mathematics

MDPI

Article

Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models

Dusmurod Kilichev, Dilmurod Turimov and Wooseong Kim *

Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea; dusmurod@gachon.ac.kr (D.K.); dilmurod@gachon.ac.kr (D.T.)
* Correspondence: wooseong@gachon.ac.kr

Abstract: In the evolving landscape of Internet of Things (IoT) and Industrial IoT (IIoT) security, novel and efficient intrusion detection systems (IDSs) are paramount. In this article, we present a groundbreaking approach to intrusion detection for IoT-based electric vehicle charging stations (EVCS), integrating the robust capabilities of convolutional neural network (CNN), long short-term memory (LSTM), and gated recurrent unit (GRU) models. The proposed framework leverages a comprehensive real-world cybersecurity dataset, specifically tailored for IoT and IIoT applications, to address the intricate challenges faced by IoT-based EVCS. We conducted extensive testing in both binary and multiclass scenarios. The results are remarkable, demonstrating a perfect 100% accuracy in binary classification, an impressive 97.44% accuracy in six-class classification, and 96.90% accuracy in fifteen-class classification, setting new benchmarks in the field. These achievements underscore the efficacy of the CNN-LSTM-GRU ensemble architecture in creating a resilient and adaptive IDS for IoT infrastructures. The ensemble algorithm, accessible via GitHub, represents a significant stride in fortifying IoT-based EVCS against a diverse array of cybersecurity threats.

Keywords: convolutional neural network; cybersecurity; deep learning; Edge-IIoTset; electric vehicle charging station; ensemble learning; gated recurrent unit; Internet of Things; intrusion detection system; long short-term memory

MSC: 68T07

Citation: Kilichev, D.; Turimov, D.; Kim, W. Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. *Mathematics* **2024**, *12*, 571. https://doi.org/10.3390/math12040571

Academic Editor: Matjaz Perc

Received: 6 January 2024
Revised: 9 February 2024
Accepted: 12 February 2024
Published: 14 February 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

As we navigate the rapidly evolving terrain of the Internet of Things (IoT) and Industrial IoT (IIoT), the role of robust intrusion detection systems (IDS) in safeguarding electric vehicle charging stations (EVCSs) becomes increasingly critical [1]. The dynamic and multifaceted nature of IoT environments demands innovative solutions that transcend traditional cybersecurity approaches.

The integration of IoT technologies into essential services, such as EVCS, poses significant cybersecurity risks. Traditional IDS, struggling to keep pace with the evolving sophistication of cyber threats and unique constraints of IoT environments, establish the need for our research. Our study is anchored on enhancing intrusion detection in IoT-based EVCS, leveraging advanced neural network architectures to address the intricate challenges inherent in these systems.

Existing IDS solutions face numerous challenges, such as scalability, adaptability, resource constraints, diverse attack vectors, and the necessity for real-time detection [2]. These challenges are exacerbated by high false alarm rates, rendering many systems unreliable. In this study, we propose a novel IDS framework tailored for IoT environments in EVCS to address these critical issues.

Our objectives are centered on developing an ensemble IDS model using convolutional neural network (CNN) [3], long short-term memory (LSTM), and gated recurrent unit

(GRU) models, evaluating its performance with the "Edge-IIoTset" dataset [4], optimizing it for resource efficiency, and benchmarking it against existing solutions. We evaluate the ensemble model's efficacy in enhancing detection accuracy, its performance using comprehensive datasets, its feasibility in resource-constrained environments, and its adaptability to evolving cyber threats.

The major contributions of this study are as follows.

1. Innovative Ensemble Architecture: We introduce a cutting-edge model merging CNNs, LSTMs, and GRUs, harnessing their combined strengths for nuanced intrusion detection.
2. Use of Real-World Datasets: Our approach is validated using authentic datasets, ensuring practical applicability in IoT EVCS environments.
3. Advanced Data Processing Techniques: Sophisticated preprocessing techniques are employed to manage complex IoT security data, enhancing model learning efficiency.
4. Comprehensive Performance Analysis: Our model outperforms existing IDS solutions in accuracy and resilience, proven through extensive testing.
5. Practical Implications and Scalability: Designed for real-world IoT applications, our model's scalability and adaptability offer significant cybersecurity advancements.
6. Benchmark for Future Research: Setting a new standard in IoT security, our work paves the way for future innovations in ensemble and hybrid model applications.

In this article, we present a groundbreaking approach to intrusion detection tailored to the unique challenges of IoT-based EVCS. Through significant advancements in IoT cybersecurity, we demonstrate the effectiveness and viability of an ensemble model in this vital domain.

In the remainder of this article, we comprehensively explore network IDS (NIDS) in the context of IoT-based EVCS. Section 2 presents the nuances of IoT in EVCS, covering the challenges, cybersecurity threats specific to IoT-based EVCS, and the critical role of NIDS in safeguarding them. It also highlights recent technological and scientific advancements, setting the stage for future research directions. Section 3 presents a review of related studies, providing a scholarly context for our research. In Section 4, we introduce our proposed NIDS framework for IoT-based EVCS, detailing its architectural overview, the integration of CNN, LSTM, and GRU models, data preprocessing techniques, evaluation metrics, and implementation specifics. Section 5 presents our experimental results, including binary, six-class, and fifteen-class classification outcomes. Next, in Section 6, we discuss these results and interpret their implications. Finally, Section 7 concludes this study, summarizing our contributions and envisioning the impact of our work in the realm of IoT security.

2. Network Intrusion Detection in IoT-Based Vehicle Charging Stations

2.1. Introduction to IoT in Vehicle Charging Stations

The integration of IoT into EVCS marks a transformative step in the evolution of smart transportation infrastructure [5]. This fusion introduces a level of sophistication and efficiency previously unattainable in traditional EVCS. IoT technology in EVCS is not merely an extension of general IoT systems; it is a specialized adaptation designed to meet the unique demands of electric vehicle (EV) charging [6].

Figure 1 depicts a schematic of a sophisticated IoT-based EVCS network, demonstrating the interconnectedness and communication between different elements, such as renewable energy sources, the power grid, IoT devices, and vehicles being charged. Each connection signifies the real-time data exchange essential for the efficient and secure operation of EVCS, which underscores the unique complexities of IoT integration in this domain compared with general IoT systems.

The key characteristics of IoT in EVCS include enhanced communication capabilities, allowing for real-time data transmission between charging stations, EVs, and network management systems. This communication is pivotal for optimizing charging schedules, managing power loads, and ensuring efficient energy distribution. This technology enables features such as dynamic pricing, user authentication, and remote monitoring, which are integral to modern EVCS [1].

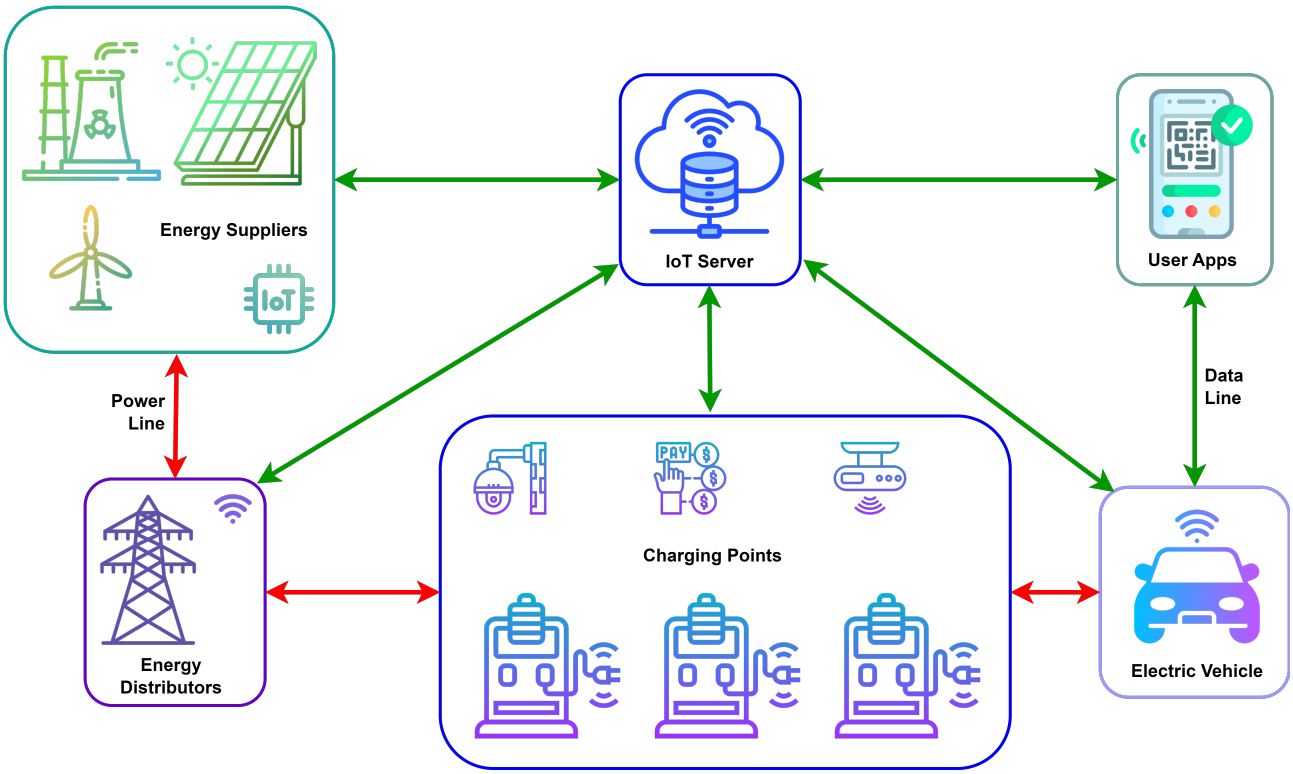

Figure 1. IoT Network Architecture for EVCS.

The roles and functionalities of IoT in EVCS extend beyond the conventional scope of general IoT systems. One of the primary differentiators is the real-time monitoring of charging processes. Unlike typical IoT applications that may tolerate delays in data transmission, IoT systems in EVCS require instantaneous data flow to ensure efficient and safe charging. This real-time capability is crucial for adjusting charging rates, monitoring battery health, and providing immediate feedback to both the user and system operator.

Another unique aspect is the integration of IoT-based EVCS into the smart grid [7]. This integration not only involves managing the energy supply to EVs but also encompasses sophisticated grid balancing. EVCS, through IoT connectivity, can act as active grid participants, aiding in demand response strategies and contributing to overall grid stability. This level of integration differs from most IoT applications, which are typically more isolated in their operations.

In addition, the remote management capabilities of IoT-based EVCS are far more advanced than those of typical IoT systems. They must accommodate a wide range of functionalities, from user authentication and payment processing to firmware updates and predictive maintenance. This level of management is critical for maintaining the security and efficiency of the charging infrastructure.

In terms of cybersecurity, IoT in EVCS presents unique challenges. The stations not only process sensitive user data but are also integral components of critical energy infrastructure. This dual role places them at a higher risk of targeted cyberattacks, necessitating more robust and specialized IDS compared with general IoT setups. The potential repercussions of a security breach in these systems are significant, ranging from personal data theft to disruptions in the energy grid, underscoring the need for advanced security measures.

2.2. Network Intrusion Detection Systems (NIDS)

NIDS are integral components in safeguarding network infrastructures, particularly in the burgeoning landscape of IoT. NIDS are designed to monitor network traffic for suspicious activities or policy violations [8]. The primary objective of NIDS in IoT ecosystems is to ensure the security and integrity of data transmission across various connected devices

and platforms. This includes the detection of unauthorized access attempts, malware propagation, and other forms of cyber threats that can compromise the functionality and safety of IoT networks [9].

NIDS operate by analyzing network traffic and identifying patterns or anomalies that signify potential security breaches. They serve as a critical line of defense against cyberattacks, mitigating the risks that come with the increased connectivity and data exchange inherent in IoT systems [10]. The deployment of NIDS in IoT environments is pivotal in maintaining not only the security but also the reliability and performance of networks [11].

Although NIDS play a fundamental role in general IoT environments, their application in the specific context of EVCS entails additional complexities and requirements. A notable differentiation is the need to handle specialized protocols unique to EVCS, such as the Open Charge Point Protocol (OCPP). OCPP is the communication standard used for communication between EVCS and central management systems. NIDS in EVCS must be equipped to monitor and analyze the traffic that adheres to this protocol, ensuring secure and efficient communication between charging points and network operators [12].

Another critical aspect is the handling of real-time data streams. EVCS, being part of a broader smart grid system, require immediate processing and response to data [7]. This necessity for real-time data handling is far more stringent than those in typical IoT applications, where delays might be permissible. NIDS in EVCS must be capable of processing high volumes of real-time data without causing significant latency or disruption in the charging process. This requirement is crucial for maintaining the operational efficiency and safety of the EVCS.

Moreover, the cybersecurity stakes in EVCS are considerably high due to their direct impact on critical energy infrastructure and personal user data. Therefore, NIDS employed in this context must be more sophisticated and capable of identifying and responding to a broad range of threats with high accuracy and efficiency. This includes advanced persistent threats and sophisticated cyberattacks that specifically target energy infrastructure and personal data.

2.3. Challenges in IoT-Based EVCS

IoT-based EVCS present a set of unique challenges that set them apart from conventional IoT systems. First, the imperative for uninterrupted service delivery is paramount. EVCS are critical components of the transportation infrastructure [5], and any disruption in their service can have immediate and tangible impacts on users. This requirement for continuous operability demands a highly reliable and resilient IoT framework capable of maintaining functionality under various conditions, such as high user demand, network congestion, and potential cyberattacks.

Second, the safety implications involved in the operation of IoT-based EVCS are of a high-stakes nature. Unlike many other IoT applications, a failure in IoT-based EVCS can pose direct risks to physical safety. This is due to the high power levels handled by these systems and the potential hazards associated with EV charging, such as electrical fires or equipment malfunctions. Consequently, the IoT systems embedded within EVCS must not only be secure from cyber threats but also robust against physical and technical failures.

Further, the integration of EVCS with broader smart grid infrastructures introduces additional layers of complexity [13]. These stations often serve as active nodes within the smart grid, participating in demand response and energy management strategies. This dual role as both energy consumers and potential energy storage or redistribution points necessitates sophisticated communication and coordination capabilities within the IoT framework. Managing this dynamic interaction between EVCS and smart grid poses significant technical risks, requiring advanced data analytics and real-time decision-making capabilities [7].

The enhanced complexity of IoT-based EVCS can be understood through the convergence of three key domains: energy systems, information technology (IT), and operational

technology (OT). This convergence represents a paradigm shift in how energy services are delivered and managed, moving away from traditional, siloed approaches toward more integrated and interconnected frameworks.

From an energy systems perspective, EVCS are not just end-user facilities but are increasingly becoming integral components of the distributed energy landscape. They interact with various elements of the energy grid, from renewable energy sources to energy storage systems, necessitating sophisticated mechanisms for energy flow management and optimization.

On the IT front, the data-centric nature of EVCS demands robust data processing and cybersecurity measures. The stations generate and process vast amounts of data, ranging from user information to operational parameters. Ensuring the security, privacy, and integrity of these data is critical, especially given the potential for targeted cyberattacks in these high-value infrastructures.

OT, which refers to the hardware and software that monitors and controls physical devices, plays a vital role in ensuring the real-time performance and safety of EVCS. The integration of OT with IT systems in the IoT framework leads to a complex interplay between digital and physical domains. This integration is challenging because it requires seamless interoperability and synchronization between systems that were traditionally separate.

The convergence of these three domains in IoT-based EVCS results in a multifaceted ecosystem. Managing this ecosystem requires not only advanced technological solutions but also a holistic understanding of the interactions between energy systems, IT, and OT. This complexity is further amplified by the need to adhere to regulatory standards and adapt to evolving technologies and user demands. As a result, developing and maintaining IoT systems in this context requires a multidisciplinary approach that encompasses aspects of cybersecurity, electrical engineering, data science, and systems integration.

2.4. Cybersecurity Threats Specific to EVCS

The cybersecurity landscape of IoT-based EVCS is fraught with unique threats, distinct from general IoT vulnerabilities. A primary concern is tampering with charging processes. Attackers can manipulate the charging operation, potentially leading to overcharging or undercharging of EV batteries. This not only damages the batteries but can also result in safety hazards, such as battery overheating. Further, such tampering can disrupt the overall service availability, causing inconvenience to users and eroding trust in EV infrastructure.

Interception of communications between EVs and EVCS is another significant threat. These communications often include sensitive data, such as user credentials, payment information, and vehicle specifications. Cybercriminals intercepting these data can engage in identity theft, financial fraud, or unauthorized access to EV controls. This interception not only compromises user privacy but also threatens the integrity of the entire charging network.

Attacks on the grid-interactive functionalities of EVCS present a more severe threat. These stations are increasingly being integrated into smart grid systems [7], playing a role in energy management strategies such as demand response. Cyberattackers targeting these functionalities can disrupt the energy distribution, potentially causing wider grid instabilities or blackouts. Such attacks can escalate from localized issues at individual EVCS to broader challenges affecting the energy grid at large.

2.5. Role of NIDS in IoT-Based EVCS

The deployment of NIDS in IoT-based EVCS is crucial, not just as a security measure but also as a means to ensure operational efficiency and reliability. The unique network topologies and traffic patterns inherent to these stations require the specialized adaptation of NIDS.

As aforementioned, one of the primary adaptations involves the handling of proprietary protocols, such as OCPP, which is widely used for communication between EVCS and central management systems. In this context, NIDS must be proficient in monitoring and

analyzing traffic adhering to these protocols to effectively detect any anomalies or malicious activities [12]. This proficiency is essential for preempting and mitigating threats that could compromise the communication integrity between EVCS and the central network.

In addition, EVCS deal with high-frequency transaction data, encompassing everything from user authentication and billing information to real-time energy consumption metrics. NIDS must be capable of processing this high-volume data stream without causing latency issues, ensuring that any malicious activities embedded within the data are promptly identified and addressed. This capability is crucial for maintaining the confidentiality, integrity, and availability of the data and services provided by EVCS.

2.6. Technological and Scientific Innovations

The landscape of NIDS is rapidly evolving, with recent technological advancements significantly enhancing their applicability to IoT-based EVCS. A key development in this domain is the integration of artificial intelligence (AI), particularly in anomaly detection. AI-driven anomaly detection systems are adept at handling large-scale and diverse data generated by charging networks. These systems employ machine learning (ML) algorithms to analyze patterns in network traffic, enabling them to identify irregularities that could indicate a cyber threat. This capability is especially beneficial in the context of EVCS, where traffic patterns can vary significantly and unpredictably.

Another noteworthy advancement is the use of deep learning (DL) techniques in NIDS. DL models, trained on vast datasets, can uncover subtle and complex patterns indicative of cyber threats. This approach is highly effective in detecting sophisticated attacks that might elude traditional detection methods. In the dynamic environment of EVCS, where attackers may employ advanced tactics, DL-enhanced NIDS provide an additional layer of security.

The development of real-time IDS is also significant. These systems are designed to process and analyze data in real-time, providing immediate responses to potential threats. This feature is crucial for EVCS, where delays in threat detection and response can have immediate and severe consequences.

Scientific research plays a vital role in advancing the capabilities of NIDS in addressing the unique challenges presented by EVCS networks. One area of focus is the optimization of NIDS for low-latency environments. Research in this field aims to develop algorithms and architectures that can quickly process large volumes of data without compromising the performance of EVCS networks. This is crucial for maintaining the operational efficiency of these stations while ensuring robust security.

Another research domain is the development of context-aware NIDS. These systems are designed to understand the specific context of an EVCS network, including typical patterns of usage and expected traffic flows. By having a contextual understanding, NIDS can more accurately identify anomalies, thereby reducing the likelihood of false positives and improving overall detection accuracy.

Studies on network segmentation and isolation strategies are also significant. By creating segmented networks within EVCS, researchers aim to limit the potential impact of a security breach. This approach ensures that an intrusion in one segment does not compromise the entire network, thus enhancing overall resilience.

Moreover, research is being conducted on the integration of NIDS with other cybersecurity tools, such as firewalls and intrusion prevention systems. This integrated approach allows for a more comprehensive defense strategy that combines the strengths of various tools to provide robust protection against various cyber threats.

In light of these advancements, it becomes imperative to address the symbiotic relationship between technological innovation and cybersecurity in the IoT-based EVCS ecosystem. As we harness the power of AI and DL to fortify NIDS, there emerges a parallel need to ensure these systems are not only resilient against evolving cyber threats but also adaptable to the technological evolution within EVCS infrastructure. Future-oriented research is thus oriented towards creating NIDS frameworks that are inherently flexible,

capable of integrating new algorithms and methodologies without extensive overhauls. This adaptability is crucial in maintaining the efficacy of NIDS amid rapid technological advancements, ensuring that cybersecurity measures evolve in tandem with the systems they protect.

2.7. Future Directions and Research Opportunities

The field of network intrusion detection, particularly in the context of IoT-based EVCS, is at the forefront of significant research and development. One emerging trend is the advancement of predictive IDS, which aim to not only detect ongoing threats but also predict potential vulnerabilities and attack vectors through advanced data analytics and AI algorithms. This proactive approach could significantly enhance the security posture of EVCS by anticipating and mitigating risks before they materialize.

Another area of intense research is the integration of blockchain technology for secure communication and data integrity within EVCS networks [14]. Blockchain's decentralized and tamper-resistant ledger could offer a novel technique to secure myriad transactions and data exchanges in these systems, from payment processing to energy consumption records [15].

Efforts are also being made to develop adaptive and self-learning NIDS. These systems would be capable of evolving their detection algorithms in real time, adapting to new threats as they emerge. This adaptability is crucial in an environment in which threat actors continuously refine their tactics.

Integrating renewable energy sources with EVCS presents both challenges and opportunities for network intrusion detection. On the one hand, the incorporation of renewable energy sources, such as solar or wind, adds complexity to the network, increasing the potential attack surface. This complexity arises from the need to manage and secure the bidirectional flow of energy and information between the EVCS and renewable energy sources.

On the other hand, this integration offers opportunities to develop advanced energy management systems that can intelligently balance charging demands with renewable energy availability. NIDS in this integrated environment would need to be sufficiently sophisticated to handle the variability and unpredictability of renewable energy sources while ensuring dynamic interaction security.

Another potential challenge lies in adapting to rapidly evolving technologies in EVs and charging infrastructure. As EVs become more advanced and incorporate features such as vehicle-to-grid capabilities, the role of NIDS will need to expand to cover these new functionalities. This expansion requires continuous research and development to ensure that NIDS can effectively secure these technologies against emerging threats.

Moreover, the standardization of communication protocols and security measures across different EV technologies and charging infrastructures remains a challenge [16]. Future research should focus on developing universal security standards and protocols that can be applied across various platforms and technologies, ensuring a cohesive and secure EV charging ecosystem.

3. Related Work

The exploration of cybersecurity in EVCS encompasses various facets, with research focusing on several key areas. First, comprehensive cybersecurity risk analyses [17], investigations into vulnerabilities induced by manufacturers [18], and post-cyber event investigation frameworks [19] collectively address the broad security challenges in EVCS. These studies delve into infrastructure and protocol vulnerabilities, underscore the need for enhanced security measures, and introduce sophisticated frameworks for post-event analysis.

Second, the application of ML techniques specifically for detecting distributed denial-of-service (DDoS) attacks in EVCS networks is another notable research area [20,21]. Existing research efforts focus on comparing various ML classifiers to identify the most effective methods for maintaining the stability and security of EVCS within smart city infrastructures.

Third, a substantial body of work focuses on the application of advanced ML techniques, such as deep neural network (DNN) and LSTM algorithms, to counteract cyber threats in EVCS [22–25]. This research spans the development of effective IDS, the challenges posed by the integration of EVCS with emerging technologies such as 5G, and the use of techniques such as WCGAN combined with DL classifiers for enhanced attack detection.

Finally, the realm of privacy preservation in EVCS has been addressed through research into adaptive, differentially private federated learning mechanisms [26]. This is crucial in optimizing privacy while maintaining data utility in federated learning environments, presenting solutions to balance privacy and model performance.

In contrast to earlier models that primarily focus on Distributed Denial of Service (DDoS) attacks using datasets like IoT-23, our model's ability to classify more complex and diverse attacks such as injection, scanning, malware, and Man-In-The-Middle (MITM) sets a new benchmark in the field. Additionally, the utilization of the Edge-IIoTset dataset, which captures real-world traffic, further validates the practical applicability of our model in real-time IoT environments, a distinct edge over the CIC-IDS2018 dataset used in some prior studies (Table 1).

Table 1. IDS in EVCS: A Comparative Table.

Authors	Year	Model	Dataset	IoT/IIoT Devices	Class	Attack
ElKashlan, M. et al. [20]	2023	Filtered Classifier, Decision Table	IoT-23	23 types, home	2 class	DDoS
ElKashlan, M. et al. [21]	2023	Naïve Bayes, J48, Attribute select, Filtered classifier	IoT-23	23 types, home	2 class, 5 class	DDoS, C&C, Botnet, Scan
Basnet, M. et al. [22]	2020	DNN, LSTM	CIC-IDS2018	simulated	2 class, 5 class	DoS
Basnet, M. et al. [23]	2021	Stacked/deep LSTM	own dataset	simulated	4 class	FDI, DDoS
Basnet, M. et al. [24]	2022	EC-WCGAN	CIC-IDS2018	simulated	2 class, 5 class	DoS
Our proposed method	2023	CNN-LSTM-GRU	Edge-IIoTset	+10 types, industry	2 class, 6 class, 15 class	DDoS, Injection, Scanning, Malware, MITM

Together, these research efforts represent a comprehensive approach to understanding and mitigating the cybersecurity risks associated with EVCS, reflecting the diverse and complex nature of security challenges in the critical infrastructure of smart cities.

4. Proposed NIDS Framework for IoT-Based EVCS

4.1. NIDS Framework Theory

In the realm of safeguarding IoT-based Electric Vehicle Charging Stations (EVCS) against cyber threats, our proposed Network Intrusion Detection System (NIDS) is anchored in a rich tapestry of theoretical principles that span statistical learning, optimization theory, and deep learning paradigms. This section elucidates the foundational theories that coalesce to form the backbone of our NIDS, illustrating its capacity to navigate the complex data ecosystems inherent in EVCS environments.

At its core, our NIDS is predicated on the principle of anomaly detection, a cornerstone of statistical learning theory. This principle posits that anomalies manifest as deviations from established data patterns, serving as harbingers of potential intrusions. The efficacy of anomaly detection in our context is underlined by its adaptability to the multifarious and dynamic nature of data flows within IoT-based EVCS, enabling the discernment of irregularities indicative of cybersecurity breaches.

The edifice of our approach is further strengthened by robust mathematical models that employ a synthesis of classification algorithms. Rooted in the rich soils of optimization theory and probabilistic frameworks, these models adeptly categorize network data into normative and anomalous classes based on learned behavioral patterns. This classification mechanism is instrumental in the NIDS's ability to sift through the voluminous data streams, pinpointing anomalies with precision and alacrity.

Underpinning our NIDS is an ensemble of sophisticated Deep Learning (DL) techniques, each selected for its unique theoretical properties and applicability to the task at hand.

Convolutional Neural Networks (CNNs): Theoretically celebrated for their prowess in feature extraction, CNNs employ convolutional layers to distill salient features from raw data. This capability is paramount in unraveling the complex, pattern-rich tapestry of network traffic, laying bare the subtle signatures of cyber threats.

Recurrent Neural Architectures (LSTMs and GRUs): Designed to surmount the challenges posed by the vanishing gradient phenomenon, these architectures excel in modeling temporal dependencies. Their theoretical capacity to retain information over extended sequences makes them invaluable for monitoring the continuous, temporally linked data streams characteristic of EVCS operations.

The strategic deployment of our NIDS within the IoT architecture is informed by the theoretical precepts of distributed computing and edge analytics. By embedding the NIDS at the edge, we leverage the theoretical benefits of proximal data processing—namely, the minimization of latency and the judicious conservation of bandwidth. This alignment with the resource-aware ethos of IoT ecosystems ensures that the NIDS operates with both efficiency and agility, embodying the ideal balance between security imperatives and operational constraints.

4.2. Architectural Overview

The proposed NIDS framework is an integration of advanced neural network architectures adept at learning and identifying complex patterns indicative of cyber threats. The proposed model harnesses the strengths of CNN, LSTM, and GRU algorithms to analyze network traffic data for intrusion detection. A detailed representation of this ensemble architecture is shown in Figure 2.

At the heart of our NIDS framework lies a DL model that operates in two critical dimensions: spatial feature extraction and temporal sequence processing. First, the CNN layers effectively capture spatial dependencies within individual data packets [27]. This process uses convolutional filters that slide across the input data to identify crucial features such as specific packet sizes or unusual protocol behavior that could signify an intrusion attempt.

Following the spatial analysis, the temporal characteristics of the data are deciphered by the LSTM and GRU layers. LSTMs are adept at recognizing long-term dependencies, preserving knowledge of events that occurred many steps back in the sequence, which is essential when attacks comprise a series of discreet but related actions [28]. GRUs complement this by focusing on more recent information, allowing the model to adapt rapidly to the most current data inputs and enhancing its ability to detect anomalies in real-time traffic flow [29].

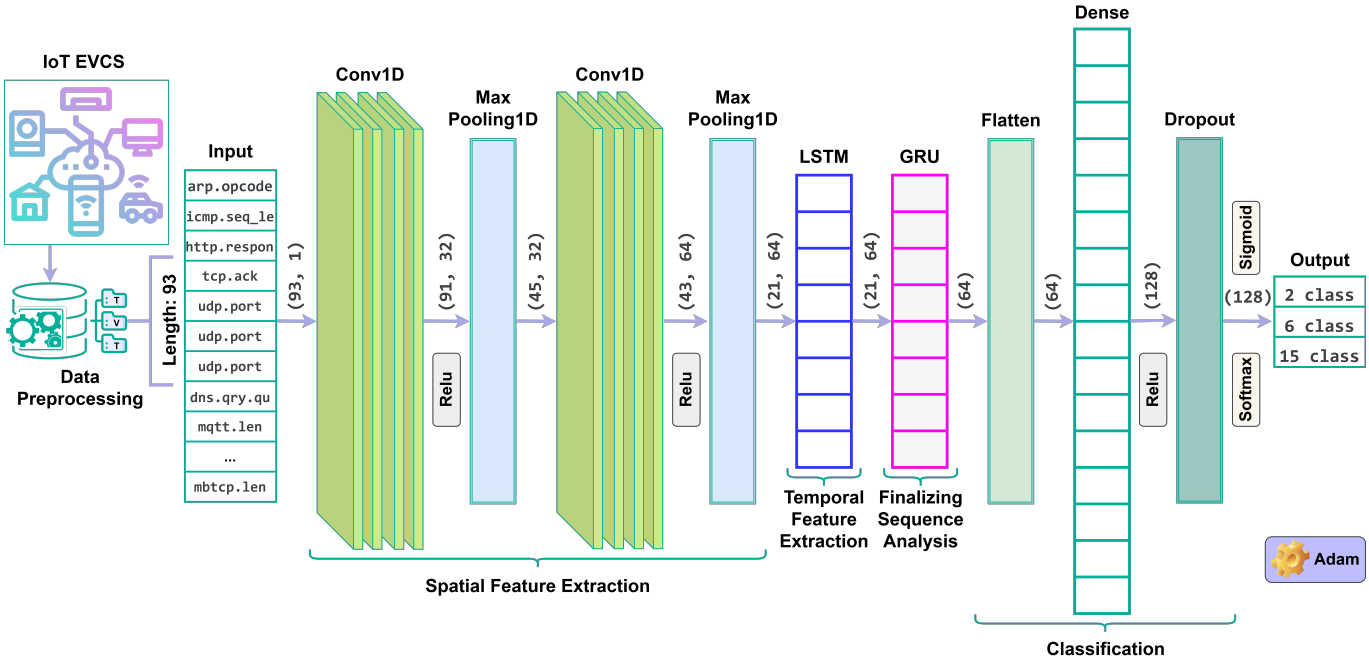

Figure 2. Ensemble Model Design and Architecture.

The proposed model begins with an input layer designed to receive a vectorized form of network traffic data. The input shape is tailored to the dimensions of the feature set extracted from the network packets. The data undergo a series of transformations through two Conv1D layers, each followed by a MaxPooling1D layer to reduce dimensionality and emphasize the most salient features.

The sequential aspect of the data is then processed through a hybrid LSTM-GRU arrangement-a single LSTM layer with return sequences set to true feeds into a GRU layer, creating a deep, sequential model capable of handling complex time-dependent patterns. This combination captures a comprehensive temporal profile of traffic data, encompassing both short-term fluctuations and long-term trends indicative of intrusive behavior.

To finalize the classification, the model is flattened and passed through a dense layer with ReLU activation, introducing nonlinearity and aiding in learning complex patterns. A dropout layer is included to mitigate overfitting, followed by a softmax activation layer that classifies the traffic data into predefined categories ranging from normal to various types of attack vectors.

The model is compiled with the Adam optimizer, which is known for its efficiency in handling large datasets and its adaptive learning rate capabilities. The loss function employed is sparse categorical cross-entropy, which is particularly suited for classification problems in which the classes are mutually exclusive.

This innovative NIDS framework is designed to be a cornerstone in defense against cyber threats in IoT-based EVCS. Using a DL approach that integrates CNN layers for feature extraction with LSTM and GRU layers for temporal data analysis, the proposed model not only identifies existing threat patterns but also adapts to emerging anomalies. It stands as a testament to the potential of AI in fortifying the cybersecurity measures of critical infrastructure within the smart city ecosystem.

4.3. Integration of CNN, LSTM, and GRU

In the quest to bolster the cybersecurity infrastructure of IoT ecosystems, particularly EVCS, the integration of CNN, LSTM, and GRU presents a formidable approach [30]. This confluence of neural network models forms a sophisticated analytical framework capable of discerning intricate patterns within sequential data that are characteristic of intrusion activities.

The synthesis of CNN, LSTM, and GRU models facilitates a dual-phase analysis–spatial followed by temporal–each phase tackling different data aspects. CNNs are adept at extracting spatial features from input data (Figure 3). They apply a series of learnable filters to input sequences, capturing essential features such as the signature of packet headers or the frequency of specific network events. This is particularly crucial in the context of EVCS, where the myriad of devices and communication protocols introduce a complex and dense feature space [12].

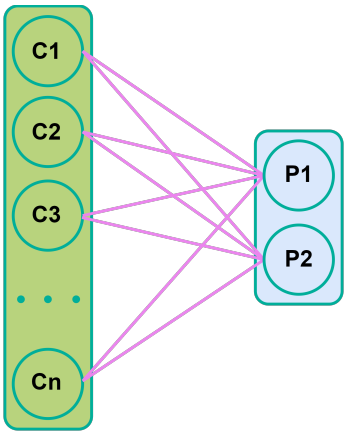

Figure 3. CNN: Spatial Feature Extractors.

The spatially enriched features identified by the CNN layers serve as input to the LSTM and GRU layers. The LSTM layers are engineered to remember information over extended time intervals, making them particularly effective at understanding the long-range dependencies within the data–dependencies that often hold the key to identifying sophisticated cyber threats [31]. Meanwhile, the GRU layers provide the model with the flexibility to reset information that is no longer relevant, allowing for a more adaptable and efficient analysis of the temporal aspects of the data.

The LSTM's architecture, with its memory cells and gates, provides a mechanism for learning which data in a sequence is important to keep or discard (Figure 4). In the context of EVCS network traffic, this means being able to retain critical information about a sequence of actions that could indicate a coordinated attack while ignoring irrelevant data.

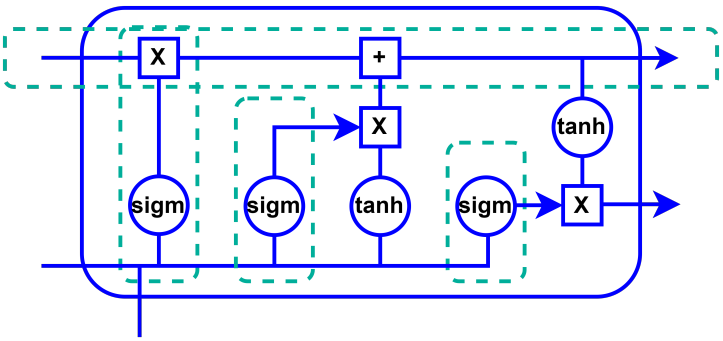

Figure 4. LSTM: Guardians of Temporal Coherence.

Complementing LSTM, GRU simplifies the gating mechanism and merges the forget and input gates into a single update gate (Figure 5). This allows the GRU to make fewer parameter updates, thereby reducing computational complexity without significantly compromising the network's performance. For real-time NIDS applications in IoT-based EVCS, where computational resources are at a premium, this efficiency is invaluable [32].

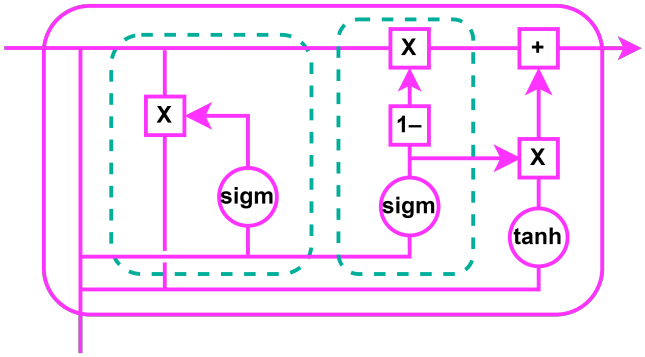

Figure 5. GRU: The Temporal Refiners.

The integration of CNN, LSTM, and GRU within the proposed model is seamless. The output from the convolutional layers–rich in spatial feature representation–flows into the LSTM and GRU layers, which further process the data in the temporal dimension. This sequential processing pipeline ensures that every piece of information is optimally used to make informed decisions about the nature of the traffic–whether it is benign or malicious.

Our ensemble approach strategically combines the strengths of these models through a sophisticated weighted voting mechanism. This mechanism assigns weights to each model's predictions, calibrated based on their performance in the validation phase, ensuring a balanced contribution to the final intrusion detection decision. This nuanced integration not only enhances the detection accuracy but also ensures robustness against diverse cyber threats, marking a significant advancement in safeguarding IoT-based EVCS.

The academic implications of this ensemble approach are profound. It provides a blueprint for designing sophisticated NIDS that can learn from complex data streams and adapt to evolving cyber threats. Future work may explore the scalability of the proposed model across different IoT platforms [6], further refine the model to handle encrypted traffic, and develop unsupervised learning techniques to autonomously label and classify new types of intrusions.

The CNN-LSTM-GRU ensemble model is not merely an architectural novelty; it is a methodologically sound and empirically robust approach to safeguarding IoT infrastructures. By leveraging the distinctive capabilities of CNNs for feature extraction and the sequential data processing prowess of the LSTM and GRU layers, the proposed model sets a new standard for NIDS in IoT environments. Its application in EVCS represents a significant leap forward in the domain of IoT security, promising enhanced resilience against cyber threats in an increasingly interconnected world.

4.4. Data Preprocessing

Edge-IIoTset is a comprehensive, realistic cybersecurity dataset designed for IoT and IIoT applications [33]. It is tailored for ML-based IDS in both centralized and federated learning contexts. This dataset was generated using a custom-built IoT/IIoT testbed encompassing a diverse range of devices, sensors, protocols, and cloud/edge configurations. It includes data from more than 10 different IoT devices and identifies 14 distinct IoT and IIoT attack types, categorized into five threats. The dataset features 61 highly correlated features out of 1176 identified, covering various sources, such as alerts, system resources, logs, and network traffic. In addition, it provides a primary exploratory data analysis and evaluates ML approaches in different learning modes.

The preprocessing of Edge-IIoTset constitutes a pivotal phase in our research, designed to render the data compatible and optimized for the intricate workings of the ensemble model. This phase encapsulates a series of methodical steps, ensuring that the data not only reflect the underlying complexities of IoT environments but are also conducive to effective DL.

Initially, the dataset comprised 63 features representative of the diverse and multifaceted nature of network traffic within IoT-based EVCS. Preprocessing started with a focus

on categorical variables, which are predominant in network datasets. Variables such as HTTP methods, DNS query lengths, and MQTT topics were subjected to label encoding. This step transformed these categorical strings into a numerical format, a prerequisite for subsequent ML algorithms.

Following the encoding, the numerical representations underwent one-hot encoding. This transformation is particularly crucial because it converts categorical integer features into a binary matrix, thereby mitigating any misleading ordinal relationships that traditional numerical encoding might imply. One-hot encoding expands the feature space, enabling the model to better understand and differentiate categorical data. Consequently, the number of features after the one-hot encoding increased to 119.

Given the expanded feature space, the next step involved streamlining the dataset.

- The dataset was scrutinized for duplicate records, and such instances were removed to prevent biases in the model's learning process.
- The data was examined for null values, ensuring the integrity and consistency of the dataset.
- A novel approach was adopted in which a hash function was employed for each column to identify identical columns. By comparing the hashes, groups of identical columns were identified, and all but one in each group were removed. This step is crucial for reducing redundancy in the dataset, thereby enhancing the model's efficiency.

After the reduction and cleaning processes, the feature count decreased to 99. To further refine the dataset, a Chi-squared test was applied. This statistical test is instrumental in feature selection because it evaluates the independence of each feature against the target variable. The Chi-squared test scored each of the 99 features, allowing us to identify and select the top 93 features that exhibited the most significant relationships with the target variable. This selection was influenced by the intrinsic ability of the CNN component in the ensemble to discern and use the most pertinent features effectively.

The data processing efforts culminated in the distribution of network traffic as follows, effectively delineating the varied landscape of normal and anomalous activities within the dataset (Table 2).

Table 2. Distribution of Processed Records.

Class			**Records**
Normal	Normal	Normal	1,399,624
Attack	DDoS	DDoS_UDP	121567
		DDoS_ICMP	67,939
		DDoS_TCP	50,062
		DDoS_HTTP	48,544
	Injection	SQL_injection	50,826
		Uploading	36,957
		XSS	15,068
	Scanning	Vulnerability_scanner	50,026
		Port_Scanning	19,977
		Fingerprinting	853
	Malware	Password	49,933
		Backdoor	24,026
		Ransomware	9689
	MITM	MITM	358

The final dataset was then divided into a ratio of 70:10:20 for the training, validation, and testing sets, respectively. This division ensures a comprehensive evaluation of the model across different data subsets. Further, a standard scaler was employed to normalize the training, validation, and testing data. This normalization is crucial because it scales the

features to a standard range, thereby preventing any feature with a high magnitude from dominating the learning process and ensuring uniform contributions from all features.

The meticulous preprocessing of Edge-IIoTset plays a crucial role in the success of the ensemble model. By transforming, reducing, cleaning, and normalizing the data, we ensure that the dataset is not only representative of the real-world scenario but also primed for effective and efficient DL, laying a robust foundation for the subsequent phases of model training and validation.

4.5. Evaluation Metrics

For the effective evaluation of the ensemble model, we employed a tailored set of metrics that aligned with the objectives of the IDS within IoT-based EVCS [3].

1. Accuracy is quantified as the ratio of correctly predicted observations to the total observations:
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \quad (1)$$
This metric offers a primary indication of the model's overall classification performance, particularly pertinent in datasets with balanced class distributions.
2. Precision is the proportion of true positives among predicted positive observations:
$$Precision = \frac{TP}{TP + FP}. \quad (2)$$
Recall is the ratio of true positive observations correctly predicted:
$$Recall = \frac{TP}{TP + FN}. \quad (3)$$
Precision and recall are crucial in scenarios where the costs of false positives and false negatives are significant, such as in IDS.
3. F1-score is the harmonic mean of precision and recall, offering a balance between the two:
$$F1 - score = 2 * \frac{(Recall * Precision)}{(Recall + Precision)}. \quad (4)$$
F1-score is particularly valuable in contexts where an equitable tradeoff between precision and recall is desirable.
4. A confusion matrix is a specific table layout that visualizes the performance of an algorithm. This matrix provides an in-depth perspective of classification accuracy, revealing the nature of errors, which is indispensable for refining a model.
5. Log loss or logarithmic loss measures performance in which the prediction output is a probability value between 0 and 1:
$$\text{Log loss} = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (5)$$
where y_i is the true label, and $\hat{y}_i$ is the predicted probability.

It is an essential metric for evaluating a model that outputs probabilities and assessing the model's confidence in its predictions.

These metrics collectively form a robust framework for evaluating the ensemble model's performance. By focusing on accuracy, precision, recall, F1-score, confusion matrix, and log loss, we gain comprehensive insights into the model's ability to accurately and reliably detect intrusions in the specialized context of IoT-based EVCS. This approach ensures that the model is not only effective in identifying threats but also efficient in minimizing false alarms, which is paramount in real-world applications.

4.6. Implementation Details

In this study, the implementation of the ensemble model was skillfully executed using Python for its wide-ranging library support, particularly TensorFlow and Keras for DL, alongside Scikit-learn for data preprocessing. Pandas and NumPy complement these for effective data manipulation. Version control was meticulously managed using Git, with the project's codebase and version history accessible at the repository https://github.com/TATU-hacker/CNN-LSTM-GRU.git, uploaded on 17 November 2023. The computational backbone of the project was the Kaggle GPU P100 platform, known for its formidable processing capabilities, which significantly expedited the training and inference phases.

To address the constraints of IoT environments, the ensemble model was designed with scalability and efficiency at its core. It can adapt seamlessly to varying data volumes, a critical feature for IoT applications. To ensure compatibility with IoT devices, known for their limited processing capabilities, the model was optimized for computational and memory efficiency and tailored for potential integration with edge computing, thereby minimizing latency and reducing bandwidth requirements. This thoughtful combination of software choices and hardware optimization ensures the model's applicability in the dynamic and resource-constrained landscape of IoT-based EVCS.

5. Experimental Results

The essence of empirical validation lies in the rigor of experimental analysis, wherein theoretical models confront the test of practical performance. This section presents a detailed exposition of the experimental results derived from the evaluation of the ensemble model, tailored for intrusion detection within the intricate framework of IoT-based EVCS. Using a methodological approach, the model was subjected to various tests, ranging from binary to multifaceted multiclass classifications. Each test was meticulously designed to probe the model's predictive prowess across a spectrum of scenarios that mirror the heterogeneity of potential security breaches in IoT environments.

Binary classification trials were aimed at discerning the presence or absence of intrusion attempts, thus laying the groundwork for the model's capability to distinguish between normal operations and anomalies. Progressing to more granular levels, six-class and fifteen-class classification tests were orchestrated to evaluate the model's ability to identify specific types of intrusions, each with its unique signature and implications (Table 3).

Table 3. Model Performance Metrics.

Performance Metric	2 Class	6 Class	15 Class
Test Loss	0.0000	0.0532	0.0632
Test Accuracy (%)	100	97.44	96.90
Epoch	6	50	50
Training time (s)	1885.46	14803.63	14719.47
Testing time (s)	42.53	42.20	40.65

5.1. Binary Classification Results

In an era where precision is paramount, the ensemble model demonstrates remarkable proficiency in binary classification within the specialized sphere of IoT security for EVCS. The model's acumen, distilled through only six epochs, yielded a test loss imperceptible to statistical significance and a test accuracy that epitomizes perfection (Figure 6). Such exemplary performance, encapsulated within 1885.46 s of training and only 42.53 s of inferential judgment, heralds not only the model's computational efficiency but also its potential deployment in scenarios where the immediacy of threat detection is paramount.

The ensemble's binary classification endeavor, delineating "No Intrusion" from "Intrusion", culminated in an exemplary synchronization with the ground truth, as evinced by the congruence of precision, recall, and F1-score, each reaching the pinnacle of 1.00 for both categories (Table 4). This zenith of classification metric unanimity, seldom achieved in the

intricate domain of cybersecurity analytics, highlights the model's sophisticated capacity to discern with meticulous exactitude.

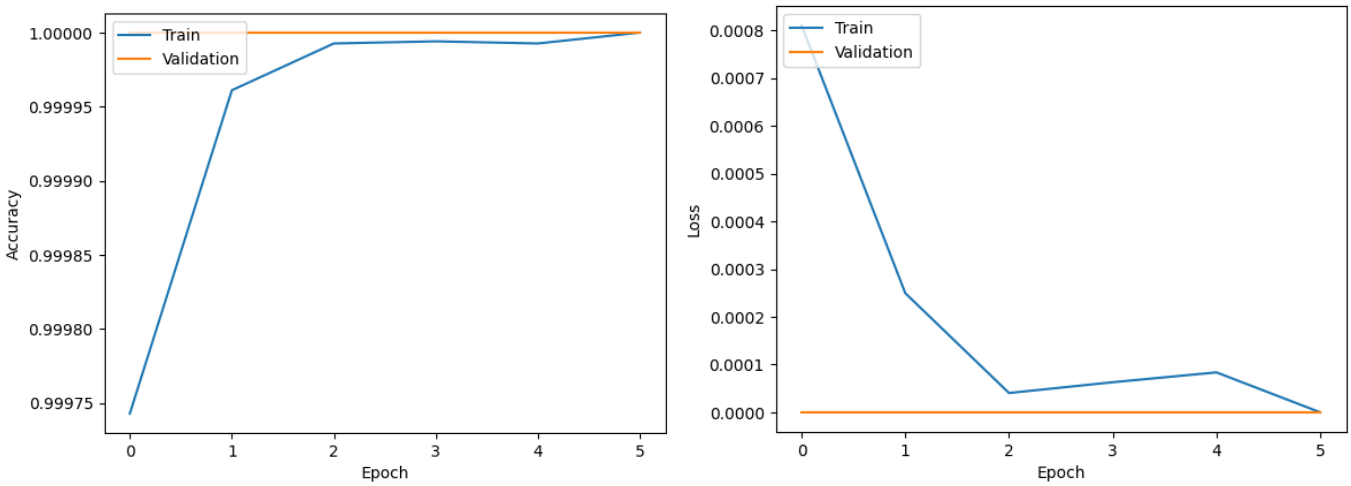

Figure 6. Model accuracy and loss.

Table 4. Classification Report.

	Precision	Recall	F1-Score	Support
No Intrusion	1.00	1.00	1.00	279,968
Intrusion	1.00	1.00	1.00	109,122
accuracy			1.00	389090
macro avg	1.00	1.00	1.00	389,090
weighted avg	1.00	1.00	1.00	389,090

The classification report and ensuing confusion matrix–both in their raw and normalized states–serve as a testament to the model's impeccable discriminative abilities (Figures 7 and 8). They exhibit an unequivocal dichotomy between normalcy and intrusion, a dichotomy that is stark and devoid of the ambiguity that often plagues classification endeavors. This absolute bifurcation in the model's predictive capabilities marks a significant milestone in the quest for robust, fail-safe security systems in the burgeoning field of IoT.

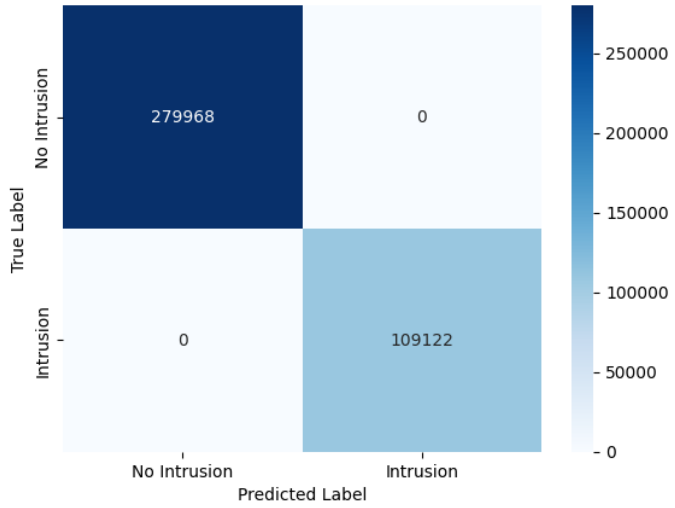

Figure 7. Confusion Matrix.

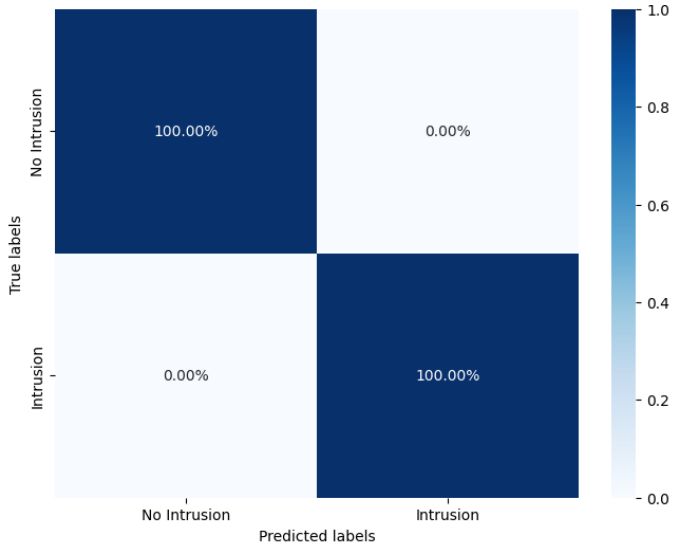

Figure 8. Normalized Confusion Matrix.

5.2. Six-Class Classification Results

The model's ability to distinguish between the six nuanced threat landscapes is reflected in an impressive accuracy of 97.44%, a metric that stands as a testament to its robustness and the veracity of its training (Figure 9). This level of accuracy, particularly in the complex and often chaotic environment of IoT security, speaks to the model's sophisticated feature extraction and classification capabilities. Although the test loss of 0.0532 indicates room for refinement, it remains a commendable figure given the intricacy of the task at hand (Figure 9). Further, the extended training duration of 14,803.63 s indicates the model's intensive learning process and the rapid testing time of 42.20 s underscores its practical efficiency. This juxtaposition of extended training with swift testing is emblematic of a model that, once trained, can offer real-time, reliable threat detection, which is crucial for the active defense of IoT systems.

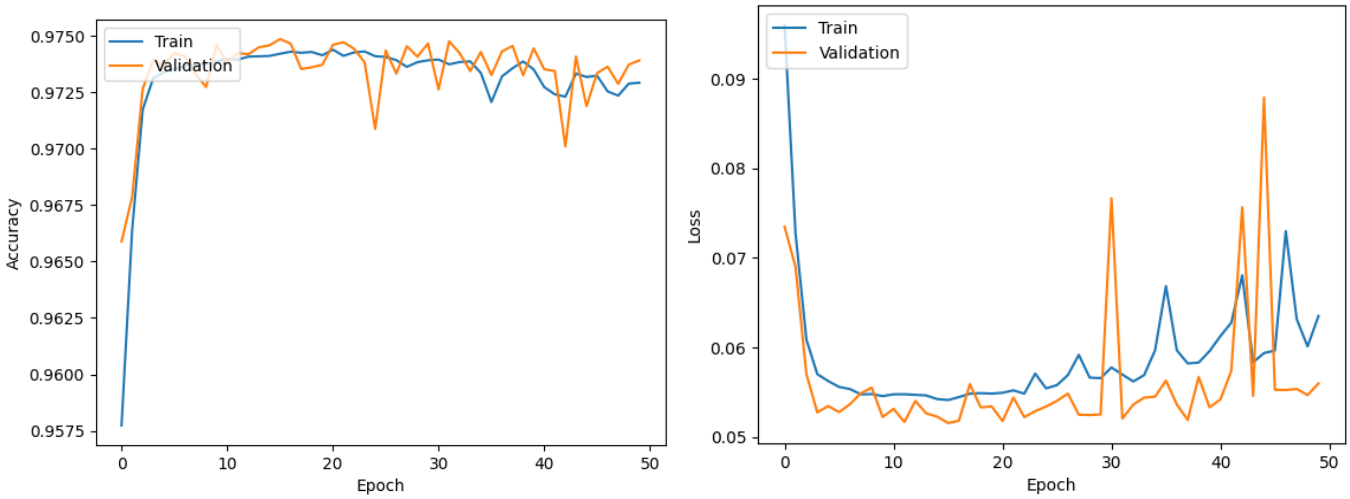

Figure 9. Model accuracy and loss.

The proposed model exhibits exceptional precision in the "Normal" category, achieving perfect scores across precision, recall, and F1-score metrics (Table 5). The "DDoS" and "Scanning" categories also showed high metrics, demonstrating the model's adeptness at identifying these particular types of intrusions. Challenges surfaced in the "Injection" and

"Malware" categories, where the precision and recall metrics indicated a greater difficulty in class distinction, suggesting potential avenues for future research and model enhancement.

Table 5. Classification Report.

	Precision	Recall	F1-Score	Support
Normal	1.00	1.00	1.00	279,968
DDoS	0.98	0.97	0.98	57,614
Scanning	0.94	0.94	0.94	14,163
Injection	0.72	0.95	0.82	20,415
MITM	1.00	1.00	1.00	67
Malware	0.95	0.62	0.75	16,863
accuracy			0.97	389,090
macro avg	0.93	0.91	0.91	389,090
weighted avg	0.98	0.97	0.97	389,090

The confusion matrix and its normalized counterpart reveal a high degree of congruence between the predicted labels and true classifications, with most predictions accurately aligning with their respective categories (Figures 10 and 11).

Figure 10. Confusion Matrix.

Figure 11. Normalized Confusion Matrix.

5.3. Fifteen-Class Classification Results

Based on the fifteen-class classification, the ensemble model's ingenuity was rigorously evaluated in its ability to discern a detailed spectrum of cybersecurity threats, each with unique signatures and behavioral patterns. After a formidable training duration of 50 epochs, the model emerged with a commendable test accuracy of 96.90% (Figure 12). Although slightly lower than the six-class classification accuracy, this figure remains significantly high given the complexity introduced by the finer granularity of threat categories. The test loss of 0.0632, although higher than previous test results (Table 3), aligns with expectations for a more challenging classification task and underscores the tradeoffs inherent in multiclass classification (Figure 12). The training time, recorded at 14,719.47 s, indicates the considerable computational resources deployed in this endeavor. However, the model's testing efficiency, as evidenced by the brief testing time of 40.65 s, affirms its potential for real-time application.

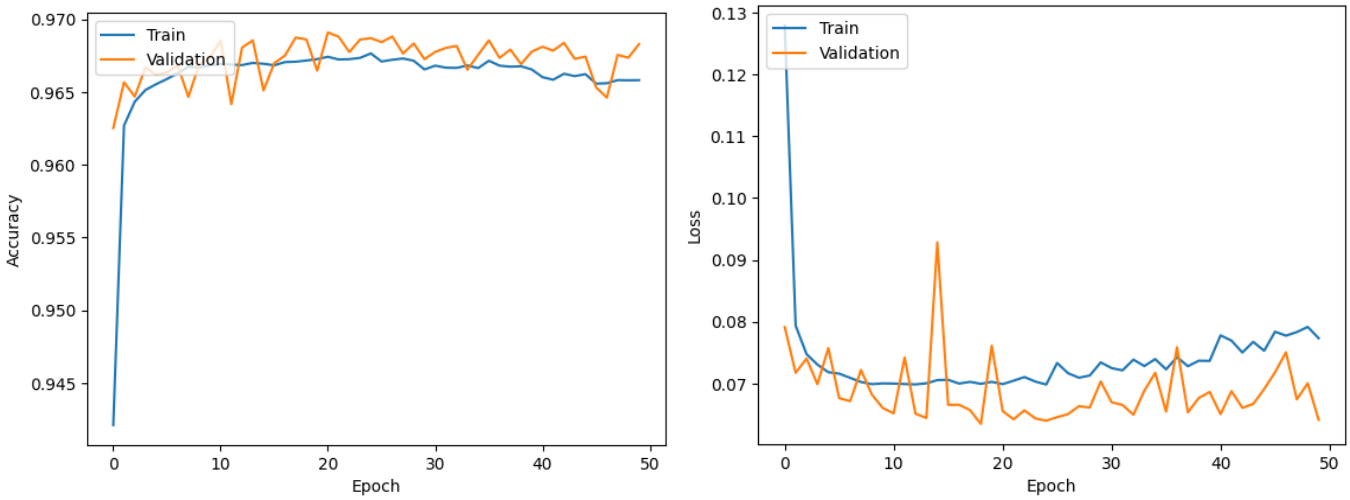

Figure 12. Model accuracy and loss.

The classification report reveals the ensemble model's nuanced understanding of diverse attack vectors (Table 6). With perfect precision and recall in the "Normal" and "DDoS_UDP" categories, the model demonstrates its ability to identify clear-cut patterns of network behavior and straightforward intrusion attempts. However, the "SQL_injection" and "XSS" categories, with lower precision, indicate a propensity for false positives, where the model's judgment may benefit from additional refinement. The "Password" and "Fingerprinting" categories, which show disparities in precision and recall, suggest a more complex interplay of features that could require advanced analytical strategies to improve classification accuracy.

Table 6. Detailed Classification Report.

	Precision	Recall	F1-Score	Support
Normal	1.00	1.00	1.00	279,968
MITM	1.00	1.00	1.00	67
Uploading	0.90	0.68	0.78	7426
Ransomware	0.90	0.90	0.90	1978
SQL_injection	0.62	0.82	0.71	10,026
DDoS_HTTP	0.95	0.90	0.93	9675
DDoS_TCP	0.97	0.93	0.95	10,117
Password	0.65	0.56	0.60	10,102
Port_Scanning	0.85	1.00	0.92	3979
Vulnerability_scanner	0.99	0.92	0.96	10,023
Backdoor	0.98	0.92	0.95	4783
XSS	0.64	0.88	0.74	2963
Fingerprinting	1.00	0.27	0.43	161
DDoS_UDP	1.00	1.00	1.00	24,332
DDoS_ICMP	0.99	1.00	1.00	13,490
accuracy			0.97	389,090
macro avg	0.90	0.85	0.86	389,090
weighted avg	0.97	0.97	0.97	389,090

The confusion matrix presents an elaborate portrayal of the model's performance, with dominant true positive rates across most categories (Figure 13). It also highlights cross-class confusion, particularly between "Password" and other forms of malware, revealing subtleties in the dataset that the model may not fully capture. The normalized confusion matrix, which depicts the proportion of correct predictions within each class, underscores the model's proficiency while also illuminating those classes where precision is paramount (Figure 14).

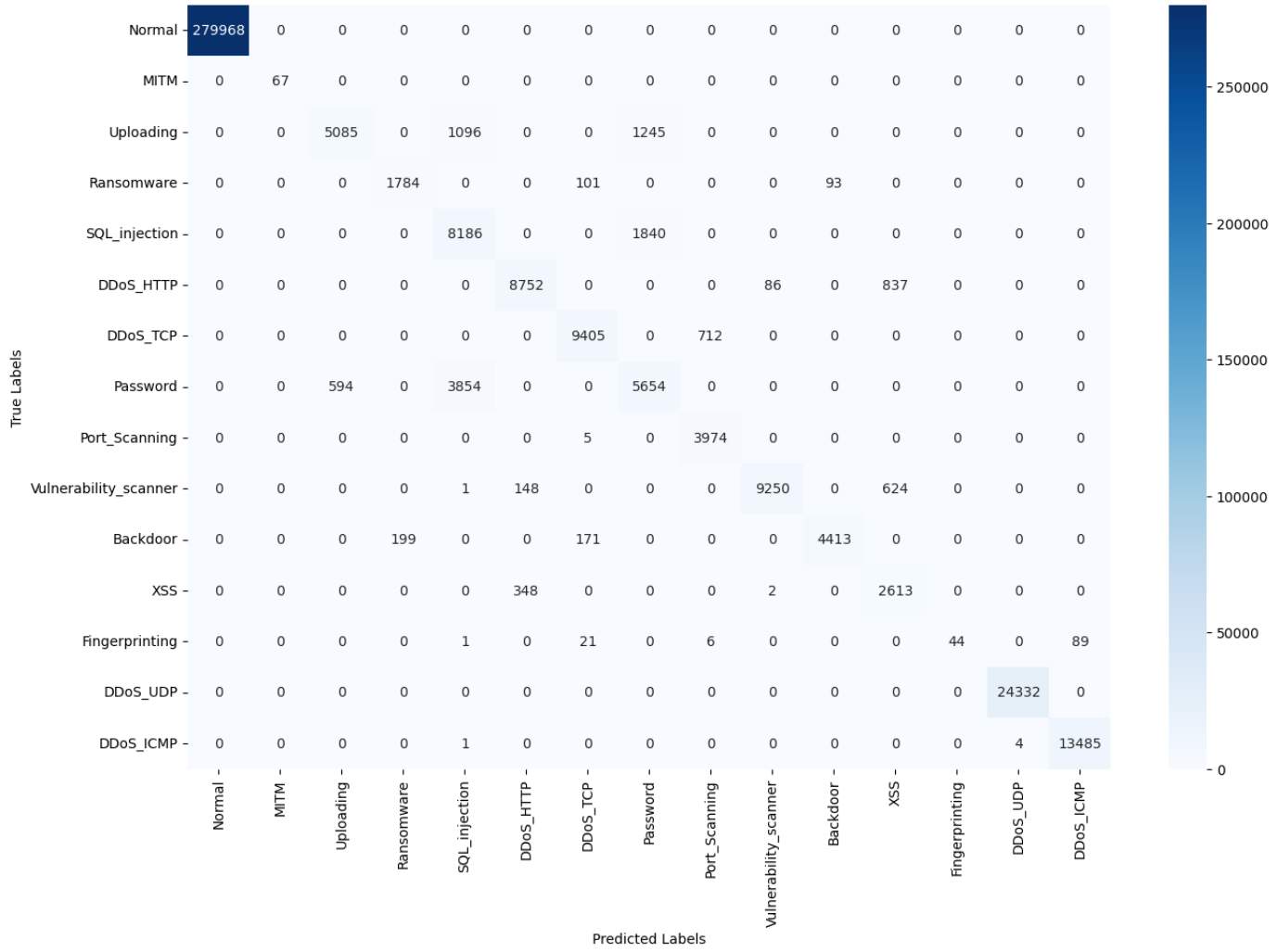

Figure 13. Confusion Matrix.

In synthesizing these results, the fifteen-class classification demonstrates the model's substantial capability to accurately identify a range of intrusion types in IoT contexts. Although certain classes present opportunities for improvement, the overall performance suggests that the ensemble model is a formidable tool in the sophisticated domain of cybersecurity threat detection. Future work will seek to enhance the model's discernment in those categories that posed challenges, refining its predictive power and bolstering its operational readiness for deployment in live environments.

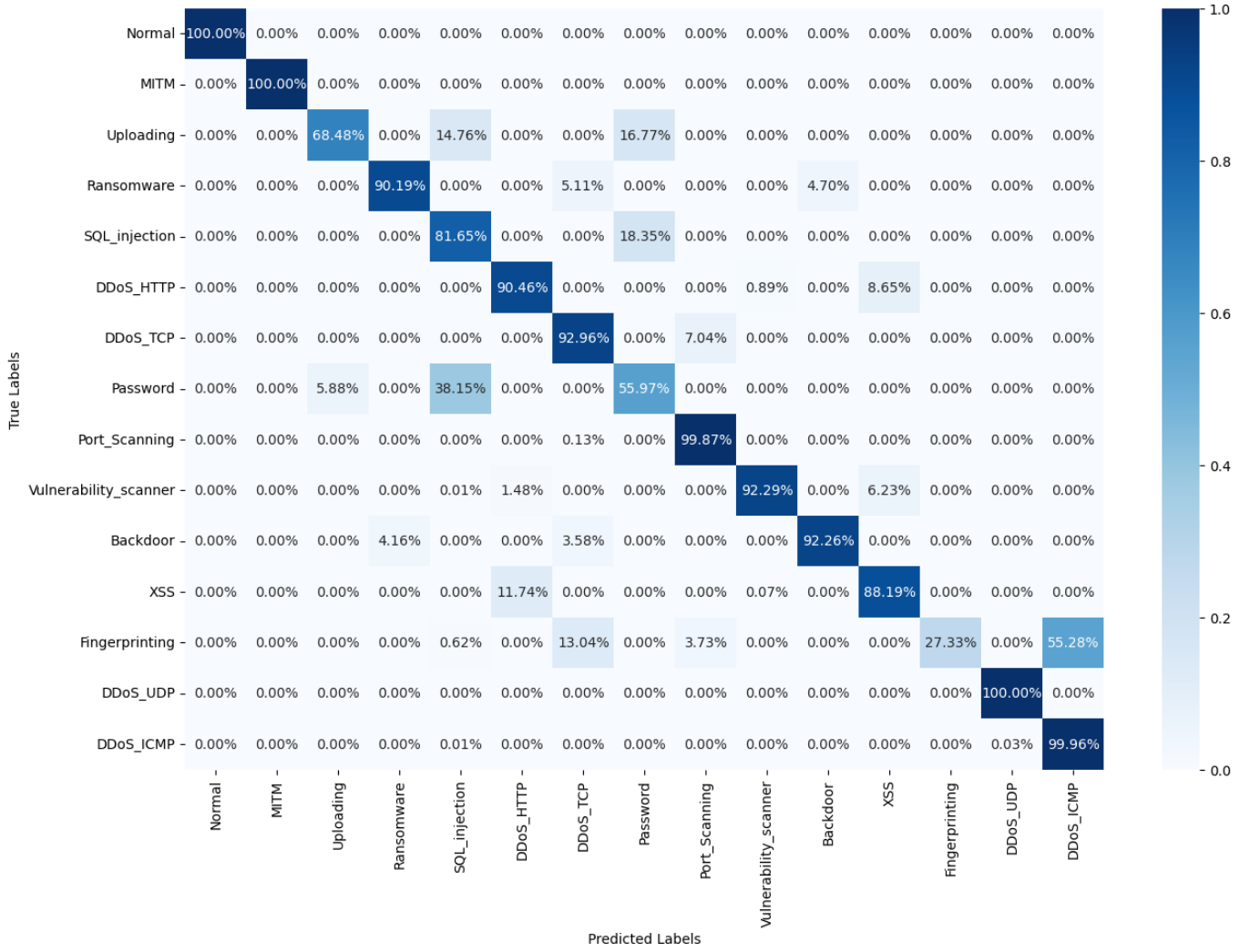

Figure 14. Normalized Confusion Matrix.

6. Discussion

We performed a comprehensive examination of the CNN-LSTM-GRU ensemble model within the diverse and challenging domain of IoT security for EVCS. A comparative analysis, as detailed in Table 7, situates the ensemble model within the context of recent advancements, delineating its standing against contemporary architectures in the field.

Table 7. Comparison of Model Accuracies.

Model	Year	Accuracy (%)		
		2 Class	6 Class	15 Class
DNN [33]	2022	99.99	96.01	94.67
Inception Time [34]	2022	-	-	94.94
CNN-LSTM [35]	2022	100	98.69	-
VGG-16 [36]	2023	100	-	94.86
DeepAK-IoT [37]	2023	-	-	94.96
LNKDSEA [38]	2023	99.99	84.97	80.12
RNN [39]	2023	100	92.53	90.22
MAGRU [40]	2023	99.99	-	-
CNN-LSTM-GRU	2023	100	97.44	96.90

In the binary classification domain, CNN-LSTM-GRU achieved parity with the unassailable accuracy of its peers, where models such as CNN-LSTM [35], VGG-16 [36], and RNN [39] also have perfect scores. This uniform excellence across models underscores a maturing understanding and effective handling of binary classification tasks in the IoT security domain.

The model's success in achieving 100% accuracy in binary classification can be attributed to the complementary strengths of its constituent architectures. The convolutional layers effectively capture spatial hierarchies in the data, which is particularly useful in identifying patterns indicative of intrusion within the IoT EVCS context. LSTM components contribute to this high performance by capturing long-term dependencies, allowing for an effective understanding of sequence progression in temporal data, a feature common in network traffic. GRUs further refine the model's capability by addressing the vanishing gradient problem often encountered in recurrent networks, thereby enhancing the learning process for long sequences without the need for extensive computational resources.

In the six-class classification scenario, CNN-LSTM-GRU displayed a notable accuracy of 97.44%, surpassing most of its contemporaries and falling slightly behind CNN-LSTM's leading edge. This performance indicates CNN-LSTM-GRU robust feature extraction and sequence learning capabilities, which are critical for distinguishing between a broad spectrum of intrusion behaviors.

The fifteen-class classification, characterized by its intricacy and the granular distinction of intrusion types, demonstrated that CNN-LSTM-GRU maintained a high accuracy of 96.90%. This is a commendable achievement, especially when juxtaposed with DeepAK-IoT [37] and Inception Time [34], which represent the upper echelon of performances in this category. Notably, CNN-LSTM-GRU showed marked superiority over LNKDSEA [38] and RNN [39], underscoring the efficacy of the ensemble approach in managing the increased complexity of fine-grained classifications.

The CNN component of our ensemble model is primarily responsible for spatial feature extraction. Unlike traditional models such as the DNN [33] and RNN [39], which may lack depth in feature extraction, the CNN layers in our model provide a comprehensive analysis of the input data's spatial characteristics. This is evident in the binary classification results, where our model matches the perfect accuracy of the CNN-LSTM [35] and the VGG-16 [36], which are known for their strong feature extraction capabilities.

For temporal analysis, the LSTM and GRU components of our model are critical. The LSTM layers capture long-term dependencies, while the GRU layers focus on shorter-term data sequences. This dual approach allows our model to outperform traditional architectures like the DeepAK-IoT [37] and LNKDSEA [38], particularly in the multi-class classification tasks. It can recognize complex attack patterns that unfold over time, which might be overlooked by models without this temporal depth.

These comparative outcomes not only validate the ensemble model's capability but also propel the discourse on the potential of hybrid models. The integration of multiple neural network architectures may well be the harbinger of a new paradigm in IoT security, where the complexity of threat detection is met with an equally sophisticated analytical arsenal.

Moreover, the results present an impetus for the continued exploration of ensemble methods in DL, pushing the envelope in terms of accuracy, adaptability, and computational efficiency. As the digital infrastructure of IoT expands, the ensemble model's adaptability and learning depth will be pivotal in safeguarding the integrity and robustness of the interconnected systems.

Considering these findings, the CNN-LSTM-GRU ensemble architecture emerges as a potent architecture, heralding a promising direction for future research to further refine and optimize DL strategies for intrusion detection, ensuring that they remain at the vanguard of the ever-evolving cybersecurity landscape.

7. Conclusions

Our investigation into the domain of cybersecurity for IoT infrastructures, particularly focusing on EVCS, culminates with a suite of notable contributions that set a new benchmark for IDS. The introduction of an innovative ensemble architecture that leverages the combined strengths of CNN, LSTM, and GRU, represents a leap forward in the detection of intricate intrusion patterns. The model, rigorously trained and validated against real-world datasets, demonstrates a superior ability to navigate the complexities of cyber threats with impressive accuracy. This study not only demonstrates the feasibility of employing advanced neural network architectures for intrusion detection but also paves the way for future research in securing IoT ecosystems against sophisticated attacks.

The advanced data processing techniques and comprehensive performance analysis employed in this study underscore the depth and rigor of our approach. By achieving high accuracy across binary, six-class, and fifteen-class classifications, the proposed model is robust and adaptable to several potential security breaches. The practical implications of this research extend well beyond theoretical exploration, offering scalable solutions for real-time applications across various IoT scenarios.

As we lay down the groundwork for future explorations, the proposed model stands as a benchmark in the field and a touchstone for ensuing innovations in cybersecurity, inviting the scholarly community to engage with our findings, replicate our success, and venture further into the untapped potential of DL models. Thus, this study does not signal a terminus but rather a beacon, illuminating the path toward a more secure and resilient digital future.

Author Contributions: This manuscript was designed and written by W.K., D.K. and D.T. W.K. conceived the main idea of this study. D.K. and D.T. wrote the programs and conducted all the experiments. W.K., D.K. and D.T. contributed to the analysis and discussion of the algorithms and results. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) (no. NRF2022R1F1A1074767).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rimal, B.P.; Kong, C.; Poudel, B.; Wang, Y.; Shahi, P. Smart Electric Vehicle Charging in the Era of Internet of Vehicles, Emerging Trends, and Open Issues. *Energies* **2022**, *15*, 1908. [CrossRef]
2. Aldaej, A.; Ahanger, T.A.; Ullah, I. Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments. *Sensors* **2023**, *23*, 9869. [CrossRef]
3. Kilichev, D.; Kim, W. Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. *Mathematics* **2023**, *11*, 3724. [CrossRef]
4. Rashid, M.M.; Khan, S.U.; Eusufzai, F.; Redwan, M.A.; Sabuj, S.R.; Elsharief, M. A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. *Network* **2023**, *3*, 158–179. [CrossRef]
5. Peyman, M.; Copado, P.J.; Tordecilla, R.D.; Martins, L.D.C.; Xhafa, F.; Juan, A.A. Edge Computing and IoT Analytics for Agile Optimization in Intelligent Transportation Systems. *Energies* **2021**, *14*, 6309. [CrossRef]
6. Lobato, E.; Prazeres, L.; Medeiros, I.; Araújo, F.; Rosário, D.; Cerqueira, E.; Tostes, M.; Bezerra, U.; Fonseca, W.; Antloga, A. A Monitoring System for Electric Vehicle Charging Stations: A Prototype in the Amazon. *Energies* **2023**, *16*, 152. [CrossRef]
7. Lee, H.C.; Liu, H.Y.; Lin, T.C.; Lee, C.Y. A Customized Energy Management System for Distributed PV, Energy Storage Units, and Charging Stations on Kinmen Island of Taiwan. *Sensors* **2023**, *23*, 5286. [CrossRef] [PubMed]
8. Al Sawafi, Y.; Touzene, A.; Hedjam, R. Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *J. Sens. Actuator Netw.* **2023**, *12*, 21. [CrossRef]
9. Gou, W.; Zhang, H.; Zhang, R. Multi-Classification and Tree-Based Ensemble Network for the Intrusion Detection System in the Internet of Vehicles. *Sensors* **2023**, *23*, 8788. [CrossRef] [PubMed]
10. Awajan, A. A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. *Computers* **2023**, *12*, 34. [CrossRef]
11. Fatani, A.; Dahou, A.; Abd Elaziz, M.; Al-qaness, M.A.A.; Lu, S.; Alfadhli, S.A.; Alresheedi, S.S. Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks. *Sensors* **2023**, *23*, 4430. [CrossRef]

12. Zeinali, M.; Erdogan, N.; Bayram, I.S.; Thompson, J.S. Impact of Communication System Characteristics on Electric Vehicle Grid Integration: A Large-Scale Practical Assessment of the UK's Cellular Network for the Internet of Energy. *Electricity* **2023**, *4*, 309–319. [CrossRef]
13. Strielkowski, W.; Streimikiene, D.; Fomina, A.; Semenova, E. Internet of Energy (IoE) and High-Renewables Electricity System Market Design. *Energies* **2019**, *12*, 4790. [CrossRef]
14. Florea, B.C.; Taralunga, D.D. Blockchain IoT for Smart Electric Vehicles Battery Management. *Sustainability* **2020**, *12*, 3984. [CrossRef]
15. Tappeta, V.S.R.; Appasani, B.; Patnaik, S.; Ustun, T.S. A Review on Emerging Communication and Computational Technologies for Increased Use of Plug-In Electric Vehicles. *Energies* **2022**, *15*, 6580. [CrossRef]
16. Arif, M.; Kim, W.; Qureshi, S. Interference Characterization in Cellular-Assisted Vehicular Communications With Jamming. *IEEE Access* **2022**, *10*, 42469–42480. [CrossRef]
17. Hamdare, S.; Kaiwartya, O.; Aljaidi, M.; Jugran, M.; Cao, Y.; Kumar, S.; Mahmud, M.; Brown, D.; Lloret, J. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. *Sensors* **2023**, *23*, 6716. [CrossRef]
18. Sarieddine, K.; Sayed, M.A.; Assi, C.; Atallah, R.; Torabi, S.; Khoury, J.; Pour, M.S.; Bou-Harb, E. EV Charging Infrastructure Discovery to Contextualize its Deployment Security. *IEEE Trans. Netw. Serv. Manag.* **2023**, 21, 1287–1301. [CrossRef]
19. Girdhar, M.; Hong, J.; You, Y.; Song, T.J.; Govindarasu, M. Cyber-Attack Event Analysis for EV Charging Stations. In Proceedings of the 2023 IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 16–20 July 2023; pp. 1–5. [CrossRef]
20. ElKashlan, M.; Aslan, H.; Said Elsayed, M.; Jurcut, A.D.; Azer, M.A. Intrusion Detection for Electric Vehicle Charging Systems (EVCS). *Algorithms* **2023**, *16*, 75. [CrossRef]
21. ElKashlan, M.; Elsayed, M.S.; Jurcut, A.D.; Azer, M. A Machine Learning-Based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCSs). *Electronics* **2023**, *12*, 1044. [CrossRef]
22. Basnet, M.; Hasan Ali, M. Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station. In Proceedings of the 2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES), Bangkok, Thailand, 15–18 September 2020; pp. 408–413. [CrossRef]
23. Basnet, M.; Hasan Ali, M. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. *IET Gener. Transm. Distrib.* **2021**, *15*, 3435–3449. [CrossRef]
24. Basnet, M.; Hasan Ali, M. WCGAN-Based Cyber-Attacks Detection System in the EV Charging Infrastructure. In Proceedings of the 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES), Beijing, China, 9–12 December 2022; pp. 1761–1766. [CrossRef]
25. Basnet, M.; Hasan Ali, M. Deep-Learning-Powered Cyber-Attacks Mitigation Strategy in the EV Charging Infrastructure. In Proceedings of the 2023 IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 16–20 July 2023; pp. 1–5. [CrossRef]
26. Islam, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Atiquzzaman, M. An Intelligent Privacy Preservation Scheme for EV Charging Infrastructure. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1238–1247. [CrossRef]
27. Lilhore, U.K.; Manoharan, P.; Simaiya, S.; Alroobaea, R.; Alsafyani, M.; Baqasah, A.M.; Dalal, S.; Sharma, A.; Raahemifar, K. HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning. *Sensors* **2023**, *23*, 7856. [CrossRef]
28. Sayegh, H.R.; Dong, W.; Al-madani, A.M. Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data. *Appl. Sci.* **2024**, *14*, 479. [CrossRef]
29. Ahmad, I.; Imran, M.; Qayyum, A.; Ramzan, M.S.; Alassafi, M.O. An Optimized Hybrid Deep Intrusion Detection Model (HD-IDM) for Enhancing Network Security. *Mathematics* **2023**, *11*, 4501. [CrossRef]
30. Meliboev, A.; Alikhanov, J.; Kim, W. Performance Evaluation of Deep Learning Based Network Intrusion Detection System across Multiple Balanced and Imbalanced Datasets. *Electronics* **2022**, *11*, 515. [CrossRef]
31. Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S.; Alimi, O.A. Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things. *J. Sens. Actuator Netw.* **2022**, *11*, 32. [CrossRef]
32. Kethineni, K.; Gera, P. Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. *Systems* **2023**, *11*, 304. [CrossRef]
33. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, *10*, 40281–40306. [CrossRef]
34. Tareq, I.; Elbagoury, B.M.; El-Regaily, S.; El-Horbaty, E.S.M. Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT. *Appl. Sci.* **2022**, *12*, 9572. [CrossRef]
35. Khacha, A.; Saadouni, R.; Harbi, Y.; Aliouat, Z. Hybrid Deep Learning-based Intrusion Detection System for Industrial Internet of Things. In Proceedings of the 2022 5th International Symposium on Informatics and its Applications (ISIA), M'sila, Algeria, 29–30 November 2022; pp. 1–6. [CrossRef]
36. Tomar, K.; Bisht, K.; Joshi, K.; Katarya, R. Cyber Attack Detection in IoT using Deep Learning Techniques. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; pp. 1–6. [CrossRef]
37. Ding, W.; Abdel-Basset, M.; Mohamed, R. DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. *Inf. Sci.* **2023**, *634*, 157–171. [CrossRef]

38. Koppula, M.; LM, L.J. LNKDSEA: Machine Learning Based IoT/IIoT Attack Detection Method. In Proceedings of the 2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS), Bengaluru, India, 19–21 April 2023; pp. 655–662. [CrossRef]
39. Salih, K.M.M.; Ibrahim, N.B. Enhancing IoT Forensics through Deep Learning: Investigating Cyber-Attacks and Analyzing Big Data for Improved Security Measures. In Proceedings of the 2023 4th International Conference on Big Data Analytics and Practices (IBDAP), Bangkok, Thailand, 25–27 August 2023; pp. 1–8. [CrossRef]
40. Ullah, S.; Boulila, W.; Koubâa, A.; Ahmad, J. MAGRU-IDS: A Multi-Head Attention-Based Gated Recurrent Unit for Intrusion Detection in IIoT Networks. *IEEE Access* **2023**, *11*, 114590–114601. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.