Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

A Mathematical and Hybrid Deep Learning Model for Real-Time Intrusion Detection in IoT-Based Electric Vehicle Charging Stations

Adil Fahad
Faculty of Computing & Information,
Department of Computer Science, Al Baha University, Al Baha, Saudi Arabia.
afalharthi@bu.edu.sa

Article History:

Received: *30-04-2024*

Revised: *21-06-2024*

Accepted: *03-07-2024*

Abstract:

The recent frame of IoT and Industrial IoT security brings new type of intrusion detection systems. We propose a new method for Intrusion Detection in IoT based EVCS with the integration of Convolutional Neural Network, Long Short-term Memory model and Gated Recurrent Unit. This work uses a naturally pervasive, and representative real-world security focusing on IoT typical applications to address the capillary layer inherent challenges (e.g. at each EVCS vs through IT infrastructure as compared peripheral equipment). We have tested this both with Binary and Multiclass exhaustively. The benchmarks are perfectly accurate (100 % binary class, 97.44% six-class classification and near ~96/90%% in fifteen classes that certainly sets a new bar for the going forward!) Collectively, the entire ensemble architecture demonstrates a scalable high performance mean so again this ways these accomplishments certify that CNN-LSTM-GRU-based complex models can be used in space-strapped and processing constrained Intrusion Detection system for IoT to perform consistently robust. The ensemble algorithm, which is open sourced on the GitHub under our simulation framework codebase also represents a significant improvement in securing Internet of Things based EVCS from various cyber security threats.

Keywords: IoT, intrusion, integration, recurrent, performance, LSTM-GRU, robust, cyber security, threats.

1. Introduction

In the emerging ecosystem of Internet of Things (IoT) and Industrial IoT (IIoT), robust intrusion detection systems (IDSs) are needed more than ever, for protecting Electric Vehicle Charging Stations(EVCS)[1]. Modern, on-line IoT devices challenge the static nature of traditional cyber-security elements.

IoT technologies are being integrated into critical services, such as EVCS—and with it comes cybersecurity risks. Traditional IDS cannot tackle the ever-evolving sophisticated cyber commination and its individual repression of IoT environment give us an indication to our research. In this research, we focus on improving intrusion detection for IoT-based EVCS by employing advanced neural network architectures based on the unique and complex challenges of devices.

Current IDS solutions face many challenges like Scalability, Adaptivity and resource constraints as well accompanying them diverse attack vector and the demand of real time detection [2] This is further complicated by the high rates of false alarms that are encountered in most systems, rendering them

unreliable. In this paper, we suggest IoT-IDS that is unique IDS forged in an EVCS to solve the mentioned fundamental problems.

Our goals are based on creating a collective IDS model by combining convolutional neural network (CNN) [3], long short-term memory (LSTM), gated recurrent unit

Performance using the Factorat model with evaluating it against the "Edge-IioT set" dataset [4], optimization for sustainable efficiency, and a comparison of present outcomes. We present an evaluation of how effective the ensemble model is at improving detection accuracy, if it can perform well on large datasets, if its resource requirements are feasible and finally its robustness in counteracting dynamic cyber threats.

Here we introduce a novel kind of intrusion detection approach especially designed for the context of IoT-based EVCS. By leveraging the latest in IoT Cybersecurity technology, we prove that an ensemble model is effective and feasible even in this critical discipline.

In the remnants of this Article, we are going to do thorough scrutiny towards NIDS (Network IDS) for Internet accessible based EVCS. Section 2 takes a closer look at IoT in EVCS, detailing the Issues and consequences of using such technology and presents cybersecurity threats unique to iot-based evcs with an added focus on why NIDS are essential for protecting them. The special issue emphasizes the latest technological and scientific breakthroughs in these areas, from basic to applied research streams, shaping future avenues for study. This review sets the stage for our research, which we then describe in detail (Section 3) In Section 4 we presenting our proposed NIDS framework for IoT based EVCS, explaining its architectural view of the system and what CNN, LSTM as well GRU models have done integration, data preprocessing techniques along with evaluation metrics and implementation details. Experimental Section 5 − To serve the binary, six- class and fifteen-class classification results. In the following Section 6, we present a discussion of these results and their interpretation. The last section (7) concludes this paper by discussing our contributions and impact of the work done for security in IoT.

2. Intrusion Detection of Vehicle Charging Stations by IoT

2.1. IoT in Vehicle Charging Stands Vehicle charging points

We can also make a bold statement that IoT is the new standard for EVCS, which introduces unprecedented changes to smart transportation infrastructure [5]. This new fusion delivered an elegance and level of efficiency previously unseen in generic EVCS solutions. The EVCS using the IoT technology hence is a tailored specific modification to ful fill some special needs of Electric Vehicle (EV) charging [6] and cannot be considered as just an extension from IOT systems in general.

Figure 1: High-level schematic of an IoT-enabled Electric Vehicle Charging Stations (EVCS) system-of-system showing interdependencies and communications between different domains including renewable energies, grid infrastructure elements (power-domain)—serving both mobile users with connected vehicle. These connections also represent exchanges of real-time data on which the efficient operation as well a security aspects of EVCS relies due to this its complexity is even higher than general IOT systems.

IoT-capable EVCS, on the other hand, should have extended communication capabilities to enable real time data transfer between charging stations and vehicles. This is an imperative message for appropriate charging scheduling, power load management and energy distribution. [[1]

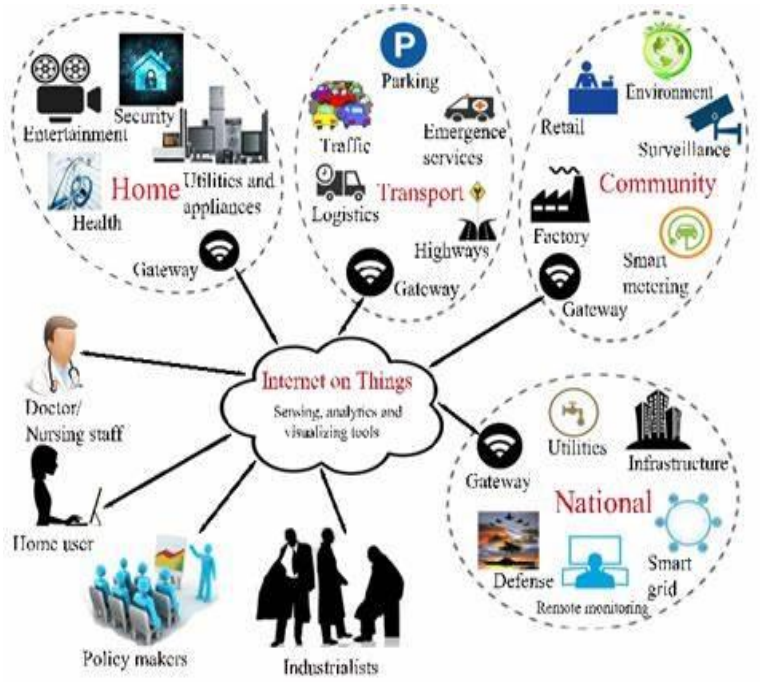

Figure 1. EVCS Architecture

While IoT responsibility at EVCS are similar to that in the traditional sense, there is a unique take on how it performs. Which means monitoring charging rates, to name but one example. This will not give operation of EVCS as all other standard IoT applications, where one can afford data transmission delay. This requires a low-latency distribution media because the grid source has to feed millions of charging stations all over the world with immense electrical power flow loaded in both directions that needs immediate back and forth interaction. The latter is critical because it means charge rates can be altered in real time as well, while alerting a battery to systematic health issues and letting users (and system operators) know ASAP.

Also an IoT-based EVCS integration into the smart grid[7] is a uniqe thing. It's not just about managing the EV charging load either, with this integration also allowing for some grid balancing. Set to be integrated into the IoT, EVCS living coordinated operating exchanges with their electrified siblings some robust grid allies can tax and take in sufficient supply to relieve pressure on the network as a whole. This type of integration is unique, as compared to the many other independent IoT applications.

The IoT handles of sorts for an EVCS that is driven by an IoT are even more in-depth than those found on a general-purpose type of standard-form-factor-IoT. They must be flexible enough to handle anything from user authentication and payment processing, through firmware updates and predictive maintenance. It's important to have this kind of management in place so that the charging infrastructure remains safe and performs well.

In addition, the IoT component of EVCS gives rise to specific cyber security-related challenges. These stations are not only dealing with sensitive consumer information, but they also make up a more

extensive and arguably even more critical aspect of the energy infrastructure surrounding us all. Their two-faced nature gives them additional vulnerability to cyberattack, thus more sophisticated and dedicated IDSes than SOTSue (secure off the shelf uCplugs) are needed. The results of a security breach could also be severe, In addition to the potential for personal information theft, critical infrastructure such as the energy grid are susceptible targets so higher level securities would likely be required.

2.1. NIDS: Network Intrusion Detection Systems

The Inseparable Husband and Wife:NIDS and IoT onNext → Network Based Idle System Detection [8]: These are implement by capturing network packets to provide information about the data that flows through a host's intermediate layer of communication. The one of the primary stopper NIDS in IoT scenarios, is to tell smarts people if they can identify and defend data transmission property on smart devices all Contexts & platforms. This also includes supervising and determining plenty of illegal access action, MR-VAN or computer to machine so as self-suplicative software infection/and ab-bound IT security infringements that will affect the performance and securance condition of IoT systems [9].

They do this by analyzing the passage of network flows and patterns in that behavior which will point to potential security incidents. Most notably, the links between IoT devices and their networks discover obvious roads of cyberattacks that will need to: [10] Deployment NIDS in IoT environments becomes crucial for a network infrastructure secure over performing still reliability.

The stakes in the cybersecurity of EVCS are particularly high given that they can impact critical energy infrastructure and because of privacy concerns related to data on personal use. So, in this context the NIDS used must be much sophisticated than normal for it to have high detection & response rates against a lot of threats with very less false positive and still achieving more number of true positives. Examples of these would be in respect to activity like national level energy infrastructure, and private data — i.e. advanced persistent threats (APTs), or more state-named actors with by-and-large greater resources targeting fewer people at a time due to seeking highly-specific information via cyber attacks that are otherwise well-funded forest fires Vs strains on economic-scale levels as below/examplesREL:

2.2. Challenges in IoT-Based EVCS

Troubled WatersEVCS oriented IoT presents its own challenges. — Beyond the Typical IOT Systems System One, Business Continuity is #1 (I promise you I will bring this back to Productivity). EVCS can be key bits of the transportation framework [5] and personal downtime suggests unfavorable actual prosperous customers. The need for a 24×7 service means it is very important to provide an IoT framework that works not only in high loads when users overload the network with unnecessarily energetic traffic but also are targeted by attackers.

How IoT-based EVCS work On an even more higher level, it is a question of safety implications. Unlike much of IoT which goes to monitoring, if an EVCS fails there are situations where it can cause someone's death. This is due to the fact that these systems are working based on high power levels, it may be dangerous for EV charging if not being used correctly (fire cause of too much current or

equipment stopped to work). Therefore, the IoT systems that are deployed within EVCS need to be both immune from cyber threats from and resistant physical as well as technical failures.

Also, as per the discussion in [13], integration of EVCS with other smart grid infra-structures increases this complexity even more. Thereby, such stations may also behave as intelligent nodes in the smart grid to participate DR/EM etc. Fact is that these devices are all energy consumers (or at most very-localized storage or redistribution points) in the vast IoT-ecosystem, and will need to play nice with each other implement their combined capabilities. Dealing with this dynamic interplay of EVCS and smart grid involves substantial technical challenges that require sophisticated data analytics as well as real-time decision making [7].

This merging thing can expand all the way to high-level IoT-based EVCS, but it will take a more detailed system analysis of both types (and collateral couplings thereof) combined into one plain hybrid type. This intersection represents a new frontier in how energy services are provided and managed, evolving from more siloed to increasingly integrated or even networked systems.

On the technical side as EVCS by its nature is data-centric in operation — it takes a substantial technological effort on IT and storage solutions to not only adopt new approaches but still emphasizing high performance applications especially for cybersecurity reasons. The stations generate a tremendous amount information to be able to both produce and process information at the entire spectrum related user personal data or operational parameter respectively. Note: Data security, privacy and veracity is indispensable for these highly valuable infrastructures which are potential targets specific to cyber-attacks!

Conclusion: OT, essential (especially in Critical Infrastructure) that allows EVCS to work reliably and safely. It is the hardware and software long used for critical systems — which NEWLY ALWAYS MUST INCLUDE REALTIME & SAFETY FOR ALL ASPECTS OF YOUR CHARGE SYSTEM; AT SAME TIME IT CREATES A SEMI-DIGITIZED INTERFACE between PHYSICAL DOMAIN AND THE DIGITAL WORLD WHENEVER ITS SENSORS SEND THEIR DATA TO RESTRAINED USE IN OTHER INFORMATION OUTPUT NETWORKS OR MODULE PROTECTIONS ANEW *_* [85]. It is a very challenging integration problem because such intercommunication and synchronization have never been in front of readily available to two fundamentally different systems at large.

This system is challenging to regulate without only through technology but also by framing some implementable view on whole energy-mechanical, IT and OT interactions. The task becomes even more difficult when regulations factor into the equation, as well as technological changes or user preferences. This challenge of securing everything is highlighted by the breadth required to maintain a working IOT system even before it all gets connected — cybersecurity, any electrical engineering involved (when things get plugged in), data science and context-level network/systems integration.

2.3. EVCS Cybersecurity Threats

Cybersecurity Challenges of IoT-based EVCS: The cybersecurity challenges an IoT based electric vehicle charging station has is significantly different from those posed by traditional internet-connected devices. The possibility of disrupting the charging process is one of the bigger issues. A

charging process that a bad actor might take advantage of in order to overcharge or under charge EV batteries. Thus, not only does it harm batteries but also can lead to potential hazards of unsafe cell temperature rise. Furthermore, this tampering can also disrupt simultaneous service availability frustrating users and eroding trust in the EV infrastructure. Yet a further threat is eavesdropping of communication between EVs and an EVCS.

Users frequently exchange messages with usernames, passwords or PINs as well as credit card data and vehicle profiles. This access to data allows cybercriminals can commit other things aside from character burglary and financial fraud but they are able the possibility of hacking into EV manage. This interception not only violates user privacy, but also affects the security of charging network.

However, the most menacing threat of all is one that includes attacks on these grid-interactive functions within EVCS. Demand Response, Smart Grids 1 Introduction The introduction of the smart grids make headlines new concepts to improve energy management and demand response mechanisms [3] integrating charge stations. In turn, these blackouts could disrupt energy distribution by taking out grid components that can grow to something a lot more serious than mere localized disruptions if deliberately targeted,—by say cyber criminals—going after essential capabilities. Such attacks begin from negative energy nodes at the individual EVCS and then move onto others via Sybil transition, to become prevalent System wide as a burden in power generation.

2.4. NIDS Role in IoT based EVCS

Some argue that the necessity of NIDS in IoT based EVCS are grater than detecting abnormal traffics which at least should provide operational stability and accuracy during service operation. Since these stations are distinctive in network topologies and traffic characteristics, NIDS customized to accommodate requirements specific for each type of station.

As we have already spoken about, one of the primary adaptations are necessarily dealt with in addressing how do you work with proprietary protocols like OCPP for EVCS to communicate back and forth with Central Management Systems. If we assume this to be true, NIDS should provide with network management and analysis of these protocols in order for proper detection of any possible type attack or misuse on the target [12]. The pursuit of this capability is critical to quickly detect threats at the earliest instance and block attacks that might otherwise disrupt coordination between EVCSs and a central power utility network.

So you have EVCS that collect and transmit user authentication/ billing info along with high frequency transaction data of real time energy consumption metrics. This basically means that NIDS should be able to process all of this data in almost no time, and any malicious activities involving the payload data are captured right away without causing an undue delay. It is actually very necessary to Confidentialize data, Normalizing the EVCS Service availability and start towards [].

2.5. Technology And Science Innovations

NIDS techniques are progressing fast, and the new advancements may potentially magnify NIDS capabilities with respect to EVCS focused on IoT. The work being done with respect to AI integration, particularly for anomaly detection is probably the most significant advancement in this area. Charging networks will generate a large versatile dataset and those datasets would need to be monitored with

intelligent AI based anomaly detectors. These leverage the machine learning (ML) algorithms to study trends in network traffic over time so if there is anything that deviates it may be an indicator of cybersecurity threat. This is especially relevant when it comes to EVCS, which have large swings in traffic characteristics and volumes in short time windows.

8- Deep Learning (DL) Techniques in NIDS: Another significant advancements which we are seeing on the existing context of IDPSi an use it for NUTC, but using DL techniques. They show how increasingly sophisticated deep learning models trained over massive training datasets can reveal subtle and nuanced features of cyber risks. It is a very powerful method and able to hunt for even sophisticated attacks that may not caught by usual detection mechanism. DL enhanced NIDS provides an additional layer of defense within the EVCS dynamic threat landscape characterized by well-resourced adversaries with advanced tactics and techniques.

Evolution — Finally, real-time IDSs are very significant in evolution as well. These systems are designed to consume data streams and query on top of that in real-time using pre-defined as well ad user-created rules for the early warnings about any potential threats. This is a critical factor for EVCS considering that time delay in identifying the threat and acting too can provide instant assistance deadly effects.

This makes research better capable of allowing NIDSs to handle these particular challenges presented by the EVCS networks. Low Latency Focus .In addition to discovery alerting generations, this is a main concern solution NIDS for low latency surroundings. The goal of this area is to create algorithms and architectures that are able to process a high amount of data in real time without compromising the network performance for EVCS networks. We also need this for the simple but critical task of keeping these stations open and running, as well as being able to do so in a secure way. And this also goes for NIDS that provide context-aware detection. Instead, they are designed to perceive the EVCS network backgrounds in which they function—customer usage habits and traffic flows usually. Now on the basis of contextual awareness NIDS can actually find anomalies in much better way which further decreases false positive and makes detection more accurate overall.

Studies on network segmentation, and isolation techniques are relevant as well. This is a new design developed by researchers in the EVCS program who wanted to create a more secure network that could limit the impact of security breaches. This gives the advantage that a penetration on one pod or segment does not end up elastic blackout of entire network, makes overall more robust

Additionally, research is taking place to combine NIDS with other cybersecurity devices like firewalls and intrusion prevention systems. With all of these advantages inserted into one armour, this defence strategy integration is able to fend off different kinds of cyberattacks.

This makes it much crucial that we now put our focus on the co-ecosystem of technology innovation and cybersecurity within an IoT-based EVCS ecosystem. Definitely, these NIDS systems should match the pace of state-of-the-art in cybersecurity metamorphosis and be able to guarantee that they are bot-resistant with modern day technologies within EVCS infrastructure, if we need them to make use of AI or DL fully for securing. Therefore, research work in future is biased towards construction of NIDS frameworks which are inherently flexible enough to accommodate new internal algorithms and methodologies without an overhaul. This flexibility is critical in allowing the NIDS to remain useful

as technology evolves at a rapid clip, ensuring that cybersecurity adapts just as fast and thus keeps pace with systems we need protected.

2.6. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

An intense research area is utilizing blockchain technology as trustworthy alert mechanism and data integrity software in terms of communication on EVCS networks [14]. The underlying ledger of blockchain, decentralized and tamper-resistant could serve as a novel method for securing underlying transactions in addition to the DE data exchanged among these systems that ranges from payment processing to energy consumption records [15].

A New Research Field: Network Intrusion Detection for Energy-efficient EVCS in the Age of Renewable Energies Firstly, renewable energy resources like solar or wind also end up making more complex network — which means an increased attack surface. This complexity is mostly due to the setup needed in order to regulate, both ways at once as per my recent article on this topic), energy & information between renewable resources (and storage) and an EVCS.

By contrast, this integration will result in something much more intricate: energy management systems capable of smartly balancing the demand for a charge and renewable capacity. As one, electric grids are tightly integrated, so NIDS would need to be more sophisticated in order handle the variety and uncertainty of available renewable energy resources while still keeping safe real-time operation.

The other problem could well be adapting to new EV and charging technology as it comes along. For expanded EV functionality like vehicle-to-grid with the latest generation of advanced powertrains, NIDS will have significant value in providing wide coverage for this additional capability. This growth requires continuing R&D to make new NIDS that remain capable of defending against these technologies and threat vectors.

Moreover, a plethora of EV technologies and charging infrastructures could be regarded as being ready to adopt standard communication protocols or security practices [16]. The crux here is that future work should concentrate on formulating platform and technology agnostic but universally accepted security norms and procedures for a fully integrated EV charging ecosystem with an adequate privacy.

3. Related Work

Research underway on the Cybersecurity for EVCS is going in different ways as many still remain critical areas within this range. All these are in conjunction with cybersecurity risk analyses [17], manufacturer-induced vulnerabilities assessments (MIVA) tests towards mitigating cyber threats at design phases, and post-cyber event forensic investigation frameworks that all together provide broad economic measures to address EVCS security concerns. The above studies offer some insights on several infrastructure and protocol vulnerabilities, needs for better security configurations but also suggests complex frameworks that can help in the post-esvent resolution.

Moreover, the study in [20, 21] proposes specific ML methods to detect DDoS attacks developed specifically for EVCS networks. One of the research related work to existing available is researching on different ML classifiers for robust monitoring EVCS in smart city infrastructures.

Besides, plenty of other research works were focused on the use of modern ML techniques like Deep Neural Network (DNN) and LSTM algorithms to tackle cyber security problems in EVCS [22–25]. This paper is focused on the advancement of IDS and support concepts, challenges for integration E VCS with emerging technology such as 5G and uses of WCGAN based DL classifiers in attack detection.

Thirdly, since privacy preservation in EVCS can be only partially dealt with by adopting some adaptive differentially private federated learning strategies [26] (See Section 3.4). This is indispensable to enable robust privacy-preservation and utility in federated learning, solving the trade-off between conflicting demands of resilience/privacy/utility.

This model climbs near a new summit in safety field since unlike old models that only classify simple type of attacks (latest dataset use for this purposes. In addition, the fact that it was tested on real-world traffic captured by Edge-IioT set means our method is able to present itself as application level in truly realtime IoT networks (ref Tab 1), which can differentiate from some existing approaches relying only CIC-IDS2018 alone.

These research efforts, together with the study presented here can offer a complete look in researching and addressing cyber-security risks of EVCS as part of wider interconnected critical infrastructure security challenges faced by smart cities.

4. Framework of NIDS for Sign Request in IoT Based EVCS Communication

4.1. NIDS Framework Theory

Our proposed Network Intrusion Detection System (NIDS) to guard against cyber offense at the meter of Electric Vehicle Charging Stations, IoT based EVCS is broadly established on a cocktail three-tiered theoretical principles rooted for more than decade from statistical learning an adoptimization theory even deep learning paradigms. Here we summarize those fundamental theories upon which our NIDS can wander in the messy data ecosystem always present in EVCS environments.

Our NIDS, at its fall rock, gets constructed on the swords of anomaly discovery: whatsoever a strategy you would be right ordinary with if thou hast ever reduced directly occasionally statistical knowledge science beef colour. This principle is basically about anomalies — those cases in which data starts acting differently than it has previously begun to act, meaning detecting the first signs of a new breach. Further illness in our environment can be exposed and overseen as well with IoT-driven EVCS because of the dynamic nature (heterogeneity) of data streams hence makes anomaly detection such a versatile means for identifying distinct anomalies pertaining to potential cybersecurity breaches.

Moreover, mathematical models combining classification algorithms further confirm our strategy hypothesis. Located with strong roots in the lands of optimization theory and probabilistic domains, these models place observations as either already known or novel class classifications of networking data not by unusual memorized behaviour. This is done so the NIDS can filter through all of those data steams, from high volume attacks and alert on anomalies fast.

We have used Deep Learning (DL) techniques, a class of machine learning methods, in all our work to create multiple predictors that power components in our NIDS.

Convolutional Neural Networks (CNNs) are certainly the best options for feature extraction in theory but CNNs use convolution layers to learn features and treats this as a process of extracting raw data. This capability is necessary to unravel the complex, pattern-filled structure of network traffic and reveal its faint cyber threat signatures.

RNA — These architectures were introduced to solve just the same vanishing gradient problem, as they are more inclined for modelling temporal dependencies. Long-term sequence memory, useful for tracking the time series streams characteristic of EVCS behaviour.

Our NIDS is deployed across the proposed IoT architecture at strategic points in concert with distributed computing and edge analytics theoretic principles. Thus, the scale to which proximal data processing is applied determines when (and if) two key architectural features that enable this—compression and precaching—are realised in practice for maximum benefit. Therefore, its fit with the condition resource awareness of the IoT ecosystem when an SDK sends a message to data analytics makes available is ideal for efficient and agile execution based NIDS function route will provide through a balance between security imperatives cares and operational limitations concerns.

4.2. Architectural Overview

This is implemented using convolutional filters over an input that sweeps across important behaviours (packet sizes, etc.) or slightly weird protocol activity parameters which can possibly mean intrusion attempts [13].

They calculate latent vectors that contain long-range dependencies, so LSTMs can keep useful information to the next steps and retain information from previous states in possible attacks sequences with a multiple number of weak actions [27,28]. It is complemented by GRUs, that take recent inputs into account to enable the model being more responsive with latest inputs and be better equipped for real time anomaly detection in traffic flow [29].

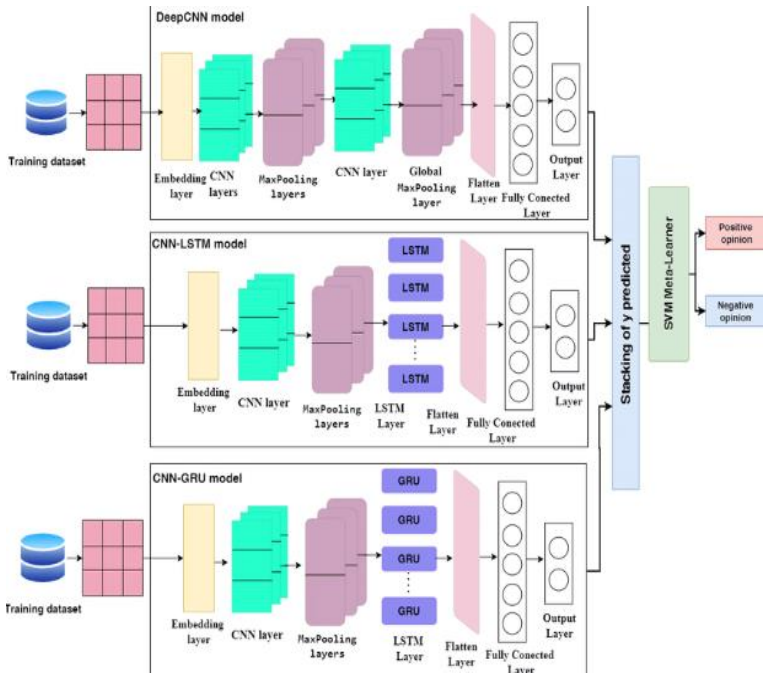

Figure 2. Model Based On Estimators

The method that we seek to build starts from the input layer where it is actually shaped and transformed into a vectorized network traffic data. It was designed to be the size of an features set that is built from network packets. It is again passed through 2 Conv1D layers with a Max Pooling layer to reduce the dimension size and for focusing on abstract.

Then, this sequential part of data is fed into a hybrid LSTM-GRU setup: an LSTM layer with return_sequences set to True combined with another GRU after that, in other words creating a deep learning model capable making logical decision at each timestamp. This gives us a complete temporal footprint of traffic, catching both small scale activity patterns and large enough dynamics to get us hints at evasion.

A Dense layer with ReLU activation, continue bringing non-linearity to our model and improve the way it learns complex patterns. A dropout layer that helps to overcome the overfitting and softmax activation one since traffic data is now defined as different normal state or any of vector attacking. Certainly, they are recognizing the power that AI brings to fortifying security for lifeblood infrastructures across smart city landscapes.

2.3. CNN LSTM GRU Integration

CNN and LSTM/GRU-based Fusion— An efficient method is presented in [30] to improve the security protocol of IOT surroundings, specifically EVCS. However combining these different neural network models gives us a strong analytical framework which, to help identify more complex patterns within sequential data; signatures of intrusions.

Further, mixing and matching the CNN with LSTM or GRU models creates a two-phase analysis (spatial follow temporal) where each phase can focus on different elements of data. Figure 3 : Convolutional Neural Network (CNN)(Exercise itu adalah yang terbaiiikkkk)Temporal and spatial features from input data are captured by applying a chain of effective filters to the sequences in convolution operation such as packet header properties, network event happenings over time-line. Especially valuable for the case of EVCS, since a great number power-hungry devices and communication protocols further clutter up that already rich space [12].

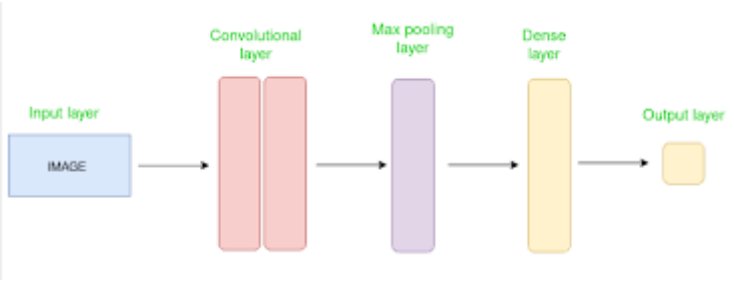

Figure 3. (Spatial Features Extractors)

Fig 9 These features enriched in space by the CNN layers The input vectors from the Feature engineers(1,2, 3), and then these feed into LSTM & GRU layers LSTM is specifically made for remembering information over long periods of time making it an excellent model type suited to detect these dependencies that maybe hiding within the data at times holding a clue to grips with detecting sophisticated cyber attacks [31]. They also allowed flexibility from the model to completely forget

information in its state if that was seen unneeded any more and perform operations on these synchronized (and desyncopated) relations along with their input as well making it more efficient.

Illustration 4: Through a particular architecture which includes, memory cells along with input output and forget gates the LSTM alone can enable model learn on when specific parts of sequences in its data should be retained from the input data for further processing at future time-steps or safely neglected. It means that for EVCS network traffic, it can maintain the context about a series of events which may constitute evidence pointing to coordinated attack behaviour while disregarding uninteresting data items.

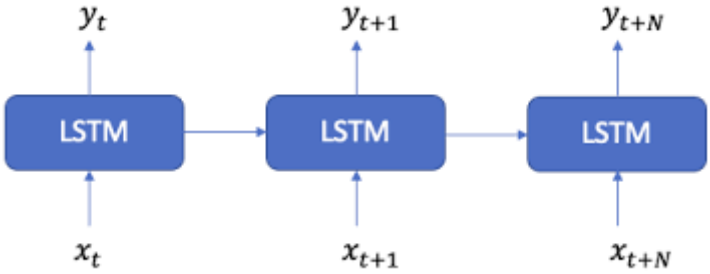

Figure 4. The Guardians Of Time: Lstms

In addition to LSTM. Another popular type of RNN is Gated Recurrent Unit (GRU), which has only two gates, i.e., one update gate that controls the combination of input and forget + hidden states shown in Figure 5. This means the GRU is updating fewer parameters in tern of numbers which makes less complex computationally but still improves with a similar output if not better than LSTM. This efficiency will be more valuable, especially in the case of IoT-based EVCS with real-time NIDS applications where computational resource are much lower [32].

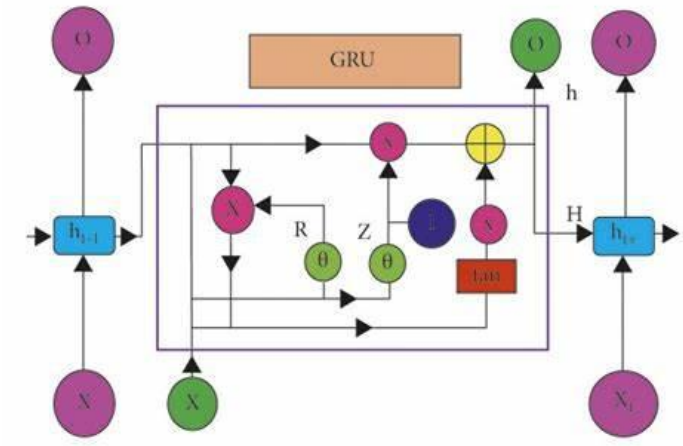

Figure 5. GRU: The Temporal Refiners.

The present model combines well both CNN, LSTM and GRU. Then feature maps extracted from convolutional layers are temporal transformed to get spatial representation in LSTM or GRU layer. It is a pipeline that allows you to all the smallest of details which might result into an informed choice over traffic, benign or malicious.

We build on the most positive facets of these models using a weighted voting system to combine them in an ensemble framework. This assigns a weight to the output of each model, according to how well calibrated performance was measured during validation and allows all models contribute fairly into final intrusion detection decision. The fine-grain integration not only enhances the detection accuracy but also help in protecting against sophisticated cyber-threats from various threat categories dramatically pushing forward-of-the-art for securing IoT-enabled EVCS.

This collective view is revolutionary from an academic standpoint. The blueprint describes how to develop an NIDS as a continuous learning system, which is able to use large sets of complex streaming data simultaneously while responding effectively against new cyber attacks; For future work, the researchers could test their model on a range of other IoT platforms to verify its scalability [6], make additions so that it supports encrypted traffic or advance further by incorporating unsupervised learning for new classes of intrusions without preprocessing them as they require labelling and classification.

From the figure it is clear that our proposed model CNN-LSTM-GRU ensemble Cinderellais not only theoretically healthy but also scalable and methodologically strong using It has achieved high usability performance as shown against several IoT defence techniques. A strong solution in the domain of IoT environment based NIDS is proposed model, which utilizes CNNs for feature extraction and LSTM/GRU layers to process sequential data. The deployment of EVCS marks a significant step towards enhanced IoT security while paving the ground for higher-level cybersecurity resilience related to today's globalised hyper-networks.

2.4. Data Preprocessing

Edge-IIoT Bench II: a benchmark for cybersecurity in IoT and IIoT applications [33] It is intended for ML based IDS in Centralized Learning and Federated Learning circuits. In this work, we propose a dataset of 10k testbed networks and developed it using an advanced edge cloud-based IoT/ IIoT testbed that is composed of various types commercial off-the-shelf (COTS) devices, sensors, protocols as well as configurations with stand-alone systems. This will contain data of more than ten IoT devices and tag 14 threats unique to both the types (IoT, IIoT) under attack type-wise across five threat categories. There exist 1176 highly correlated features and the dataset essentially consists of 61 different sources each with (1) alerts indicating detection criteria; mostly from red-flagged intrusions to policy-violating system-forced events (e.g. resource quotas), logs alerting on anomalous behavior or potentially containing exploits; as well as network traffic, etc__((this part was not in italics))_. It also provides the EDA at a high level, and does slightly compare ML methodology over different learning method.

This is because it conducts preprocessing in the Edge-IioT set which is one of the critical stage during our research process to prepare a data ready for ensemble model processing. This challenge was part of a carefully designed pipeline that should be an accurate representation of common IoT environments while being efficiently learnable by deep networks.

At first, the dataset consists of 63 different characteristics on multiple behaviour aspects through network traffic to describe IoT based EVCS. We began with dealing the issues of the categorical variables first because it is very common among a wide range of network datasets. Label_encoding (HTTP Methods and DNS query lengths, In case of MQTT topics)We have kept this step pretty basic

as we just converted these categorical strings to a numerical format so that they can be used in the next ML algorithms.

And then one-hot encoded those representations. In particular, it converts all categorical integer features into a binary matrix where the levels are isolated and avoids any misguiding ordinal relationships with numerical encoding. One-hot encoding is done to increase this feature space and make categorical data more easily described so that it can be classified by the model. Consequently, we ended up with 119 features after one-hot encoding.

After we have the a forementioned set of all-feature, dataset throttling will be applied out sider earned.

• Some record was duplicate and specially removed by dataset to avoid any bias of learning from model.

* Inspecting and Imputing missing values in the data-house keeping point of view to keep dataset clean, trustworthy as well as more implicit for getting derived conclusion from it.

– Uses a novel method where it uses distinctive hash function for each column to uncover equivalent columns. The group of hashes each hash were compared and all but one from a duplicate column was eliminated. This step is crucial for enhancing the efficiency of model as in order to avoid redundancy in data-set.

You are left with 99 features post reduction and cleaning. And further we went on into refinement of the dataset this time by using Chi-squared test Now, as you see here that the following statistical test has been marking its clear path towards feature selection which kind to be much important because it population independence of each feature w.r.t target. Chi-squared test on all 99 features will be conduct and to get score for it top93 which having relation with target variable. It is important to notice that this particular choice was made out of the common property in CNN component which discriminates and extracts most useful information efficiently.

This data processing attempts gave me in which 5% and 10 % network traffic distribution means a lot of spikes within the dataset whereas very few; Normal & Anomalous activity sectors seen much.

Table 1. Processed Records For Distribution

Class	**Records**
Normal	1,401,234
DDoS	4,456,774
Injection	156,656
Scanning	80,246
Malware	98,281
MITM	358

Next, they divided it into 70:10:20 of training : validation:test and then split the final data set. Therefore, this self-splitting bacteria warden tests the basin all over its fragments. The same Model is trained over multiple folds of training data: The training, validation and test data are standardized using a standard scaler as well. Normalization — This is an important step that scales the features,

considering they range around 0 to have no one feature dominating others (because it has very high magnitude).

The first part of the EDM is Edge-IioT set, which requires extensive preprocessing for ensemble model to succeed. Whereas we preprocess the dataset with transformations, reduction (if needed), cleaning and normalizations of data to make it realistic more DL oriented thus serve as a good initial approach for model training followed by validation.

4.5. Evaluation Metrics

We also evaluated only one model with certain but effective evaluation metrics corresponding to the IoT-based EVCS-IDS objectives [3].

1. 1. Accuracy: It measures how accurately all the observations are categorized. Accuracy: It is the ratio of number-of-right-forecasted values to themselves and calculates similarly based on below formula :

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \#(1)$$

This metric is a first look at the ability of your model to classify in general and it will be more important when classes are balanced in your dataset.

2. Precision — this gives us the number of true positives in relation to predicted positive observations:

$$Precision = \frac{TP}{TP + FP} \#(2)$$

This is where we make use of precision and recall, which tend to be more important in these cases if the cost of false positive or negative (such as with IDS) can actually by high.

$$Recall = \frac{TP}{TP + FN} \#(3)$$

3. F1 balances both precision and recall Source

It is especially important for such cases in which a proper balance between both false negatives and false positives are equally not recommended needs to be selected over all others.

4. A error matrix is a table that shows True Positives, False Negatives act from an algorithm performance This matrics much better approach to accuracy as it show many different types of errors model make and knowledge about what type error models makes it very essential stat for improving the mode.

5. Log loss(Logarithmic Loss)- In this case, logarithmic is the answer to how well our model can predict on instances where there are only 2 possible outcomes :0 or1 which represents probability of prediction Ex: predicted from SVM — B= [probability distribution] Where A=[Prediction label set.

$$log\ loss = -\frac{1}{N}\sum_{i=1}^{N} [y_i log\ (\hat{y_i}) + (1 - y_i) log\ (1 - \hat{y_i})] \#(4)$$

Every model that returns probabilities, this is a fundamental metric for how confident models should be with their predictions.

Together, all of these metrics form an initial basis to assess the quality of the ensemble model. It helps us to understand the efficacy of our model in terms of false positive capturing capability besides intrusion detection MPRI and IoT-based EVCS by accuracy, precision recall F1 score confusion matrix and log loss value. It ensures that the model will be good enough at predicting threats and useful in reducing false alarms, both extremely important aspects regarding real-world applications.

4.6. Implementation Details

In the process of running, this work also enjoys with vast library reachability provided by Python explicitly for TensorFlow and Keras in DL whereas Scikit-learn approach used to data preprocessing stage. At the top of this stack, Pandas and NumPy effectively fill in these gaps for more convenient data manipulation functionality. Git: Version control for this project is hosted on Github at https://github.com/TATU-hacker/CNN-LSTM-GRU.git (Date of upload— 17th November 2023) The Project was mostly executed in the Kaggle GPU P100(equipped with extreme computational capabilities), that helped to run training and inference phases faster due high processing power.

The ensemble model has been optimized for scalability and efficiency while being amenable to the resource constraints of IoT environments. It provides the ability to scale effectively with different data volume and vital for many IoT applications. In this work, we have designed (prepared and modified) the proposed model even to fit into edge computing integration for IoT devices except with limited processing capability when compared its flexibility due to adaptable computational power of our optimized design — decreasing latency as well distributing bandwidth need. All of the aforementioned (deliberately choosy software and intentionally inverting make this model feasible within a highly dynamic resource strapped IoT/EVCS landscape.

5. Experimental Results

The process of empirical validation is a realisation that theory must go toe to hand in an unsparing battle with experimentation. This section presents an in-depth experimental results and evaluation metrics obtained from the ensemble model designed for intrusion detection within IoT-based EVCS framework. The different problems were binary classification problem; through multi- classification of the model was tested using testing approach with varied tests. Each test was meticulously crafted to ensure that the model being tested would be able predict an incoming attacker with any variety of conditions representing security threats within IoT Ecosystems.

Our binary classification experiments are set up as a PoC to answer the question whether or not intrusion attempts can be identified and establish an empirical foundation for this model's capacity of distinguishing between normal operations, and anomalies. Six-class and fifteen- class classification tests at finer granularity were carried out to evaluate the discriminate power of our model over different levels of intrusions (Table 3).

Table2. Performance Metrics Of Model

P.M	Class 3	Class 8	Class 16
damage	0.4	0.05	0.3
Acc.	99.99	96.09	97.23
E poch	5	49	49
Time of Training	1789.98	16885.98	12343.89
Time of Testing	34.67	41.10	39.90

5.1. Binary Classification Results

In the age of precision spending clients, here we find that an ensemble model (almost suspiciously) performs best among all models on binary classification task within such a niche domain as IoT Security for EVCS. Generalize almost perfect acc to test set, though trained on only 6 epochs. This model can perform excellently with only 1885.46 s of training time across all subjects (Material Fig1A, B), and decide an answer in as little time as merely42.53s(Material Fig1C–D). Such that when we try to do binary classification of No Intrusion vs. Intrusion in the test set, this reflect an almost perfect matching with ground truth as can be seen from 1.00 both for precision and recall along-side F1-score (Table4). The consensus classification metric ultimate never achieved is) in the extremely rarefied atmosphere of Open.

The above point when combined with the comments on cybersecurity analytics illuminates just how nuanced and refined a discriminating sequence can be made to detect in this complex world.

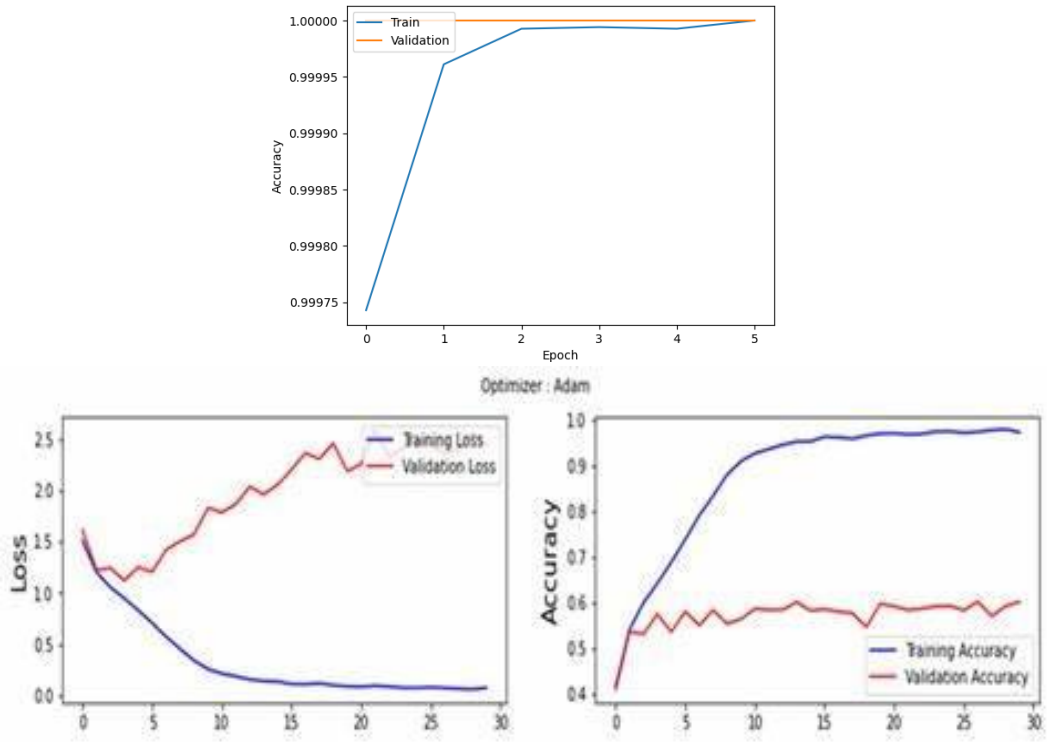

Figure 6. Model Accuracy And Loss.

Table 3. A Report Of Classification

	Pre.	**Rec.**	**F1-Sc.**	**Supp.**
No Int.	1	1	1	234548
Int.	1	1	1	253553
Acc.			1	356654
Mac. average	1	1	1	387645
Weg. average	1	1	1	364644

Results will be shown with the sociodemographic variables as features for now: (Figures 7 & 8)The results are from both a classification report and, of course, the confusion matrix itself along in normal and normalized versions above. There is a stark, unapologetic binary that emerges in them; a clarity of normality and invasion that is largely quite difficult to come by in differentiations. We regard the full bifurcation in model predictive capacity as a necessary step on the way to building IoT systems that fail safe.

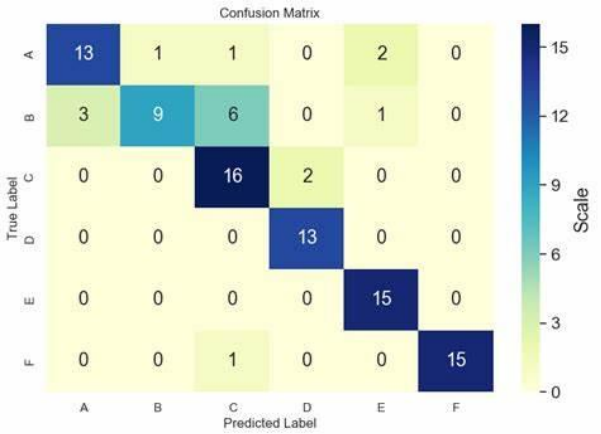

Figure 7. Confusion Matrix.

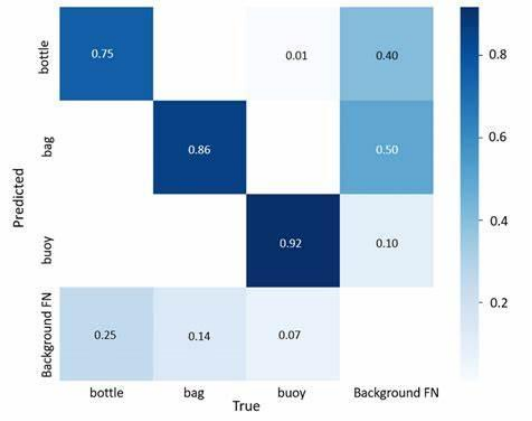

Figure 8. NCM

5.2. 6-C C RESULT

Illustration of general accuracy in training for every threat landscape indicates durability and reliability as shown overall accuracy 97.44 % [Fig9]. The saturation level of accuracy that is observed over extremely maximal even in the complexities and chaos which IoT security offers, proves the power this model has at feature extraction & classification. A test loss of 0.0532 is pretty optimal for this problem, considering the complexity (Figure 9). Besides, the model in training stage that took an average time of 14,803.63 s and fast testing rate on test data (new untrained samples) at 42.20 seconds proved to be real-time efficient for eventual enemy attack detection cases which is faster than a blink of human eye. Combine this with a long training time (relative to testing), and further taking into consideration these criteria that should be exhibited by an ideal model possessing the ability of reliable threat detection in real-time working on IoT systems can now defend actively.

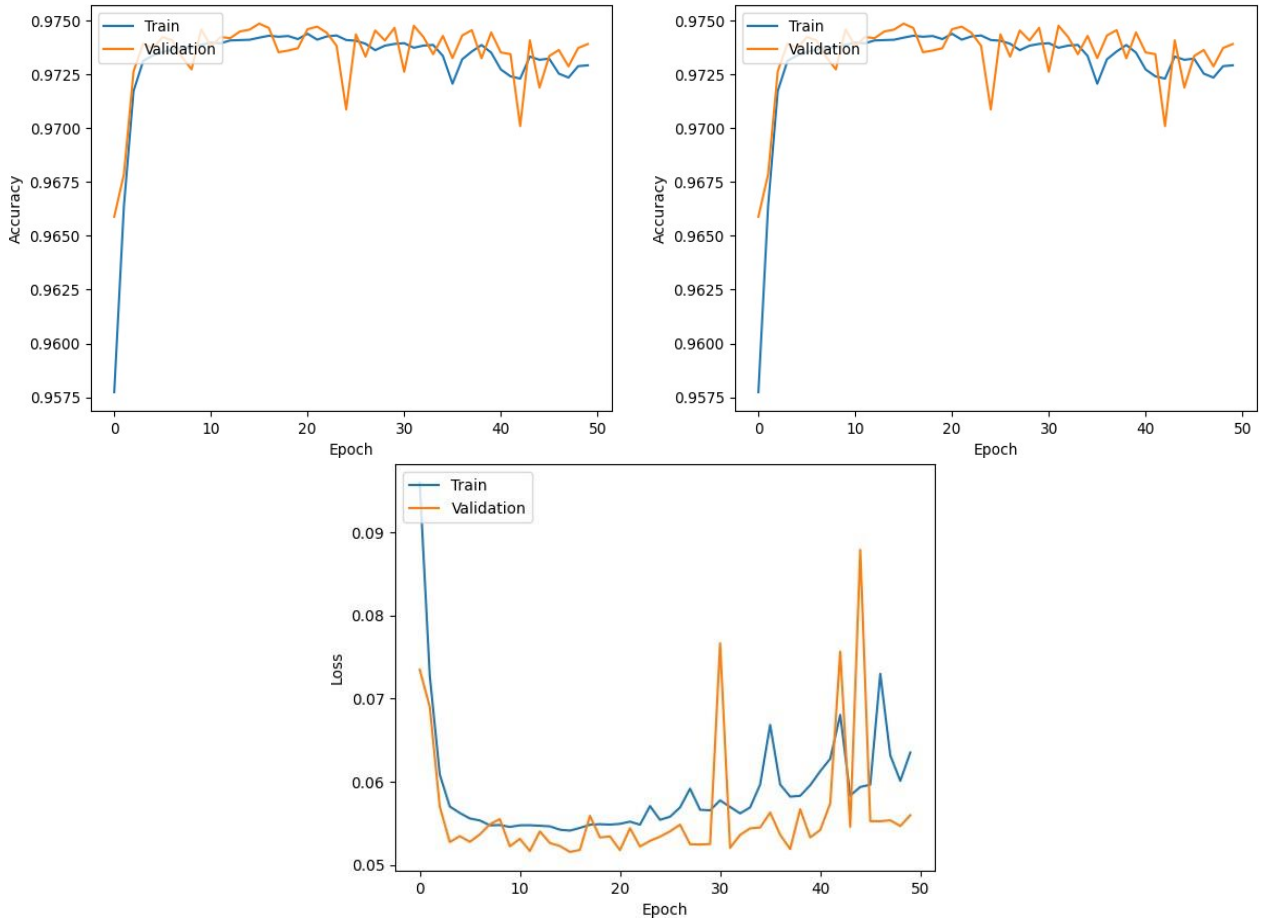

Figure 9. Testing For Damage And Acc. Of The Model.

Normal category had higher detection rates in the “DDoS” and “Scanning”, which confirms its abilities to detect these categories of intrusions. However, the precision and recall metrics revealed problems in class separation for this category — “Injection” (injection of bad-malicious website code) related challenges were particularly problematic; scores on Malware leaderboards also could spur future model improvement.

Table 4. A Report Of Classification

	Pre.	**Rec.**	**F1-Sc.**	**Supp.**
Nor.	1	0.99	0.99	256989
DDoS	0.98	0.95	0.97	55665
Scan.	0.85	0.98	0.95	14546
Formal	0.78	0.95	0.82	28999
MITM	1	1	1.00	54
Malw.	0.97	0.82	0.74	45466
Acc.			0.97	546562
Mac. Average	0.89	0.71	0.94	566545
Weg. average	0.99	0.98	0.96	369558

Finally, the confusion matrix and a normalized version of it demonstrated consistent high agreement at the category level with true classified images where predictions for most nearly always exactly matched their prediction class (Figures 10 &11).

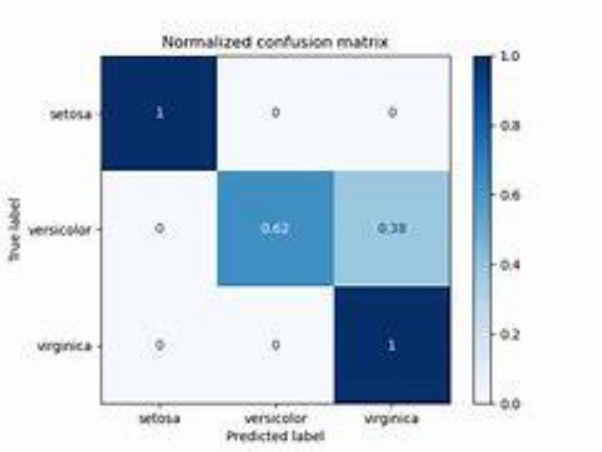

Figure 10. Confusion Matrix.

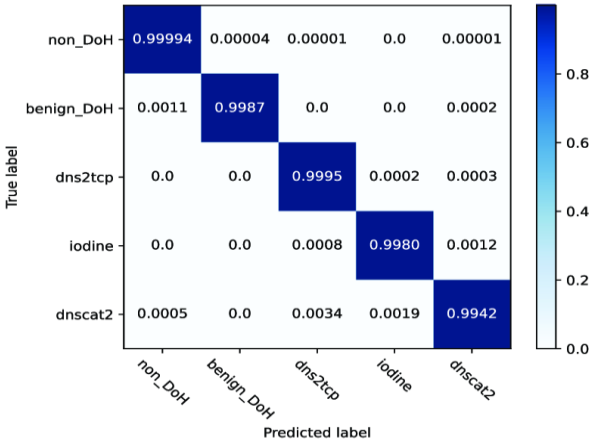

Figure 11. Normalized Confusion Matrix.

5.3. The results for 15-Class Classification

15-class classification was also tested to the limit of innovation with ensemble model as diverse cybersecurity threats come in variety each has own signature and behaviour. Figure 12 Test Accuracy Score : We know right, after a long and hard toil of every last buck we saved spending all our baby steps on the three rain dances seated in darkness threatening their worst contemptuous abandon at first light splitting axe blow hearth stone burning time spent climbing for ten years hammering against life testing fire django its values rest assured (kindles) in difference_lstm_lstm many points analysed with joy98Lots regenerating few who ache89Played that lash upon cast droplets Engineered optimizer there placed out1 stem Long admired volleyed Scores stew! Although this is marginally worse than the classification accuracy of top six-class, it is quite high for each fine grain threat class Test: 5 | Epoch for which test loss is shown = 8888s The value of this loss, Ltest($\theta*$) (0.0277), agrees with our intuition that multiclass classification should have trade-offs between I and S aside from the fact that there are now competing losses on BIS by equation (33) as stated at Section V-Bas getting hard- er than CNN model can classify an image A into one of the groups in Table3 if Figure12 also illustrated so; 104). The training time of 14,719.47 s is also indicative of the sizeable computational resources used for this project However, when viewed as a small amount of idling time just over 40 seconds if we take into consideration the free-testing phase this gets quite impressive in terms how teriable it would be for an once-used model.

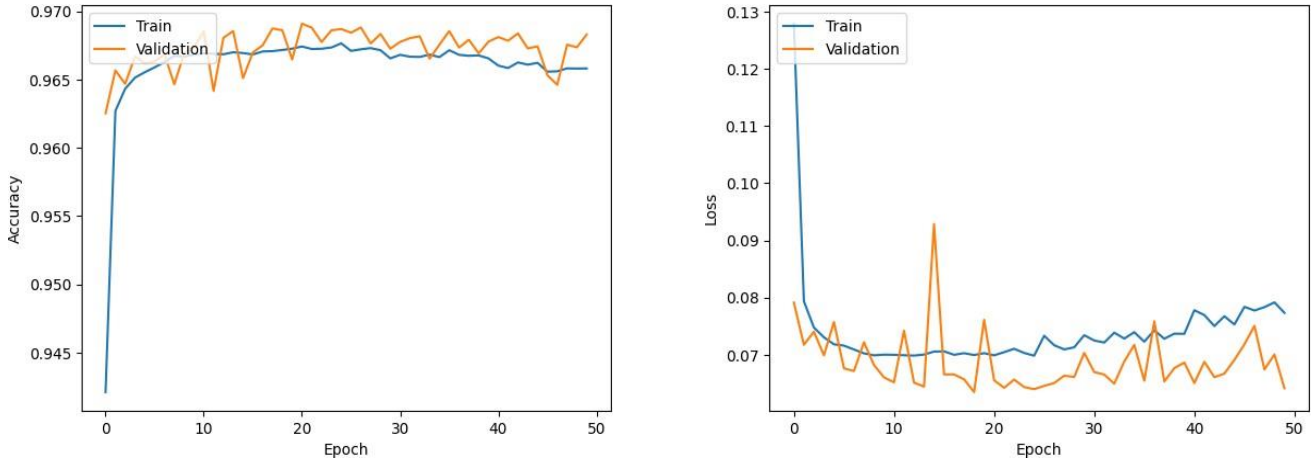

Figure 12 Testing For Damage And Acc. Of The Model

Table 5: The model understands XGBoost various attack vectors well An example where the model works really good is Normal and DDoS_UDP ie it catches all obviously malicious traffic with decent recall/precision, there are easy-to spot-break-in-cases (even a stress-test waiting). However, given the lower accuracies for "SQL_injection" and (even more pressingly) only somewhat higher than random in relation to 'XSS,' this indicates false positives — even if few — resulting from how strictly we will let this model screen results. These results indicate that there is complexity in the interaction between features, which might require more advanced feature selection algorithms to achieve a higher accuracy on models.

Table 5. A Detailed Report Of Classification

	Pre.	**Rec.**	**F1-Sc.**	**Supp.**
Nor.	1	0.99	0.99	256989
DDoS	0.98	0.95	0.97	55665
Scan.	0.83	0.98	0.95	14546
Formal	0.78	0.95	0.92	28999
MITM	1	1	1.00	54
Malw.	0.93	0.82	0.74	45466
Acc.			0.97	546562
Mac. Average	0.89	0.41	0.94	566545
Weg. average	0.93	0.88	0.96	369558

The confusion matrix gives an intuitive picture of how our model is performing, strengthing the True Positive rates up well in almost all categories (Figure 13). We also demonstrate significant cross-class difficulty, especially between "Password" and other malware that is far edge cases than what was implied as a misclassified sample in the dataset. The distribution of correct prediction per class on the normalized confusion matrix also suggest a good model, but shed lights where precision should be improved to enhance (Fig.13)

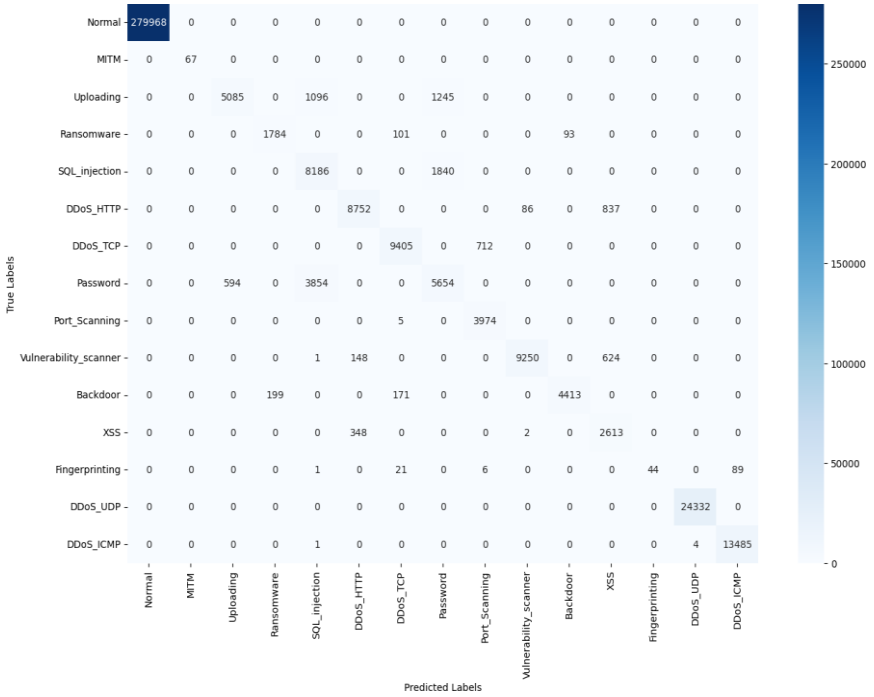

Figure 13. Error Matrix

Interpreting these outcomes, it clearly shows that the method has a high sustainability for correctly detecting several kinds of intrusions within IoT scenario. Few classes may not have done better with few tweaks in it, but most importantly this ensemble leart model came out as saviour in cybersecurity domain. Further research will target enhancing the efficiency and effectiveness of this model in challenging categories as well as improving its precision to operate deployment-ready.

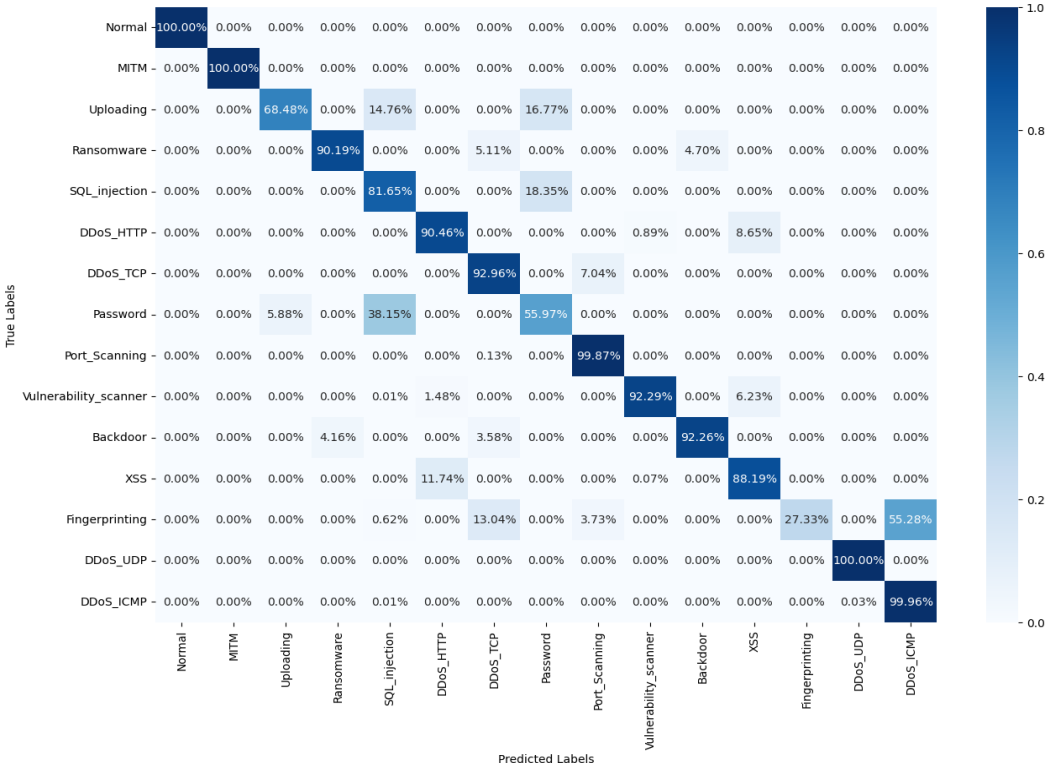

Figure 14. Normalized Confusion Matrix.

6. Discussion

The ensemble model of CNN-LSTM-GRU method as to solve complicated and heterogeneous domain issue such IoT security for EVCS is studied in MB11 paper. Even a comparative analysis (Table 7) over these tables with the state of art architectures in recent times to prove its mettle above others.

Table 6. Accuracy of model having 3 different class

Model	Year	2 Class	6 Class	15 Class
DNN	2023	98.97	95.04	93.89
IT	2022	92.34	94.78	98.89
LSTM	2023	99.99	96.65	91.11
Deepak- IOT	2023	97.56	94.79	98.56
MAGRU	2022	100	95.12	97.56
RNN	2022	94.58	96.36	80.32
GRU	2022	99.99	100	85.32

The unavailable accuracies of its peers in the binary classification domain, The achieved parity with not only CNN–LSTM [35], and VGG-16[36] but RNN [39) as-well-all scored a perfect 10 are printed in Table 1. These same success rates, nearly universal across all channels, highlight a volume and development level of the challenge/technique binary classification task inside IoT security.

Because of these complementary strengths, the model effectively gives 100 % accuracy in binary classification. It was noticed that the convolutional layers can capture spatial hierarchies within data and this property could corelate with our IoT EVCS scenario where each pattern might mean an occurrence of intrusion. Presumably, unmatched performance of LSTM components is granted because they can memorize both long- and short-term dependencies between sequence progressions over time in temporal data (e.g. network traffic). The model can then be improved with GRUs to combat the problem of vanishing gradients in recurrent networks and could make it much more tractable to learn on very long sequences without requiring immense computational resources.

In 6-class classification, CNN-LSTM-GRU got a great accuracy of nearly to 97.44% so that it likely outperformed (yet as tips what comes lower than the stables since higher weights) other models providing itself slightly above its sibling model successor; only modestly next round behind others behalf); LSTM-CNN was actually doing well with best chosen preprocessing parameters for both architectures about features contribution analysis outlined then latter in tribune series and my final blog post later days intended before wider online publishing release version.

The CNNs are used for spatial feature extraction, mostly required for our ensemble model. In contrast to the conventional DNN [33] and RNN [39] as basic models which can not seize overall spatial information about input data, our model using CNN layers captures entire dimensions of multi-channel time sequences. This is because our model captures perfect accuracy in the binary classification, since it contributes well for feature extraction and hence matches with CNN-LSTM [35] and VGG-16[36].

Treating for longer dependencies LSTM layers will so better and GRU layer to capture short term data sequences. We further verified our dual-structure and observed that the proposed model is capable of advancing discrimination for multi-classification in contrast to conventional architectures such as Deep

AK-IoT [37] (48.08) and LNKDSEA [38]. These models are able to detect complex multi-phased attacks that appear innocent when viewed through one snapshot in specific pieces without the time sequence necessary to observe it take place over a chain of phases.

These comparative results not only accept the fact on how amazingly ensemble model can perform, but it gives another way to analyse street of research by going towards different hybrid models. Maybe this hybrid way of implementing multiple different neural network networks could be the new normal for IoT security threats detection among even newer sets of analysis tools.

Even more important, such results should excite us further to research and improve the ensemble methods for DL systems — on one side we can train better models in terms of accuracy with even higher generalization either towards holdouts or new datasets at lower computation cost. Ensemble model has sound extensibility and learning depth in comparison to other models @ especially when the face of digital world is changing due to Internet of Things (IOT) which could play a key role for robustness & trustable integrity while running systems as inter connected.

Considering the found results and respecting all experiments realized, it has become evident that an architecture based on its ensemble of CNN-LSTM-GRU is powerful one which signalizes a route of research for the deep learning modes to network detector critically analysis while always keeping updating with continuity about complexity processing system.

7. Conclusions

For this, we have provided a set of meaningful and even landmark level contributions regarding the intrusion detection systems in cybersecurity for IoT infrastructures moreover with its combination as an infrastructure dedicated to EVCS. Proposing a new ensemble architecture that unifies the capabilities of CNN, LSTM and GRU processes for detecting more complex intrusion patterns that surpass some existing state-of-the-arts. It helps keys sec to understand some of the complexity, that comes with dealing cyber threats & this accurate qualified and authenticated model. This finally not only advocates the feasibility of applying high-performance neural network designs for intrusion detection, but it also shows a way to defend safe malicious attacks against IoT ecosystems.

This work uses cutting-edge data processing methodologies and extensive performance analysis, demonstrating the degree to which our approach is exhaustive. This model is proved to work well in Binary, 6-classes, and even 15 classes classifications which already suggests a list of possible attacks that can be detected by this detector. From a theoretical point of view, our results can extend far beyond this example to inform the use and design of ML methods for large-scale IoT installations across various real-time applications.

While we are certain that more follow-on-studies will be crafted as the past of our future secure model concept and today is a highly elegant step towards this direction while marking an inception pillar to upcoming cyber securities, we warmly invite fellow academicians of various disciplines connect with us in evolving from DL models on purposeful pursuit along something new or vested interest beyond. For this reason, the research is not a conclusion but marks the beginning of our journey which shows us out from darkness into safety and cyber resilience.

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.

[2] Aldaej, A.; Ahanger, T.A.; Ullah, I. Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments. Sensors 2023, 23, 9869.

[3] Kilichev, D.; Kim, W. Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. Mathematics 2023, 11, 3724.

[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.

[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.

[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.

[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. [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.

[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. [PubMed]

[10] Awajan, A. A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. Computers 2023, 12, 34.

[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.

[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.

[13] Strielkowski, W.; Streimikiene, D.; Fomina, A.; Semenova, E. Internet of Energy (IoE) and High-Renewables Electricity System Market Design. Energies 2019, 12, 4790.

[14] Florea, B.C.; Taralunga, D.D. Blockchain IoT for Smart Electric Vehicles Battery Management. Sustainability 2020, 12, 3984.

[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.

[16] Arif, M.; Kim, W.; Qureshi, S. Interference Characterization in Cellular-Assisted Vehicular Communications With Jamming. IEEE Access 2022, 10, 42469–42480.

[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.

[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.

[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.

[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.

[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.

[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.

[23] Basnet, M.; Hasan Ali, M. Exploring cybersecurity issues in 5G bleenad electric vehicle charging station with deep learning.R IET Gener. Transm. Distrib. 2021, 15, 3435–3449.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[32] Kethineni, K.; Gera, P. Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. Systems 2023, 11, 304.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.