electric vehicle charging systems (evcs). Algorithms. 2023;16(2):75. doi:10.3390/a16020075

[29] Basnet M, Ali MH. Deep reinforcement learning-driven mitigation of adverse effects of cyber-attacks on electric vehicle charging station. Energies. 2023;16(21):7296. doi:10.3390/en16217296

[30] Basnet M, Ali MH. WCGAN-based cyber-attacks detection system in the EV charging infrastructure. 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES); 2022. IEEE.

[31] Warraich ZS, Morsi WG. Early detection of cyber–physi cal attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. Sustain Energy Grids Networks. 2023;34:101027. doi:10.1016/j.segan.2023.101027

[32] Dalal S, Manoharan P, Lilhore UK, et al. Extremely boosted neural network for more accurate multi-stage cyber attack prediction in cloud computing environment. J Cloud Comput. 2023;12(1):14. doi:10.1186/s13677-022-00356-9

[33] Bhandari G, Lyth A, Shalaginov A, et al. Distributed deep neural-network-based middleware for cyber-attacks detection in smart IoT ecosystem: a novel framework and performance evaluation approach. Electronics. 2023;12(2):298. doi:10.3390/electronics12020298

[34] Paul, Rosebell, and Mercy Paul Selvan. A study on naming and caching in named data networking. 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2021.

[35] Li P, Ou W, Liang H, et al. A zero trust and blockchain-based defense model for smart electric vehicle chargers. J Netw Comput Appl. 2023;213:103599. doi:10.1016/j.jnca.2023.103599

[36] Thomas P, Shanmugam PK. A review on mathematical models of electric vehicle for energy management and grid integration studies. J Energy Storage. 2022;55(Part A):105468. doi:10.1016/j.est.2022.105468

[37] Torky M, El-Dosuky M, Goda E, et al. Scheduling and securing drone charging system using particle swarm optimization and blockchain technology. Drones. 2022;6:237. doi:10.3390/drones609023

[38] Adetunji K, Hofsajer I, Abu-Mahfouz A, et al. A review of metaheuristic techniques for optimal integration of electrical units in distribution networks. IEEE Access. 2020;9:1–1. doi:10.1109/ACCESS.2020.3048438

[39] Lazari V, Chassiakos A. Multi-objective optimization of electric vehicle charging station deployment using genetic algorithms. Appl Sci 2023;13:4867. doi:10.3390/app13084867

[40] Jain M, Singh V, Rani A. A novel nature-inspired algorithm for optimization: squirrel search algorithm. Swarm Evol Comput. 2019;44:148–175. doi:10.1016/j.swevo.2018.02.013

[41] Thangaraj T, Sridevi S, Chelliah CD, et al. Performance analysis of machine learning algorithms in intrusion detection system: a review. Procedia Comput Sci. 2020;171:1251–1260. doi:10.1016/j.procs.2020.04.133

[42] Nassar AA, Morsi WG. Early detection of cyber-physical attacks on electric vehicles fast charging stations using wavelets and deep learning. IEEE Trans Ind Cyber-Phys Syst. 2024;2:220–231.

[43] Mavikumbure HS, Cobilean V, Wickramasinghe CS, et al. Cy-Phy ADS: cyber-physical anomaly detection framework for EV charging systems. IEEE Trans Transp Electrification. 2024:1–1.

[44] Fotohi R, Abdan M, Ghasemi S. A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks. J Grid Comput. 2022;20(3):22. doi:10.1007/s10723-022-09614-1

[45] Tlili F, Ayed S, Fourati LC. Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). Comput Secur. 2024;142:103878. doi:10.1016/j.cose.2024.103878

[46] Ngueajio MK, Washington G, Rawat DB, et al. Intrusion detection systems using support vector machines on the KDDCUP'99 and NSL-KDD datasets: A comprehensive survey. In: Arai K, editor. Intelligent systems and applications. IntelliSys 2022. lecture notes in networks and systems. Cham: Springer; 2023. vol 543. doi:10.1007/978-3-031-16078-3_42