A Secure Hybrid Deep Learning Technique for Anomaly Detection in IIoT Edge Computing

Bharath Konatham, Tabassum Simra, *Student Members, IEEE;*
Fathi Amsaad, Mohamed I. Ibrahem, and Noor Zaman Jhanjhi, *Senior Members, IEEE*

***Abstract*—The IIoT network involves smart sensors, actuators, and technologies extending IoT capabilities across industrial sectors. With the rapid development in connected technology and communications in industrial applications, IIoT networks and devices are increasingly integrated into less secure physical environments. Anomaly detection in IIoT is crucial for cybersecurity. This paper proposes a novel anomaly detection model for IIoT systems, leveraging a hybrid deep learning (DL) model. The hybrid DL approach combines Gated Recurrent Units (GRU) and Convolutional Neural Networks (CNN) for anomaly detection in IoT edge computing. The proposed CNN+GRU model achieves a notable 94.94% accuracy, underscoring the importance of careful model selection for IIoT anomaly detection. The paper suggests exploring XGBoost with hybrid CNN+GRU architectures as a future direction for high accuracy in complex IIoT contexts. The Experimental results indicate a 96.41% accuracy, excelling in metrics like false alarm rate (FAR), recall, precision, and F1-score. Based on these findings, we recommend future researchers consider advanced hybrid architectures and enhance efficiency using XGBoost with hybrid CNN+GRU. This approach holds promise for significant contributions to IIoT systems' security and Performance evolution .**

***Index Terms*—Cybersecurity, Anomaly Detection, Industrial Internet of Things (IIoT), Edge Computing, Deep Learning.**

I. INTRODUCTION

Anomaly detection plays a crucial role across various domains, including network security, financial systems, and industrial operations [1]. Its primary objective is to identify unexpected or abnormal behavior that deviates from established patterns, facilitating prompt intervention and the maintenance of system integrity. As the digital landscape becomes increasingly data-rich, traditional rule-based and statistical methods [2] face challenges in effectively uncovering anomalies. The manifestation of anomalies in edge IIoT data refers to unforeseen or irregular patterns observed within data collected from edge devices. Detecting such anomalies in edge IoT data is paramount for ensuring system reliability, security, and optimal performance [3].

The dynamic scale of data generation in the digital era has propelled the ascendancy of deep learning in IoT systems [4]–[7]. Deep learning's ability to handle extensive datasets surpasses conventional machine learning techniques, rendering it apt for analysis within IoT contexts. Its capacity to dynamically generate data representations [8] and seamless integration with IoT ecosystems [9] positions it as a valuable asset. Consider a smart home scenario wherein IoT devices autonomously interact, birthing a fully intelligent dwelling [4]. This synergy has prompted researchers to explore advanced deep learning models to address the challenges of anomaly detection [10], [11].

Figure 1 shows an overview of the industrial anomaly detection paradigm, wherein IoT device-generated data undergoes preprocessing and is subsequently input into pre-trained deep learning models for anomaly identification. Recent research has directed attention toward harnessing deep learning models, encompassing Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and Convolutional Neural Networks (CNN) to elevate the accuracy and efficiency of anomaly detection. These models exhibit remarkable adeptness in capturing intricate patterns and temporal correlations within data, thus augmenting the efficacy of anomaly identification [12]. This study undertakes a comprehensive evaluation of well-established deep learning models, including CNN, GRU, LSTM, and Hybrid models such as CNN+GRU, Autoencoder+CNN, Autoencoder+LSTM, Autoencoder+GRU, alongside the potent gradient boosting algorithm XGBoost to ascertain their proficiency in detecting anomalies within industrial IoT systems [13], [14].

Anomaly detection is vital across diverse domains, including network security, finance, and industrial systems, to identify deviations from expected patterns or abnormal behavior. Within the context of edge-based Internet of Things (IoT) systems, anomalies manifest as unexpected or irregular patterns within data collected from edge devices. Detecting these anomalies is pivotal for preserving system reliability, security, and optimal Performance.

In response to the challenges posed by growing data complexity, deep learning has emerged as a cornerstone of research in IoT systems; with the capacity to handle extensive datasets and capture intricate patterns, deep learning methods are well-suited for analysis within IoT contexts. As these methods generate data representations and integrate seamlessly into IoT ecosystems, they offer promising avenues for anomaly detection. This study delves into anomaly detection in Industrial IoT (IIoT) systems by evaluating a range of deep learning models, GRU, LSTM, and CNN, as hybrid ML model variations. By comparing the Performance of standalone models and hybrid combinations, we aim to uncover their strengths, limitations, and capabilities in anomaly detection within IIoT data.

This paper contributes to advancing edge IIoT security and anomaly detection knowledge. We provide insights into their Performance and applicability through rigorous evaluation and comparison of various deep learning models. Our study enhances the existing body of knowledge by illuminating the strengths and weaknesses of CNN, GRU, CNN+GRU, and

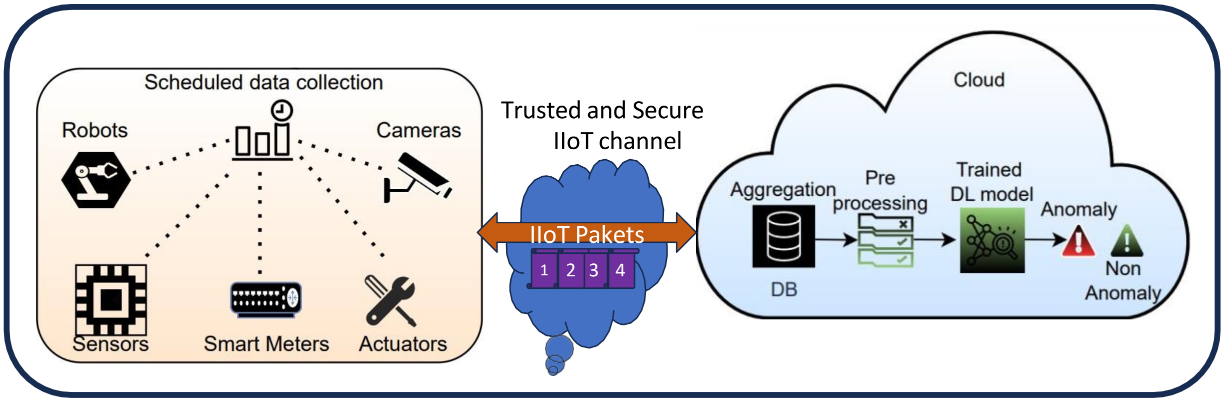


Fig. 1: Anomaly detection in IIoT Applications

LSTM models. It offers a comprehensive understanding of DL-based techniques for IIoT anomaly detection. Moreover, this research lays the groundwork for future investigations into advanced techniques and hybrid models. These models leverage the diverse strengths of different deep learning architectures, potentially leading to more effective solutions for anomaly detection in IIoT systems.

The next sections of the paper are organized as follows. Section 2 summarizes the existing research in anomaly detection in edge IIoT systems, focusing on the models under evaluation in our study. We highlight the strengths and limitations of these approaches to contextualize our work. Section 3 outlines the specific contributions our research offers, detailing the novel aspects and insights derived from our comprehensive evaluation of deep learning models. Section 4 explains our research methodology, encompassing the dataset used, the selection and configuration of models, and the evaluation metrics employed to assess their Performance. Section 5 presents our experimental setup, results, and an in-depth analysis of each model's Performance. This section sheds light on the comparative efficacy of the evaluated models. Section 6 summarizes our findings, discusses the implications of our research, and provides recommendations for future investigations, paving the way for advancements in IIoT anomaly detection. It showcases the potential of DL techniques for detecting IIoT Anomalies, offering a solid foundation for further progress in this crucial domain.

II. RELATED WORK

Anomaly detection in edge IIoT (Industrial Internet of Things) systems has garnered considerable interest among researchers due to the increasing need to guarantee the dependability and safety of these systems. Researchers have investigated numerous ML-based methods to address this challenge. In this section, we examine existing research on detecting anomalies in edge IIoT systems, particularly emphasizing the models assessed in this paper.

ML-based techniques employing CNNs find widespread application in anomaly detection within IIoT systems, offering improved capabilities to capture spatial features in IoT datasets. A data-driven fault diagnosis approach utilizing deep learning, specifically a CNN model, has been presented in previous work [15]. The outcomes of this approach reveal its effectiveness in adequately addressing local and global patterns within time series data. This capability enables efficient analysis and anomaly detection across a spectrum of IIoT applications.

A Long Short-Term Memory (LSTM) ML approach is proposed to address the training challenges in traditional Recurrent Neural Networks (RNNs) [16]. The proposed LSTM approach demonstrated higher Performance in the experiments than other recurrent network algorithms, such as real-time recurrent learning, back-propagation through time, and recurrent cascade correlation. As an enhanced LSTM-based approach, a new technique known as Encoder-Decoder architecture is introduced for anomaly detection in time series data, presenting [17]. An Electrocardiogram (ECG), leveraging DL-based Short-Term Memory (DLSTM) networks, is proposed [18]. This research highlights the effectiveness of LSTM networks in anomaly detection within time series data, demonstrating adaptability across diverse domains and datasets.

Another robust approach for anomaly detection is discussed in [19]. This method incorporates complete principal component analysis (PCA) into training deep autoencoders to enhance anomaly detection. This integration improves the model's resilience to outliers and Performance in detecting anomalies. An enhanced research effort proposes a multivariate anomaly detection technique utilizing Generative Adversarial Networks (GANs) and Gated Recurrent Units (GRUs) in their MAD-GAN framework, as outlined in [20]. This innovative approach combines the strengths of GANs and GRUs to effectively learn the underlying structure of time series data and accurately detect anomalies.

A new IIoT anomaly detection model, ESN-AE (Echo State Network - Autoencoder), is introduced in recent research [21]. As highlighted in the documentation, the ESN-AE effectively combines neural networks with Echo State Networks (ESNs), making it particularly suitable for edge devices with resource constraints. Additionally, a composite autoencoder model tailored for anomaly detection in IIoT systems is put forward in another study [22]. Diverging from conventional autoencoders, this model predicts and concurrently reconstructs input data, leading to improved anomaly detection capabilities.

An unsupervised machine learning method is introduced for Anomaly in a different version of time dataset [23]. This proposed unsupervised machine learning method utilizes a deep neural model that employs CNN and autoencoders to improve effectiveness across various real-world datasets, underscoring the potential to address anomaly detection tasks.

In [24], a network intrusion detection system designed explicitly for imbalanced data is introduced. The proposed method innovatively combines XGBoost with a weighted loss function to effectively address the challenges of imbalanced datasets.

Another research effort to enhance IIoT network intrusion detection is presented in [25]. This study introduces a deep hybrid learning model that integrates Attention-based Machine Learning with a Fully Convolutional Neural Network (FCN), along with Gradient Boosting techniques (XGBoost and AdaBoost) and Long Short Term Memory (LSTM). The results demonstrate the model's efficiency in identifying anomalies in the traffic data of IoT devices, showcasing high Performance and efficacy in detecting various cybersecurity attacks. While the primary focus is on network intrusion detection, this approach holds the potential for adaptation to other anomaly detection tasks, including those related to IoT.

An enhanced Intrusion Detection System (IDS) is proposed to secure IIoT applications by Douiba et al. [26]. The model utilizes decision tree (DT) algorithms and gradient boosting (GB), specifically with the open-source Catboost framework, for efficient IIoT anomaly detection. The IDS model is evaluated across multiple datasets and achieves high-performance metrics, including precision, recall, and accuracy. The results highlight the model's effectiveness in detecting and characterizing anomalies within IoT devices. Furthermore, a comprehensive survey on various IIoT network anomaly detection techniques, including machine learning-based approaches, is presented in the review by Ahmed et al. [2]. In this survey, the authors thoroughly discuss and compare different machine learning algorithms and their Performance in anomaly detection, providing valuable insights into this field. Detecting anomalies in encrypted Internet traffic has become a pivotal area of research, given the increasing reliance on encrypted services to safeguard consumer privacy. In a recent study closely related to our research, hybrid deep learning techniques are applied to identify anomalies in encrypted network traffic [27]. This research employed deep learning models with different publicly available datasets, including RNN, CNN, and LSTM. However, while valid, this approach suffers from the limitation of the combined model and the utilization of older datasets, not fully capturing the intricacies of contemporary cyber threats. In contrast, our research leverages a more robust hybrid deep learning solution with the most recent dataset, providing a solution proven to be more accurate and practical in detecting current cybersecurity threats.

III. CONTRIBUTION OF RESEARCH

In this section, we outline the critical contributions of our paper to the field of ML-assisted IIoT security.

A. *Problem Statement*

This study addresses the imperative need for robust anomaly detection in IIoT environments, where the convergence of diverse and dynamic data streams requires effective anomaly detection methods. The challenge lies in developing a model that can simultaneously capture spatial and temporal patterns to accurately distinguish between normal and malicious activities, ensuring the security and reliability of IIoT networks. The research aims to devise a better solution that combines Gated Recurrent Units (GRU) and Convolutional Neural Networks (CNN) to tackle these intricacies and enhance anomaly detection accuracy in Edge IIoT systems.

B. *Novelty*

In this section, we delve deeper into the novel contributions of our research. This research embodies a novel and holistic approach to anomaly detection, custom-tailored for Edge IoT environments. It pushes the boundaries of intrusion detection by addressing the unique challenges of this domain. It offers robust and accurate detection capabilities for known and emerging threats, thus significantly advancing IIoT security. The following are the main novel contributions of this work:

1) Hybrid CNN+GRU Architecture: Our work introduces a novel integration of a hybrid CNN+GRU architecture for anomaly detection in Edge IoT environments. This innovative approach capitalizes on the strengths of Convolutional Neural Networks in extracting features, combined with ML algorithms like Gated Recurrent Units for temporal sequence analysis. This fusion of spatial and temporal analysis techniques represents a pioneering solution to enhance the accuracy and robustness of intrusion detection in complex IIoT settings.
2) Tailored to Edge IoT: While many intrusion detection systems are designed for traditional network environments, our model is specifically tailored to the unique challenges of Edge IoT environments. This adaptation addresses the inherent limitations of resource-constrained Edge devices, making our approach especially relevant and impactful for emerging IoT applications at the network's edge.
3) Diverse Attack Type Evaluation: We extend the novelty of our research through a comprehensive evaluation of the proposed model's Performance across a broad spectrum of attack types. By assessing its ability to accurately detect common attacks and specific instances of novel and evolving threats, our study contributes to enhancing IIoT anomaly detection by pushing the boundaries of a hybrid DL-based detection approach.
4) Robust Normal Sample Detection: Besides its prowess in identifying anomalies, our model excels in robustly detecting standard samples, a critical aspect of intrusion detection often overlooked in previous works. This unique capability ensures that false positives are minimized, further enhancing our research's practical relevance and real-world applicability.
5) Practical Relevance: The practical relevance of our work is underscored by its potential to be deployed in real-

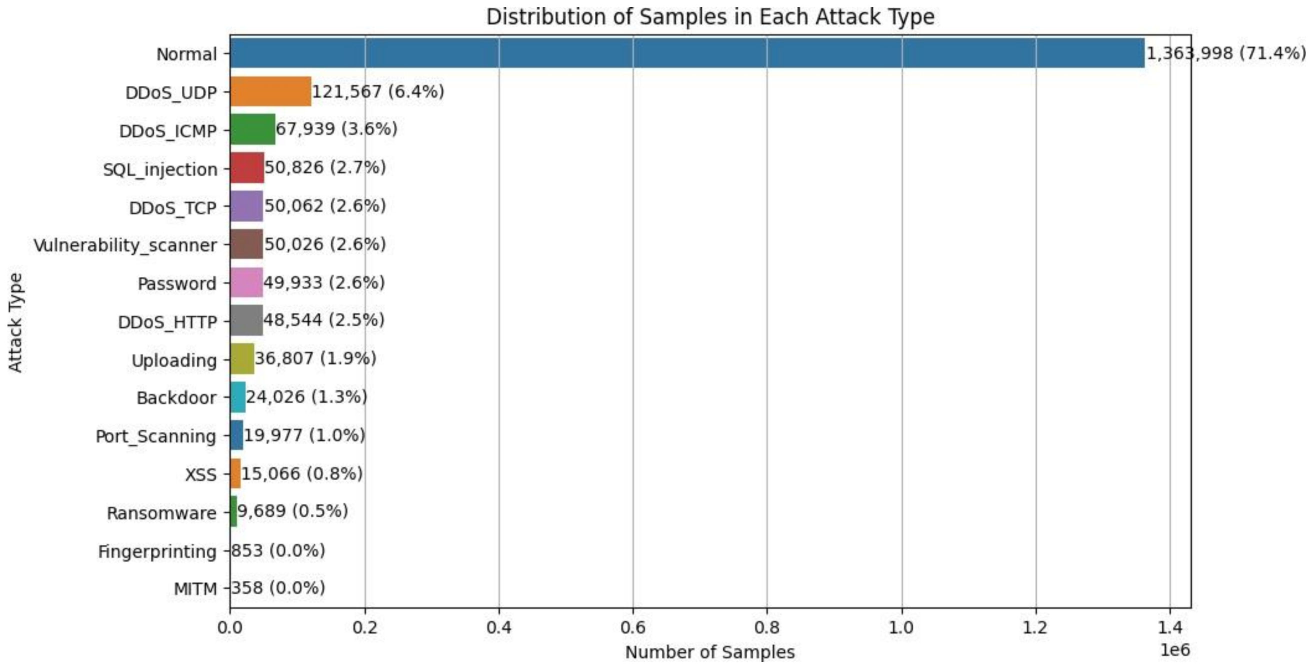


Fig. 2: Distribution of samples after preprocessing dataset

world IIoT scenarios, where the accurate and timely detection of anomalies is paramount for maintaining system integrity and security. By addressing the pressing need for effective intrusion detection in Edge IoT, our research contributes to the advancement of IIoT security, making it highly relevant in today's evolving technological landscape.

C. Methodology or Approach

Our methodology encompasses a carefully crafted pipeline that considers Edge IoT datasets' specific challenges and constraints. It leverages a hybrid security approach to extract spatial and temporal patterns efficiently. The extensive experimentation and use of performance metrics ensure a thorough evaluation of the model's capabilities. Additionally, the comparison with XGBoost provides valuable insights into our approach's novel contributions and potential advantages in anomaly detection within Edge IoT environments. The following are the main points of the followed methodology:

1) Data Preprocessing:
    a) Feature Extraction: Data preprocessing is a crucial step in any machine learning task. In our study, we performed data preprocessing specifically tailored for Edge IoT datasets. This involved the extraction of relevant features from the raw data. Given the resource-constrained nature of Edge devices, we focused on extracting features that are essential for anomaly detection, ensuring efficiency and effectiveness.
    b) Dimension Reduction: To further optimize the model for resource-constrained Edge IoT environments, we employed dimension reduction techniques. These techniques help reduce the feature space's complexity while retaining important information. Dimension reduction not only conserves computational resources but also aids in mitigating the curse of dimensionality, which is particularly pertinent in IoT data.
2) The Proposed Hybrid Convolutional Neural Network (CNN) and Gated Recurrent Units (GRU) Architecture:
    a) To capture both spatial and temporal patterns within the data, we designed a novel hybrid architecture that combines CNN and GRU.
    b) CNN Component: The CNN component focuses on spatial feature extraction. It excels at detecting patterns and features within the data invariant to translation, essential for capturing spatial characteristics in IoT sensor data.
    c) GRU Component: The GRU component, on the other hand, specializes in analyzing temporal sequences. It is well-suited for capturing time-dependent patterns and behaviors in IoT data, which is crucial for understanding the dynamics of IoT environments.
3) Model Training and Evaluation:
    a) Extensive Experimentation: We conducted a rigorous experimental phase involving diverse attack scenarios to ensure that the DL model Performance is thoroughly evaluated under various real-world conditions and could effectively detect a wide range of potential threats.
    b) ML Metrics: To assess the quality of our hybrid model, we used a comprehensive set of performance metrics. These included accuracy, recall, precision, and F1-score. These performance mea-

sures are needed to test the capabilities of identifying anomalies and minimizing false positives.

4) Comparison with XGBoost:
    a) As part of our methodology, we compared the Performance of our hybrid CNN+GRU model with that of the gradient-boosting algorithm XGBoost.
    b) This comparative analysis aimed to identify the strengths and weaknesses of the hybrid model concerning anomaly detection. By contrasting it with XGBoost, a well-established and widely-used machine learning algorithm, we gained insights into the unique advantages our hybrid approach brings to the table.

D. *Impact and Significance*

The significance of this research lies in its pioneering approach to Edge IoT anomaly detection through the development of a hybrid CNN+GRU model. Its potential to enhance cybersecurity in real-world deployments, its adaptability to evolving threats, and its practical applicability across industries underscore the far-reaching impact of this work. It serves as a beacon of innovation in IoT security, providing a valuable asset for safeguarding our modern world's increasingly interconnected and vital systems.

1) Innovative Hybrid CNN+GRU Model:
    a) At the heart of this research lies developing a hybrid CNN+GRU model specifically tailored for Edge IoT anomaly detection. This model represents a novel fusion of deep learning techniques, combining (CNNs) for spatial feature extraction and (GRUs) for temporal sequence analysis.
    b) The significance of this innovation cannot be overstated. Edge IoT environments often present complex, heterogeneous data streams that require a multifaceted approach for accurate anomaly detection. Our model addresses this challenge head-on by seamlessly integrating spatial and temporal analysis, offering a more holistic understanding of the data.
2) Enhanced Cybersecurity in Real-World IoT Deployments:
    a) One of the most striking outcomes of this research is the model's ability to accurately detect common attack types and various novel and evolving threats. Our proposed solutions aim to advance the knowledge and have implications for enhancing cybersecurity in real-world IoT deployments.
    b) As IoT continues to increase across industries, the security of these interconnected systems becomes increasingly critical. Our model's capacity to identify emerging threats, combined with its ability to distinguish regular traffic, offers a formidable defense mechanism for safeguarding these deployments.
3) Practical Relevance and Industry Applications:
    a) Beyond academic achievement, the practical relevance of this research cannot be overstated. Its impact extends to a wide range of industry applications.
    b) For industries reliant on Edge IoT, such as manufacturing, healthcare, and utilities, this research provides a reliable and versatile tool for early detection and prevention of cyber intrusions in many industry applications where any disruption can have far-reaching consequences, including financial losses and threats to public safety.
4) Mitigating Evolving Security Threats:
    a) The constantly evolving nature of cybersecurity threats necessitates adaptable and robust solutions. Our hybrid CNN+GRU model is well-suited to this dynamic landscape.
    b) By continuously improving the accuracy and effectiveness of anomaly detection in Edge IoT environments, this research contributes to the ongoing battle against cyber threats. It empowers organizations to stay ahead of adversaries and proactively protect their critical systems and sensitive data.

E. *Future Directions*

Future directions of this work could explore the applicability of more advanced deep learning architectures, such as Transformers, to capture complex temporal relationships and patterns in Edge IoT data. Investigating ensemble techniques that combine multiple models could enhance overall anomaly detection robustness.

IV. METHODOLOGY AND EXPERIMENTAL SETUP

A. *Dataset Description*

This study employed a comprehensive dataset to detect anomalies within Industrial Internet of Things (IIoT) networks, as documented in [28]. This dataset encompasses a wide array of network traffic data, containing regular traffic and various attack scenarios such as Port Scanning, XSS, Ransomware, Fingerprinting, and MITM. Data samples are collected from a real-world industrial environment, featuring multiple devices and communication protocols commonly encountered in IIoT networks to ensure the representativeness and reliability of the data. Through the utilization of this extensive dataset, we were able to effectively test the quality of different DL models for detecting and mitigating cybersecurity threats within the IIoT domain.[29-34].

The dataset comprises 2,219,201 instances and 63 features, all meticulously collected to investigate and analyze cybersecurity threats within edge computing for IIoT applications. It encompasses a wide array of information, including attributes related to network traffic, protocol-specific parameters, and various attack types. These features exhibit diverse data types, encompassing numerical (float64) and categorical (object) data. Key features include network communication attributes like IP addresses (ip.src_host, ip.dst_host), ARP protocol details (arp.opcode, arp.hw.size), ICMP protocol characteristics (icmp.checksum, icmp.seq_le), HTTP protocol fields (http.content_length, http.request.method, http.referer), and TCP/UDP protocol properties (tcp.flags, tcp.len, udp.port, udp.stream).

Additionally, the dataset contains features associated with domain name system (DNS) queries (dns.qry.name, dns.qry.type) and the MQTT protocol, Message Queuing Telemetry Transport (mqtt.conack.flags, mqtt.hdrflags, mqtt.topic). The dataset's target variable, labeled "Attack_type," is a categorical attribute that represents 15 distinct classes of cybersecurity threats. These classes encompass various threats, including Distributed Denial of Service (DDoS), ransomware, man-in-the-middle (MITM) attacks, and port scanning. Before analysis, the dataset undergoes preprocessing steps, including eliminating unnecessary columns, addressing missing and duplicate values, and randomizing the data order. Figure 2 provides a detailed breakdown of the attack types and the corresponding number of instances for each attack class before applying oversampling techniques.

For data transformation, categorical variables are subjected to one-hot encoding, while the target variable undergoes label encoding. To tackle the class imbalance issue, we employ the RandomOverSampler method, which involves oversampling the minority classes. This technique generates synthetic instances for the underrepresented classes to match the sample count of the majority class. The dataset attains a more balanced distribution by introducing additional instances, allowing machine learning models to gain insights from a broader range of instances.

We utilize the RandomOverSampler from the learning library to implement random oversampling. The rationale behind this approach is to provide the model with a more representative view of the minority classes, facilitating enhanced anomaly detection within these less frequent categories. The introduction of synthetic instances enables the model to capture the distinctive patterns and characteristics specific to the minority classes, leading to improved overall Performance and accuracy. However, it's crucial to exercise caution when employing oversampling techniques, including random ones, as they must be carefully evaluated to prevent potential issues like overfitting or introducing biases. Alternative methods may need to be considered depending on the dataset's specific characteristics and research objectives.

Following oversampling, our dataset consists of two main parts: (training and testing sets). Subsequently, feature scaling is performed using MinMaxScaler, and the input data and target variables are reshaped to meet the prerequisites of deep learning models.

B. Proposed Hybrid CNN+GRU model:

Our deep learning (DL) model leverages the strengths of both Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) to excel in IIoT anomaly detection. This architectural fusion effectively captures inherent spatial and temporal information in datasets suitable for analyzing intricate sequences, as encountered in industrial IoT applications.

In the CNN segment of the model, convolutional layers are employed to extract features from datasets. These layers use filters to identify structures and patterns from datasets, enabling the model to acquire meaningful representations. The proposed model adeptly captures hierarchical representations of the input by stacking multiple layers of the DL network with increasing filter sizes.

Algorithm 1: Proposed Hybrid Deep Learning Architecture

```
Define the Convolutional Neural Network (CNN) model
$cnn\_input \leftarrow Input(shape = input\_shape)$
$cnn\_layer \leftarrow Conv1D('relu')(cnn\_input)$
$cnn\_layer \leftarrow MaxPooling1D$
Define the Gated Recurrent Unit (GRU) model
$gru\_input \leftarrow Input(shape = input\_shape)$
$gru\_layer \leftarrow GRU('tanh')(gru\_input)$
Concatenate the outputs of the CNN and GRU models
$concat\_layer \leftarrow concatenate([cnn\_layer, gru\_layer])$
Classification layer
$output\_layer \leftarrow$
$Dense(num\_classes,' softmax)(concat\_layer)$
Combined CNN and GRU Model
$model \leftarrow Model(inputs =$
$[cnn\_input, gru\_input], outputs = output\_layer)$
```

Conversely, GRUs, recurrent neural networks (RNN), incorporate gating mechanisms that selectively update and reset their internal states dedicated to modeling data dependencies. This functionality allows the model to retain and propagate crucial information across time steps, capturing long-term dependencies in the sequence. The GRU layer within the model utilizes these gating mechanisms to learn and represent temporal patterns within the data.

Combining CNN and GRU models through concatenating their output layers permits the fusion of both spatial and temporal features. This fusion affords comprehensive data comprehension, enabling the model to make precise predictions. Algorithm 1 provides a high-level overview of the model. By harnessing the complementary strengths of CNNs and GRUs, the CNN+GRU architecture strikes a balance between capturing local spatial features and modeling temporal dynamics.

Through rigorous experimentation and evaluation, our work has substantiated the efficacy of the CNN+GRU model. It has consistently performed with high accuracy, precision, recall, and F1 score in detecting anomalies within the industrial IoT dataset. The ability to discern intricate spatial and temporal patterns empowers it to accurately identify abnormal instances, facilitating proactive security measures in industrial IoT systems. Below, we provide pseudocode, and Figure 3 illustrates the architecture of this hybrid model.

C. Model Descriptions

1) 1D-CNN Model Overview: The 1D-CNN model proposed in this study uses the Keras Sequential API. It comprises multiple layers designed to learn using valuable features from our dataset and generate predictions. This model commences with an input layer configured to accommodate data in a

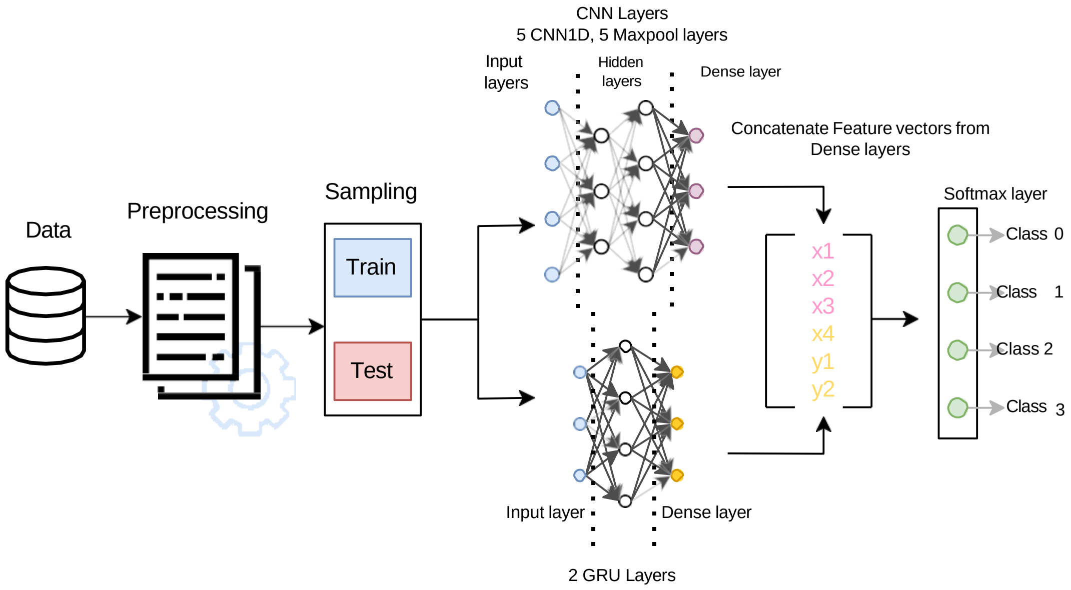


Fig. 3: The Architecture of the Proposed CNN+GRU Hybrid Deep Learning Model

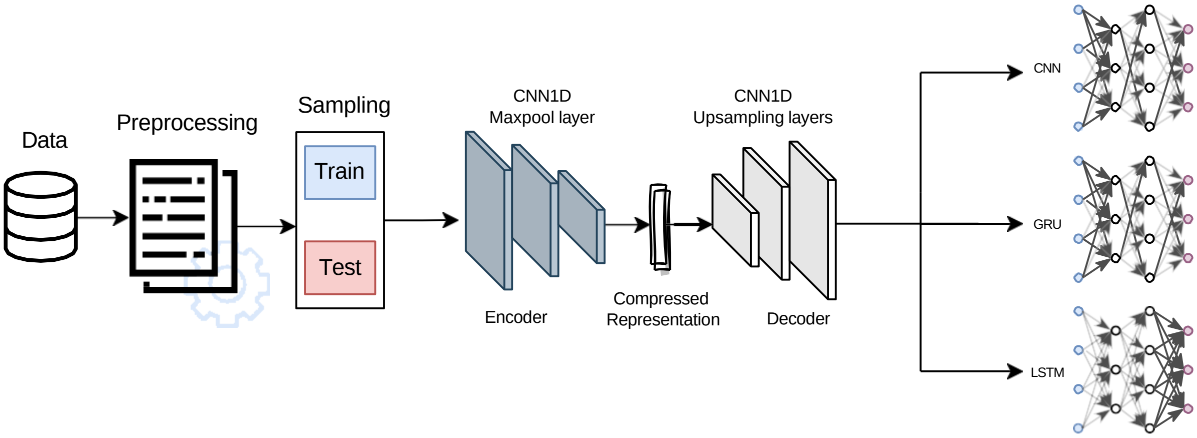


Fig. 4: Autoencoder-based Models Architecture

shape aligned with the dataset's dimensions. Subsequently, five Conv1D layers are added, each equipped with a distinct number of filters and a ReLU activation function. These layers are instrumental in extracting information using the dataset via filtering. Following each CNN layer, a MaxPooling1D layer with a size of 2 is applied to mitigate data dimensionality and capture significant features. Subsequently, a flattened layer converts the feature maps into a one-dimensional vector. Furthermore, the model incorporates two dense layers: the first dense layer, comprising 64 neurons and a ReLU activation function, focuses on learning global features, while the second dense layer, featuring the same number of neurons as the dataset's class count, utilizes a softmax activation function to yield class probabilities, enabling the final prediction.

2) *GRU Model:* The proposed GRU model is constructed using the Keras Sequential API. It encompasses two GRU layers, with the initial layer comprising 32 units and the subsequent layer comprising 64. These GRU layers utilize a blend of tanh and sigmoid activation functions to update and reset gates. The model also integrates two dense layers, employing ReLU activation functions, with 32 and 16 units, respectively. The ultimate external layer uses a softmax activation function with a number of units aligned with the dataset's class count. This GRU-based model effectively captures short- and long-term dependencies within sequential data, which is well-suited for diverse classification tasks.

3) *Overview of Hybrid CNN-GRU Model:* The proposed model represents a hybrid neural network, integrating Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) to proficiently process and learn from sequential data. Constructed using the Keras Functional API, it is designed with two distinct branches: the CNN branch and the GRU branch. The model's architectural framework is outlined as follows:

CNN Branch:

1) *Input Layer:* The model ingests data with dimensions

aligned to the dataset's structure.

2) *Convolutional Layers:* The CNN branch comprises two convolutional layers, one with 64 and 128 filters, each utilizing a ReLU activation function.
3) *MaxPooling Layers:* Max-pooling layers with a pool size of 2 are strategically placed between the convolutional layers to reduce spatial dimensions and enhance computational efficiency.
4) *Flatten Layer:* Following the final max-pooling layer, a flattened layer converts the 3D output from the convolutional layers into a 1D vector.
5) *Dense Layer:* The concluding layer within the CNN branch is a dense layer with 64 units and a ReLU activation function, enabling the model to grasp higher-level features derived from the spatial data.

GRU Branch:

1) *Input Layer:* Similar to the CNN branch, the GRU branch's input layer accommodates data of the same dimensions.
2) *GRU Layer:* The GRU layer, featuring 32 units, employs a 'tanh' activation function for gate updates and a 'sigmoid' activation function for reset gates. Recurrent dropout is disabled (set to 0), and the layer avoids unrolling the recurrent loop for efficiency. Bias terms are integrated into the update and reset gate computations, and the hidden states reset after each sequence.
3) *Dense Layer:* After the GRU layer, a dense layer with 32 units and a 'tanh' activation function is added, facilitating the model in discerning intricate patterns and features from temporal data.

Integration of Branches: Upon processing input data through the CNN and GRU branches, the outputs undergo concatenation using the concatenate layer. This amalgamated representation encompasses spatial and temporal features gleaned from both branches, enriching the final decision-making process.

Output Layer: The ultimate layer consists of a dense layer with (num_classes) units and a softmax activation function. The softmax function furnishes a probability distribution across classes, enabling the model to make a final prediction based on the highest probability. Figure 1 illustrates the structure of the unified CNN-GRU model.

D. Autoencoder Models Overview

Hybrid Models: The proposed models are hybrid neural networks combining an autoencoder with CNN, LSTM, and GRU networks to process and learn from input data efficiently. Each model is designed using the Keras Functional API and consists of two primary components: the encoder-decoder (autoencoder) module and the CNN, LSTM, or GRU modules. The employed autoencoder type is a basic convolutional autoencoder, utilizing convolutional layers for both encoding and decoding. These layers excel in capturing spatial patterns and features in the input data.

Encoder-Decoder (Autoencoder) Module: The encoder section of the autoencoder employs convolutional layers with decreasing filters to extract essential features from the input data and reduce its dimensionality. The decoder section uses upsampling and convolutional layers to reconstruct the original input from the encoded representation. Figure 4 provides an architectural overview of the autoencoder models.

Model 1:

Encoder:

1) *Input Layer:* The model takes input dimensions aligned with the dataset.
2) *Convolutional Layers:* Three convolutional layers with 32, 64, and 128 filters are used, each with a kernel size 3 and ReLU activation.
3) *MaxPooling Layers:* Max-pooling layers with a pool size of 2 are placed between convolutional layers to reduce dimensions.

Decoder:

1) *Convolutional Layers:* The decoder comprises three convolutional layers with 128, 64, and 32 filters, using ReLU activation.
2) *UpSampling Layers:* Upsampling layers with a size of 2 restore spatial dimensions.

Autoencoder: The autoencoder combines the encoder and decoder models with the same input as the encoder and output from the decoder.

Classifier:

1) The autoencoder serves as the initial classifier layer.
2) Conv1D and MaxPooling1D layers perform feature extraction and dimensionality reduction.
3) The last MaxPooling1D output is flattened.
4) Dense layers with ReLU activation process features.
5) A final Dense layer with softmax activation provides class probabilities.

Model 2:

Classifier:

1) LSTM layers replace Conv1D and MaxPooling1D layers for sequence processing.
2) LSTM layers return sequences, extracting features from them.
3) A Dense layer with softmax activation is used for classification.

Model 3:

Classifier:

1) Instead of Conv1D and MaxPooling1D layers, a GRU (Gated Recurrent Unit) layer is employed for sequence processing.
2) The GRU layer comprises 32 units and utilizes 'tanh' activation for gate updates and 'sigmoid' activation for reset gates.
3) A Dense layer with 'tanh' activation further processes features.
4) The final Dense layer with softmax activation provides a class probability distribution for classification.

1) Overview of the LSTM Model: The proposed model is an LSTM-based classifier designed specifically for time series classification tasks. This architecture comprises a sequence of LSTM layers followed by dense layers for the classification task. The key components of the model's architecture are outlined below:

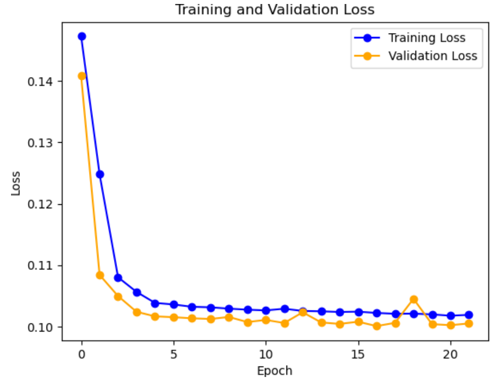


Fig. 5: CNN Loss

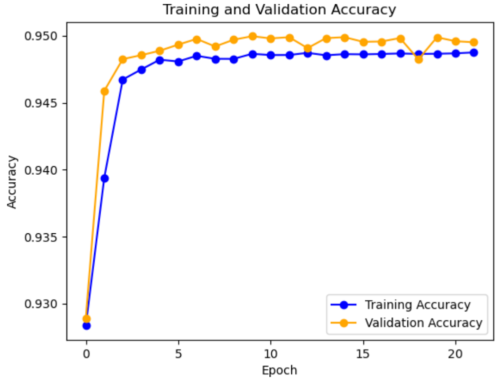


Fig. 6: CNN Accuracy

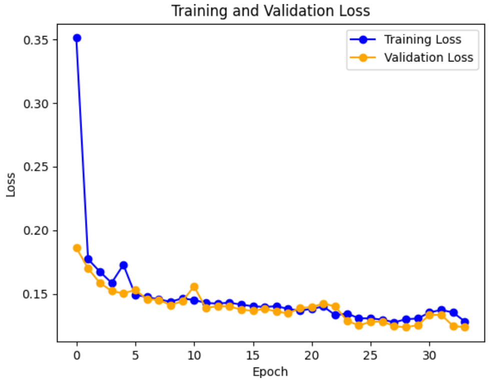


Fig. 7: GRU Loss

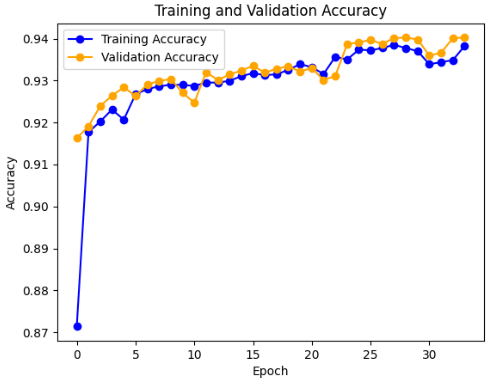


Fig. 8: GRU Accuracy

1) **LSTM Layer 1**: The first LSTM layer serves as the input layer, necessitating the specification of the input shape. It incorporates 128 units and employs the 'tanh' activation function for transformations within the LSTM units. Notably, this layer is configured to return sequences, ensuring it outputs a sequence of the same length for the subsequent layer's use rather than just the last timestep's output.
2) **LSTM Layer 2**: The second LSTM layer comprises 256 units and adopts the 'tanh' activation function. Unlike the preceding layer, it does not return sequences, outputting only the final output of the LSTM sequence. This design facilitates seamless connectivity with a traditional dense layer.
3) **Dense Layer (Output Layer)**: The ultimate layer in the model is a dense layer with several units equivalent to the number of classes in the classification task (num_classes). This layer incorporates a softmax activation function, generating a probability distribution across the classes. This characteristic makes it particularly well-suited for multi-class classification tasks.

This model effectively harnesses the capabilities of LSTM layers for processing and learning from sequential data, establishing an efficient and robust solution for time-series classification endeavors.

V. EVALUATION AND RESULTS

This section comprehensively evaluates the Performance of various deep-learning models employed for anomaly detection within encrypted IoT traffic. It involves an in-depth examination of the outcomes, emphasizing the strengths and weaknesses of each model while drawing comparisons based on performance metrics such as accuracy, precision, recall, and F1-score. The section also delves into the convergence patterns of the models and scrutinizes noteworthy observations or trends. The evaluation incorporates multiple performance metrics: Loss, Accuracy, Recall, Precision, F1-Score, and False Alarm Rate (FAR).

A. Assessing Model Performance

The XGBoost model is the top performer in accuracy, recall, precision, and F1 score. It attains an accuracy rate of 96.41% , indicating its proficiency in correctly categorizing most samples. A recall rate of 96.50% underscores its effectiveness in identifying actual positive instances, while a precision rate of 98.57% signifies its ability to maintain a low false positive rate. The high F1-score, standing at 96.03%, indicates a harmonious balance between precision and recall, reflecting the model's overall Performance. In a related research endeavor that implemented the Catboost model for intrusion detection in IoT systems [26], the reported results indicated a training accuracy of 100% and a validation accuracy of 99.27%. Furthermore,

TABLE I: Performance of the models

Model	Loss	Accuracy	Recall	Precision	F1-Score	FAR	Training Time (min)	Training Epochs
CNN	0.10211	0.94839	0.92303	0.98384	0.95196	0.00108	18	23
GRU	0.12445	0.93981	0.91766	0.97027	0.9428	0.002	35	17
GRU+CNN	0.09985	0.9494	0.92288	0.98494	0.95239	0.001	97	73
LSTM	0.12607	0.93939	0.91288	0.97455	0.94219	0.0017	36	14
Autoencoder+GRU	1.26009	0.71425	0.71425	0.71425	0.71425	0.02041	12	7
Autoencoder+CNN	0.11195	0.94695	0.92194	0.98104	0.95009	0.00127	32	30
Autoencoder+LSTM	0.23309	0.91507	0.87954	0.97054	0.92207	0.0019	37	12
XGBoost	0.0672	0.9641	0.965	0.9857	0.9603	0.0023	16	25

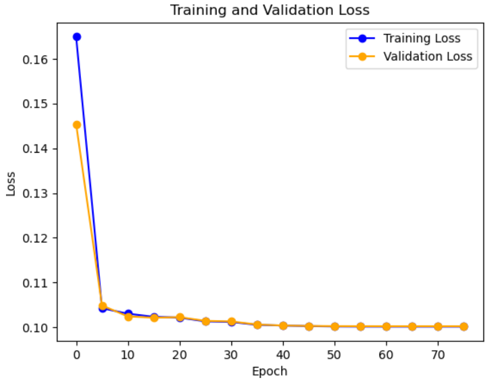


Fig. 9: CNU+GRU Loss

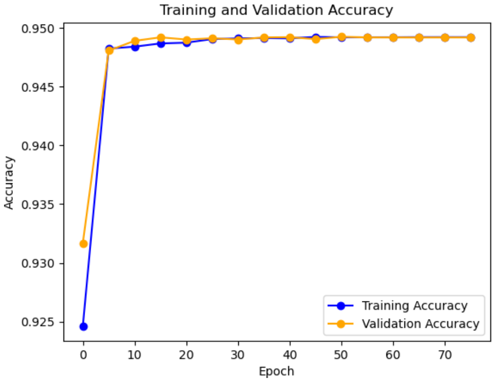


Fig. 10: CNN+GRU Accuracy

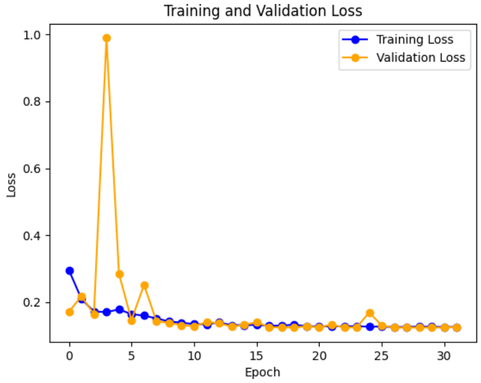


Fig. 11: LSTM Loss

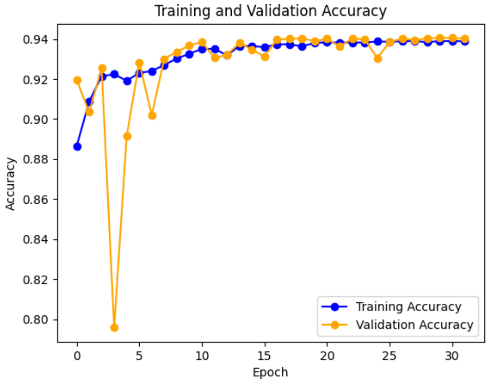


Fig. 12: LSTM Accuracy

they achieved commendable values for precision (98.42%) and recall (98.78%), signifying outstanding Performance in intrusion classification.

Comparing the two models, it becomes evident that Catboost and XGBoost attained impressive accuracy rates and excelled in classifying intrusions. The Catboost model reported a slightly higher accuracy during training, but both models exhibited robust precision and recall scores. It is imperative to consider a variety of evaluation metrics, assess potential overfitting, and analyze the problem context before concluding that high accuracy alone signifies a superior model.

In our comprehensive assessment of various machine learning models designed for IoT security anomaly detection, the XGBoost algorithm leads the way, closely followed by the impressive CNN+GRU model. The CNN+GRU model, which combines CNN GRU, stands out in multiple aspects. Notably, it demonstrates an accuracy rate of 94.94% and a recall rate of 92.28% , highlighting its proficiency in accurately identifying anomalies, particularly in the nuanced context of IoT data. Additionally, a precision rate of 98.49% and an F1-score of 95.24% further underscore its capacity to categorize anomalies while effectively minimizing false positives. Moreover, the meager False Alarm Rate (FAR) of 0.001% signifies the model's skill in avoiding unnecessary alerts, a critical characteristic in practical applications. Integrating spatial and temporal features through the incorporation of CNN and GRU layers plays a pivotal role in the exceptional Performance of this model. The CNN+GRU model demonstrates the synergy between these two architectural components and showcases its adaptability to intricate, multi-dimensional datasets such as IoT traffic. These performance metrics firmly establish the CNN+GRU model as a potent tool for fortifying IoT environments against cyber threats.

Shifting the focus to the other models, namely CNN, GRU,

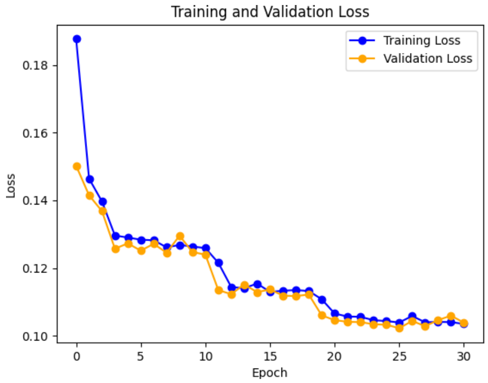


Fig. 13: Autoencoder+CNN Loss

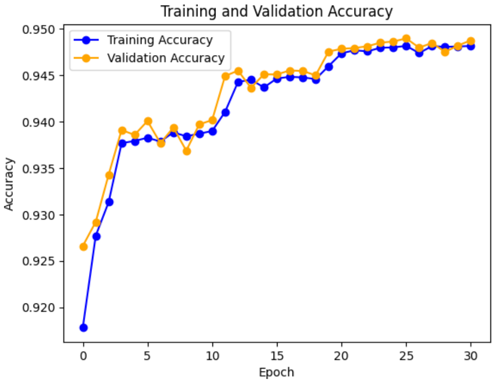


Fig. 14: Autoencoder+CNN Accuracy

and LSTM, these models consistently achieve high accuracy levels ranging from 93.94% to 94.94%. While they may not surpass the Performance of XGBoost, their accuracy rates affirm their capability to classify most samples accurately. The recall rates, ranging from 91.29% to 92.29% , indicate their efficacy in capturing actual positive instances, while the precision rates, ranging from 97.03% to 98.49% , reveal their proficiency in minimizing false positive instances. Additionally, the F1 scores, ranging from 94.22% to 95.24%, further underscore the overall Performance of these models in achieving a harmonious balance between precision and recall.

Conversely, the Autoencoder + GRU model exhibits the poorest Performance among all the models across the metrics, with an accuracy rate of 71.43%. These metrics reveal a significant disparity compared to the other models, suggesting a reduced capability in classifying diverse attack types. A more in-depth analysis is warranted to investigate the underlying causes of this subpar Performance and explore potential avenues for enhancing the model's effectiveness.

It is essential to assess the strengths and limitations of each model thoroughly. XGBoost, utilizing its gradient boosting algorithm, consistently demonstrates robust Performance across all metrics. Notably, it greatly benefits from oversampling the data for minority classes, rendering it a suitable choice for anomaly detection. Figure 22 depicts the confusion matrix of the XGBoost model, the top-performing model in our study. This matrix offers valuable insights into the model's

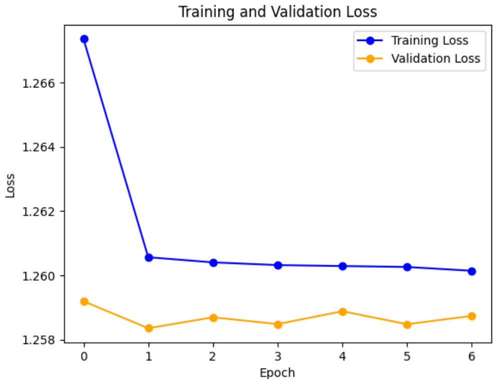


Fig. 15: Autoencoder+GRU Loss

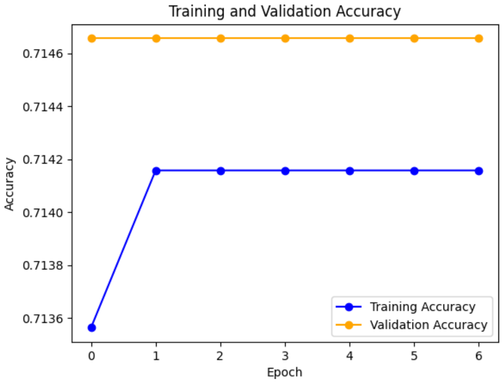


Fig. 16: Autoencoder+GRU Accuracy

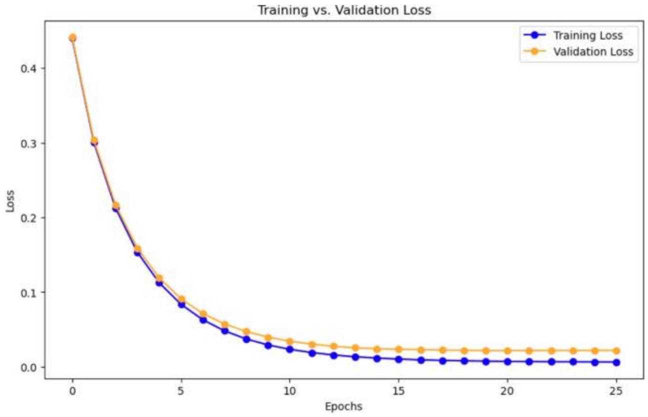


Fig. 17: XGBoost Loss

classification capabilities across various attack types. Each row in the matrix represents the actual labels, while each column corresponds to the predicted labels. The numbers within the matrix denote the count of samples falling into each category. The XGBoost model impressively exhibits accuracy and precision in classifying diverse attack types. It effectively identifies a substantial number of samples belonging to categories such as DDoS TCP, DDoS HTTP, DDoS ICMP, MITM, Fingerprinting, DDoS UDP, Password, Port Scanning, Ransomware, SQL Injection, Uploading, Vulnerability Scanner, and XSS.

Nonetheless, there are instances of misclassifications evi-

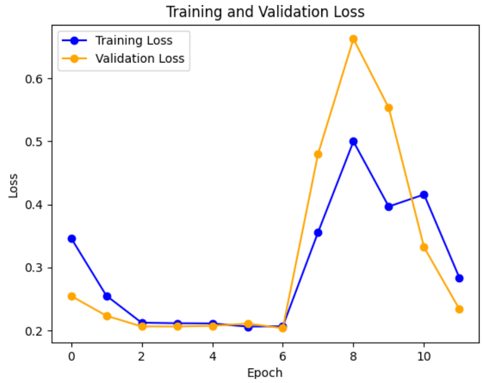


Fig. 18: Autoencoder+LSTM Loss

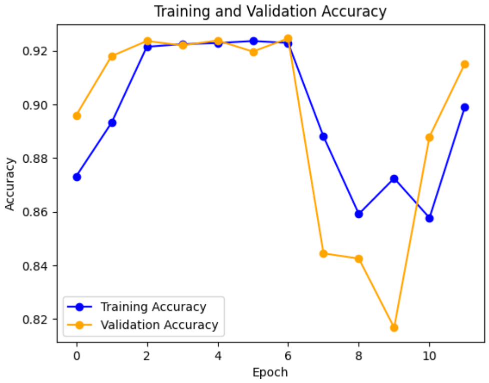


Fig. 19: Autoencoder+LSTM Accuracy

dent in the confusion matrix. For example, the model may encounter challenges when precisely distinguishing samples belonging to the Backdoor category, resulting in a few cases needing to be misclassified. Additionally, a small number of samples in the Normal category are erroneously labeled as other types of attacks. The XGBoost model showcases exceptional Performance by accurately classifying a broad spectrum of attack types and boasting outstanding precision and recall. Its minimal false alarm rate underscores its ability to effectively minimize false positives, thereby ensuring high accuracy in detecting anomalies within encrypted IoT traffic.

The deep learning models, including CNN, GRU, GRU+CNN, and LSTM, consistently exhibit commendable accuracy rates and demonstrate their effectiveness in capturing anomalies. Notably, the CNN model's Performance was solid on the original dataset. In contrast, the Performance of the other models improved significantly when the sample count for smaller classes was augmented using oversampling techniques. These techniques indicate that the CNN model's Performance is slightly degraded when confronted with an increased sample count for smaller classes. The Autoencoder + GRU model, although not performing at the same level as the others, still provides valuable insights into the potential of combining autoencoder-based feature extraction with the GRU architecture.

In conclusion, the XGBoost model emerges as the top performer, while the CNN, GRU, CNN+GRU, and LSTM models consistently exhibit strong Performance in anomaly detection. Table I and Figure 20 present an overview of the performance metrics for each model, while Figure 23 offers a comparative analysis of the models across each metric. The Autoencoder + GRU model shows room for improvement and warrants further investigation. These findings contribute to a deeper understanding of model performance and can serve as a guide for selecting appropriate models for anomaly detection in encrypted IoT traffic.

The confusion matrix depicted in Figure 21 provides valuable insights into the CNN+GRU hybrid model's Performance in categorizing various types of attacks. In this matrix, the rows represent the actual values, and the columns show the predicted values, with the numerical values indicating the sample count for each category. The CNN+GRU model demonstrates a high accuracy level in correctly identifying most attack types. Notably, it effectively classifies a significant portion of samples from categories such as Vulnerability scanning, DDoS TCP, Uploading, DDoS HTTP, Ransomware, DDoS ICMP, XSS MITM, Fingerprinting, DDoS UDP, Password, SQL injection, and Port Scanning. However, it's essential to acknowledge that the model does experience some misclassifications. For instance, misclassified samples are in the Backdoor category, indicating a challenge in accurate distinction. Similarly, a few samples in the Normal category are misclassified as other types of attacks.

Figure 22 displays the confusion matrix for the XGBoost model, which emerged as the top performer in our study. This matrix provides insights into the model's classification capabilities across various attack types. Each row corresponds to the actual labels, and each column represents the predicted labels, with the matrix entries denoting sample counts within each category. The XGBoost model exhibits high accuracy and precision in classifying various attack types. It effectively identifies a substantial number of samples from categories including Vulnerability scanning, DDoS TCP, Uploading, DDoS HTTP, Ransomware, DDoS ICMP, XSS MITM, Fingerprinting, DDoS UDP, Password, SQL injection, and Port Scanning. However, there are instances of misclassifications within the confusion matrix. Figure 22 provides valuable insights into the XGBoost model's classification capabilities for various attack types, making it evident that the model excels in accurately categorizing many attack types. Each row in the matrix corresponds to the actual labels, while each column represents the predicted labels, and the matrix entries indicate the sample counts for each category. The XGBoost model demonstrates exceptional accuracy and precision in classifying various attack types, successfully identifying a significant number of samples belonging to categories such as Vulnerability scanning, DDoS TCP, Uploading, DDoS HTTP, Ransomware, DDoS ICMP, XSS MITM, Fingerprinting, DDoS UDP, Password, SQL injection, and Port Scanning. Nonetheless, some misclassifications are observed within the confusion matrix.

When comparing the quality of the XGBoost, CNN, and GRU hybrid models in anomaly detection, it becomes apparent that each model possesses distinct strengths for different attack types. The XGBoost model detects Normal and MITM

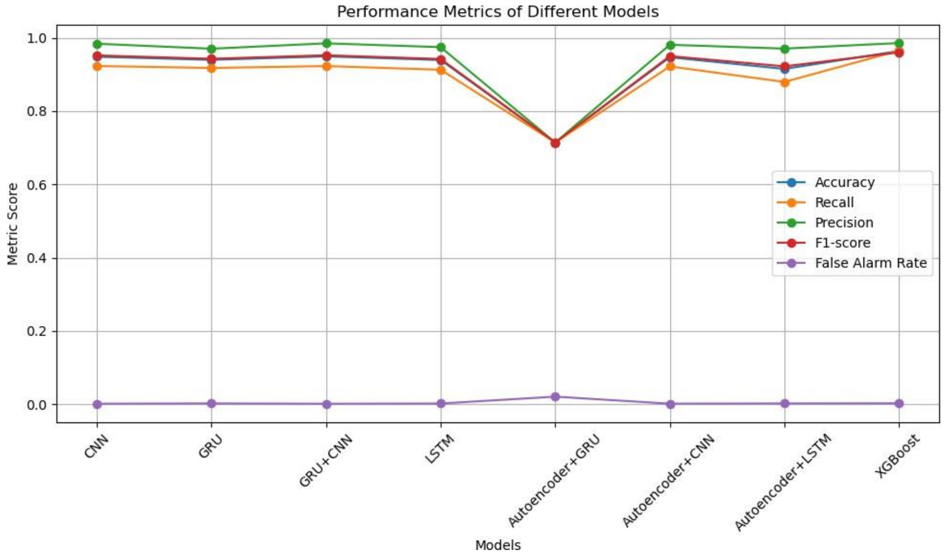
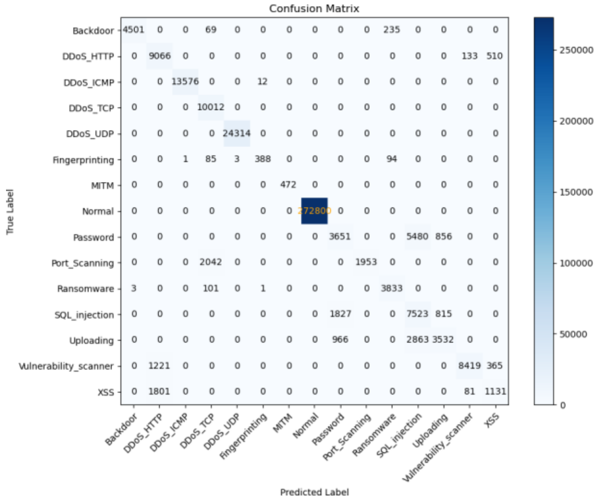
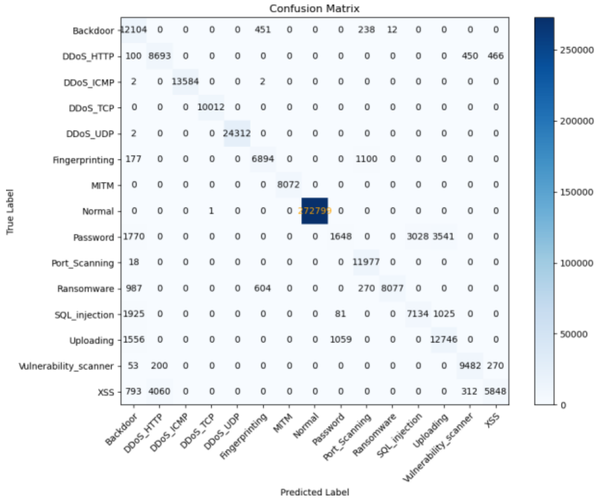


Fig. 20: Performance Comparison



	Backdoor	DDoS_HTTP	DDoS_ICMP	DDoS_TCP	DDoS_UDP	Fingerprinting	MITM	Normal	Password	Port_Scanning	Ransomware	SQL_injection	Uploading	Vulnerability_scanner	XSS
Backdoor	4501	0	0	69	0	0	0	0	0	0	235	0	0	0	0
DDoS_HTTP	0	9066	0	0	0	0	0	0	0	0	0	0	0	133	510
DDoS_ICMP	0	0	13576	0	0	12	0	0	0	0	0	0	0	0	0
DDoS_TCP	0	0	0	10012	0	0	0	0	0	0	0	0	0	0	0
DDoS_UDP	0	0	0	0	24314	0	0	0	0	0	0	0	0	0	0
Fingerprinting	0	0	1	85	3	388	0	0	0	0	94	0	0	0	0
MITM	0	0	0	0	0	0	472	0	0	0	0	0	0	0	0
Normal	0	0	0	0	0	0	0	272800	0	0	0	0	0	0	0
Password	0	0	0	0	0	0	0	0	3651	0	0	5480	856	0	0
Port_Scanning	0	0	0	2042	0	0	0	0	0	1953	0	0	0	0	0
Ransomware	3	0	0	101	0	1	0	0	0	0	3833	0	0	0	0
SQL_injection	0	0	0	0	0	0	0	0	1827	0	0	7523	815	0	0
Uploading	0	0	0	0	0	0	0	0	966	0	0	2863	3532	0	0
Vulnerability_scanner	0	1221	0	0	0	0	0	0	0	0	0	0	0	8419	365
XSS	0	1801	0	0	0	0	0	0	0	0	0	0	0	81	1131

Fig. 21: Confusion matrix for CNN+GRU model



	Backdoor	DDoS_HTTP	DDoS_ICMP	DDoS_TCP	DDoS_UDP	Fingerprinting	MITM	Normal	Password	Port_Scanning	Ransomware	SQL_injection	Uploading	Vulnerability_scanner	XSS
Backdoor	12104	0	0	0	0	451	0	0	0	238	12	0	0	0	0
DDoS_HTTP	100	8693	0	0	0	0	0	0	0	0	0	0	0	450	466
DDoS_ICMP	2	0	13584	0	0	2	0	0	0	0	0	0	0	0	0
DDoS_TCP	0	0	0	10012	0	0	0	0	0	0	0	0	0	0	0
DDoS_UDP	2	0	0	0	24312	0	0	0	0	0	0	0	0	0	0
Fingerprinting	177	0	0	0	0	6894	0	0	0	1100	0	0	0	0	0
MITM	0	0	0	0	0	0	8072	0	0	0	0	0	0	0	0
Normal	0	0	0	1	0	0	0	272799	0	0	0	0	0	0	0
Password	1770	0	0	0	0	0	0	0	1648	0	0	3028	3541	0	0
Port_Scanning	18	0	0	0	0	0	0	0	0	11977	0	0	0	0	0
Ransomware	987	0	0	0	0	604	0	0	0	270	8077	0	0	0	0
SQL_injection	1925	0	0	0	0	0	0	0	81	0	0	7134	1025	0	0
Uploading	1556	0	0	0	0	0	0	0	1059	0	0	0	12746	0	0
Vulnerability_scanner	53	200	0	0	0	0	0	0	0	0	0	0	0	9482	270
XSS	793	4060	0	0	0	0	0	0	0	0	0	0	0	312	5848

Fig. 22: Confusion Matrix of XGboost model

attacks, demonstrating impressive accuracy and a reduced false positive rate. However, it faces challenges in accurately classifying Backdoor and Password attacks, indicating room for improvement. In contrast, the CNN+GRU hybrid model exhibits outstanding precision in detecting Backdoor, DDoS_TCP, and DDoS_UDP attacks, highlighting its potential for handling network-based attacks effectively. Additionally, it achieves high accuracy in identifying DDoS_HTTP and XSS attacks, showcasing its proficiency in recognizing web-based threats. Nevertheless, the CNN+GRU model may require further fine-tuning to address misclassifications related to Fingerprinting and Password attacks. Overall, both models show promising results, with the CNN+GRU hybrid model excelling in network-based and web-based attack detection. In contrast, the XGBoost model performs exceptionally well in detecting Normal and MITM attacks with high precision.

B. Convergence of the Models

The convergence behavior of the models plays a vital role in assessing their Performance, offering insights into the training process, convergence speed, stability, and overall efficiency. In this study, we investigated the convergence of several models, including CNN, GRU, LSTM, CNN+GRU, Autoencoder+CNN, Autoencoder+GRU, Autoencoder+LSTM, and XGBoost.

Figures 5–17 provide valuable information about each model's training progress, illustrating the trends in Loss and accuracy across different epochs. Let's delve into the individual Performance of each model:

For the CNN model (Figure 5 and Figure 6), we observe a gradual decrease in Loss and a simultaneous increase in accuracy as the number of epochs increases. The CNN architecture exhibited relatively rapid convergence, with an average per-epoch runtime of 17.5 minutes and 23 training epochs.

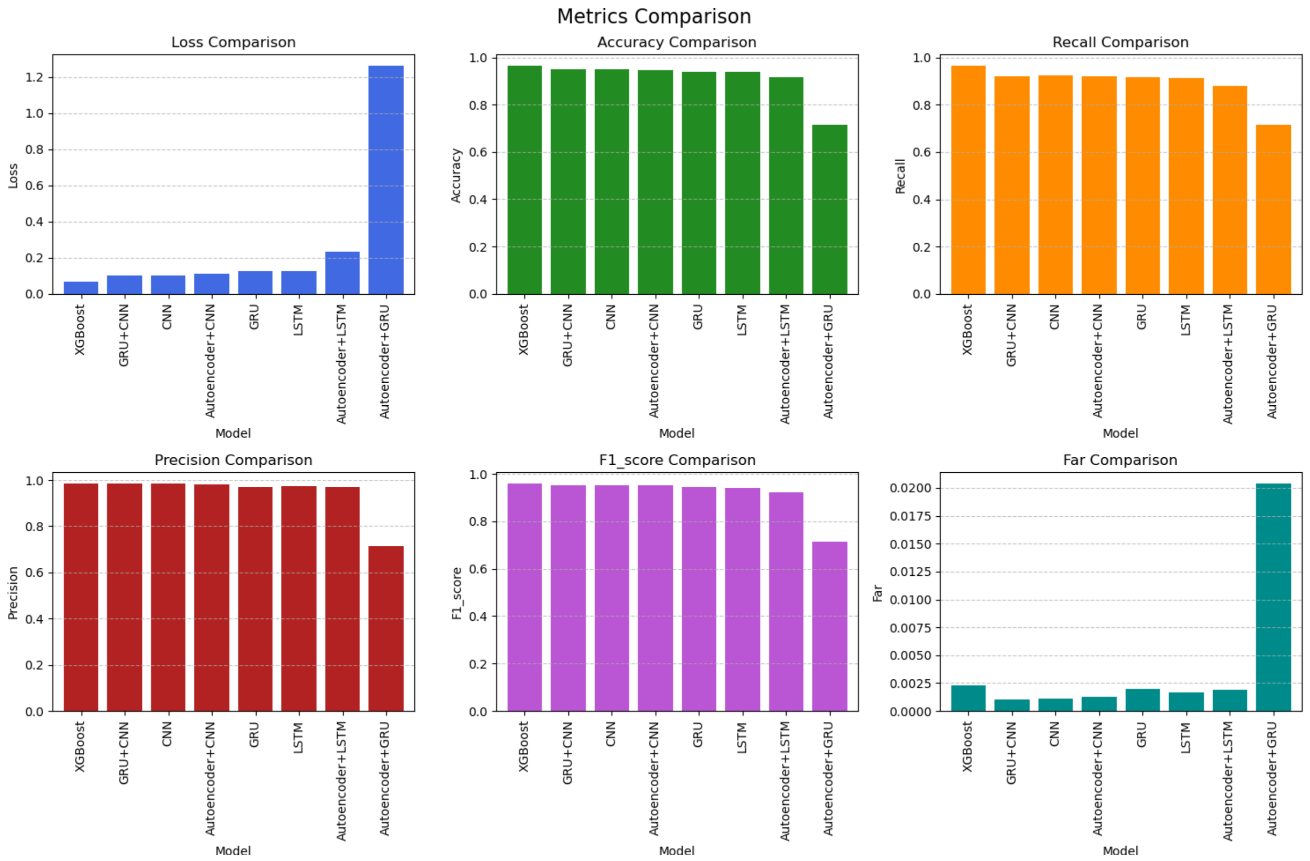


Fig. 23: Individual Comparison of metrics for different models

Such a finding suggests that the CNN model efficiently learned features from the dataset and quickly achieved convergence. The model's ability to capture spatial information through convolutional layers and its simplicity contributed to its swift convergence.

Likewise, the GRU model (Figure 7 and Figure 8) shows an overall decreasing loss trend. However, it's worth noting some training and validation accuracy fluctuations during the training process. Despite these fluctuations, the GRU model exhibited efficient convergence, with an average per-epoch runtime of 35 minutes and 17 training epochs. The GRU architecture, belonging to the family of recurrent neural networks (RNNs), excels at capturing temporal dependencies in sequential data. The model successfully learned the temporal patterns in encrypted IoT traffic, leading to convergence within a reasonable number of epochs. The observed accuracy fluctuations may indicate the model's sensitivity to specific data patterns. The CNN+GRU model, as depicted in Figure 9 and Figure 10, displays a consistently decreasing loss curve paired with a corresponding increase in accuracy. This behavior indicates a steady convergence towards the optimal solution, underscoring the efficacy of merging CNN and GRU architectures for anomaly detection. The CNN+GRU hybrid model, leveraging the strengths of both architectures, exhibited a more extended convergence time than the individual models. It took 97 minutes and 73 training epochs to achieve convergence. The ample convergence time can be attributed to the combined complexity of both architectures and the model's need to extract spatial and temporal features simultaneously. Nevertheless, despite the longer convergence duration, the hybrid model demonstrated superior Performance, highlighting the effectiveness of integrating both CNN and GRU.

Conversely, the LSTM model follows a different trajectory, as shown in Figure 11 and Figure 12. While the Loss decreases gradually over time, there is a notable dip in accuracy during the initial epochs. This pattern may signify a slower convergence rate or difficulties in capturing temporal dependencies in the data. The LSTM model exhibited a slightly slower convergence rate than CNN and GRU, necessitating an average per-epoch runtime of 36 minutes and 14 training epochs to reach convergence. The LSTM's proficiency in modeling long-term dependencies makes it suitable for handling intricate sequential data. However, the added complexity of the LSTM architecture and the extended sequence length present in encrypted IoT traffic likely contributed to the extended convergence duration.

The Autoencoder-based models, namely Autoencoder+CNN and Autoencoder+GRU, displayed distinctive patterns in their training trajectories. As depicted in Figure 13 and Figure 14, the Autoencoder+CNN model initially exhibited a gradual reduction in Loss over a few epochs, followed by a sharp decline, and eventually settled into a gradual decrease until convergence. Conversely, Figure 15 and Figure 16 demonstrate that the Autoencoder+GRU model maintained a consistent loss curve without significant fluctuations. Interestingly, the Autoencoder+LSTM model showed rapid convergence within six epochs, succeeded by a noticeable spike in loss values, indicative of overfitting. These models exhibited diverse convergence behaviors, as their objective is to acquire a compressed version of the dataset through an unsupervised learning approach. The convergence time and number of epochs required for convergence varied based on the autoencoder architecture's intricacy and the reconstruction error optimization. Generally, the convergence time was shorter than the deep learning models, with per-epoch runtimes ranging from 12 to 37 minutes and 7 to 30 training epochs.

In contrast to the Autoencoder-based models, the XGBoost model exhibited a seamless convergence pattern, as depicted in Figure 17. The Loss consistently diminished over the epochs, mirroring the convergence behavior observed in the CNN+GRU model. It also underscores the effectiveness of the XGBoost algorithm in achieving a gradual reduction in Loss and fine-tuning the model's Performance. The XGBoost model, renowned for its proficiency in handling tabular data and excelling in classification tasks, demonstrated efficient convergence with a per-epoch runtime of 16 minutes and a total of 25 training epochs. XGBoost harnesses the power of gradient boosting to optimize the objective function, resulting in rapid convergence and high predictive accuracy.

Figure 24 provides insights into the number of epochs and corresponding training time required by each model, shedding light on their computational efficiency. Models with shorter training times generally exhibit higher efficiency and demand fewer computational resources. A shorter training duration can prove advantageous, especially when dealing with extensive datasets or conducting hyperparameter tuning.

Overall, upon scrutinizing the training curves of the models, it becomes evident that both the CNN+GRU and XGBoost models showcase relatively stable and favorable convergence trends. The CNN+GRU model consistently reduces Loss, while the XGBoost model demonstrates a smooth and steady decline in loss values. These models can be regarded as top performers in convergence and optimization. Conversely, the Autoencoder-based models exhibit diverse convergence behaviors and may warrant further investigation to enhance their Performance and mitigate issues related to overfitting.

In summary, the training curves offer valuable insights into the convergence tendencies of the models. The convergence behaviors of these models varied, influenced by their respective architectures and the complexity of the task. The CNN and GRU models demonstrated comparatively swift convergence, whereas the LSTM, hybrid CNN+GRU model and XGBoost models demanded more time to reach convergence. However, it's worth noting that both the CNN+GRU and XGBoost models displayed desirable convergence patterns. In contrast, the Autoencoder-based models exhibited distinctive patterns that warrant further investigation and attention. Understanding these convergence characteristics aids in evaluating the training stability of the models and pinpointing areas with potential for improvement.

VI. CONCLUSION

In our exploration of deep-learning models for edge IIoT anomaly detection, we have assessed various neural network architectures, including CNN, GRU, CNN+GRU, LSTM, XGBoost, and Autoencoder-based models. The top-performing model is XGBoost, consistently achieving high accuracy (96.41%), precision (98.57%), recall (96.50%), and F1 score (96.03%). The CNN+GRU hybrid model closely follows, with an accuracy of 99.94%. This hybrid model combines CNN's spatial feature extraction with GRU's temporal sequence modeling, proving its effectiveness in capturing the data's local patterns and long-term dependencies.

However, Autoencoder-based models exhibit lower Performance, with an accuracy of 71.43% and limited precision, recall, and F1 scores. This suggests that the unsupervised nature of Autoencoders may need to be revised to identify anomalies in complex edge IIoT data accurately. Further improvements are necessary for these models.

Consideration of computational efficiency is vital for real-world implementation. The CNN model is the most efficient, with faster convergence and shorter training times. In contrast, the CNN+GRU model demands more computational resources but excels in detection performance. Striking a balance between Performance and computational efficiency is crucial for resource-constrained edge IIoT environments. Future work will explore optimization techniques, including data augmentation, to enhance the efficiency and Performance of the CNN+GRU model.

ACKNOWLEDGEMENT

The authors would like to thank the Air Force Research Lab (AFRL) at the US Wright Patterson Air Force Base (WPAFB), Dayton, Ohio under the Assured Digital Microelectronics Education and Training Ecosystem (ADMETE). This grant is awarded to Wright State University, Dayton, Ohio, USA, under the grant number 047814256.

REFERENCES

[1] T. H. A. Musa and A. Bouras, "Anomaly detection: A survey," in *Proceedings of Sixth International Congress on Information and Communication Technology*, X.-S. Yang, S. Sherratt, N. Dey, and A. Joshi, Eds. Singapore: Springer Singapore, 2022, pp. 391–401.

[2] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[3] A. Diro, N. Chilamkurti, V.-D. Nguyen, and W. Heyne, "A comprehensive study of anomaly detection schemes in iot networks using machine learning algorithms," *Sensors*, vol. 21, no. 24, 2021.

[4] H. Li, K. Ota, and M. Dong, "Learning iot in edge: Deep learning for the internet of things with edge computing," *IEEE network*, vol. 32, no. 1, pp. 96–101, 2018.

[5] S. Shadroo, A. M. Rahmani, and A. Rezaee, "The two-phase scheduling based on deep learning in the internet of things," *Computer Networks*, vol. 185, p. 107684, 2021.

[6] M. A. Rahman and M. S. Hossain, "An internet-of-medical-things-enabled edge computing framework for tackling covid-19," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15 847–15 854, 2021.

[7] J. Xiong, S. Bharati, and P. Podder, "Machine and deep learning for iot security and privacy: Applications, challenges, and future directions," *Security and Communication Networks*, vol. 2022, p. 8951961, 2022.

[8] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward edge-based deep learning in industrial internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4329–4341, 2020.

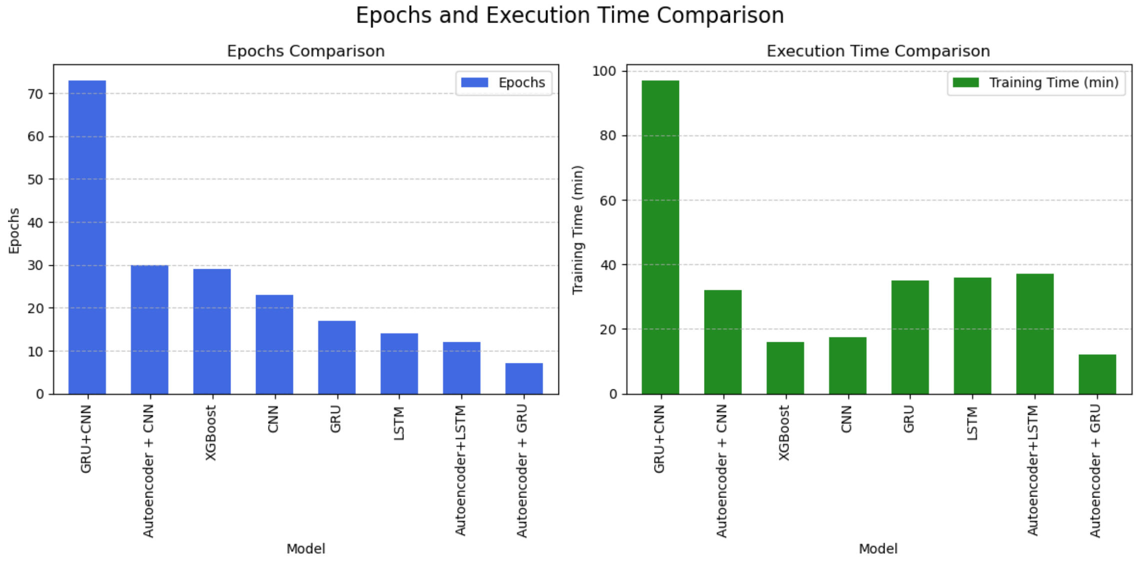


Fig. 24: Training time and epoch for different models

[9] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[10] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019.

[11] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, 2015.

[12] I. Ullah and Q. H. Mahmoud, "Design and development of rnn anomaly detection model for iot networks," *IEEE Access*, vol. 10, pp. 62 722–62 750, 2022.

[13] W. Wu, C. Song, J. Zhao, and Z. Xu, "Physics-informed gated recurrent graph attention unit network for anomaly detection in industrial cyber-physical systems," *Information Sciences*, vol. 629, pp. 618–633, 2023.

[14] R. Kale, Z. Lu, K. W. Fok, and V. L. L. Thing, "A hybrid deep learning anomaly detection framework for intrusion detection," 2022, pp. 137–142.

[15] L. Wen, X. Li, L. Gao, and Y. Zhang, "A new convolutional neural network-based data-driven fault diagnosis method," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 7, pp. 5990–5998, 2018.

[16] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[17] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. Shroff, "Lstm-based encoder-decoder for multi-sensor anomaly detection," 2016.

[18] S. Chauhan and L. Vig, "Anomaly detection in ecg time signals via deep long short-term memory networks," in *2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 2015, pp. 1–7.

[19] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," ser. KDD '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 665–674.

[20] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S. Ng, "Madgan: Multivariate anomaly detection for time series data with generative adversarial networks: 703–716," 2019.

[21] F. De Vita, G. Nocera, D. Bruneo, and S. K. Das, "A novel echo state network autoencoder for anomaly detection in industrial iot systems," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 8, pp. 8985–8994, 2023.

[22] F. Lin, C. Wang, B. Wang, H. Liu, and H. Qu, "Anomaly detection for industrial control system based on autoencoder neural network," *Wireless Communications and Mobile Computing*, vol. 2020, p. 8897926, 2020.

[23] C. Zhang, D. Song, Y. Chen, X. Feng, C. Lumezanu, W. Cheng, J. Ni, B. Zong, H. Chen, and N. V. Chawla, "A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, no. 01, pp. 1409–1416, Jul. 2019.

[24] T.-T.-H. Le, Y. E. Oktian, and H. Kim, "Xgboost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems," *Sustainability*, vol. 14, no. 14, 2022.

[25] M. Shahin, F. F. Chen, A. Hosseinzadeh, H. Bouzary, and R. Rashidifar, "A deep hybrid learning model for detection of cyber attacks in industrial IoT devices," *The International Journal of Advanced Manufacturing Technology*, vol. 123, no. 5, pp. 1973–1983, 2022.

[26] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for iot security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392–3411, 2023.

[27] K. Hayat, T. Bakhshi, and B. Ghita, "Anomaly detection in encrypted internet traffic using hybrid deep learning," *Security and Communication Networks*, vol. 2021, p. 5363750, 2021.

[28] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.

[29] Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, "Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study" International Journal of Advanced Computer Science and Applications(IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969

[30] Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.

[31] Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In 2018 4th International conference on computer and information sciences (ICCOINS) (pp. 1-5). IEEE.

[32] Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.

[33] Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 32(8), e4171.

[34] Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

Bharath Reedy Konatham (Student Member, IEEE) He received a Master of Science in Computer Science from Wright State University in the spring of 2023. His research interests include cyber security in web applications, Applications of ML in IoT, and Security of Automatic Vehicles.

Tabassum Simara She is currently pursuing a master's in computer engineering, at Wright State University. Her research interests include the application of federated learning in the cybersecurity of the Internet of Things, Machine Learning, Embedded systems

Fathi Amsaad (Senior Member, IEEE) is an Assistant Professor of Computer Science and Engineering at Wright State University, Dayton, Ohio, USA. He received the Bachelor's degree in Computer Science from the University of Benghazi, Libya, in 2002. He received a dual Master's degree in Computer Science/ Computer Engineering from the University of Bridgeport, CT, USA, in 2011/ 2012. He received a Ph.D. in Engineering with emphases in Computer Science and Engineering from the University of Toledo, OH, USA, in 2017. He has supervised or currently more than many graduate students, including Tabassum Simra. He established the Semiconductor Microelectronics Assurance, Resilience, and Trust (SMART) Cybersecurity Research Lab at 490 Joshi Research Center, Computer Science and Engineering Department, Wright State University. At the SMART Cybersecurity Research Lab, Dr. Amsaad leads a research team of several graduate students (Master's and Ph.D.), a Postdoctoral Researcher, and a Research Assistant Professor. His research interests include Assured and Trusted Digital Microelecnoces, Secure Heterogeneous Integration and Advanced Packaging, Blockchain-enabled Federated Learning, IoT Hardware Security, Machine/Deep Learning for Cybersecurity, AI Distributed Cloud Computing, Secure AI Hardware Accelerators, and Resilient Circuit Design (Memory/Microprocessor/ASICs/FPGAs). Both government and industry fund Dr. Amsaad's research, including AFRL, AFOSR, Intel, NSA, and the Ohio Department of Education. He has participated in several collaborative research proposals that have led to a cumulative sum of about $33 Million (including all partners along with Wright State University). He has served as an Organizer, Program Chair, Technical Program Committee member, Gust Editor, and on the Reviewer Board for several international conferences and journals. In addition to his research activities, Dr. Amsaad has established teaching experience in hardware security, IoT and embedded systems security, distributed computing, digital systems, network administration, and security curriculum.

.

Mohamed I. Ibrahem received the B.S. and M.S. degrees in Electrical Engineering (electronics and communications) from Benha University, Cairo, Egypt in 2014 and 2018, respectively, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech. University, USA, in 2021. He is an Assistant Professor at the School of Computer and Cyber Sciences, Augusta University, USA. He also holds the position of Assistant Professor at Benha University, Egypt. Dr. Ibrahem received the Eminence Award for the Doctor of Philosophy Best Paper from Tennessee Tech. University, USA. His research interests include machine learning, cryptography and network security, and privacy-preserving schemes for smart grid communication and AMI networks.

Prof. NZ Jhanjhi Prof. Dr. Noor Zaman Jhanjhi (N.Z Jhanjhi) stands as a distinguished senior Professor, Academician, Researcher, and Scientist in the field of Computer Science, specializing in Cybersecurity. Currently holding the position of Professor at the School of Computer Science at Taylor's University, Malaysia, he brings a wealth of experience and expertise to the academic and research landscape. As the Program Director for the Postgraduate Research Degree Programmes in Computer Science and the Director of the Center for Smart Society (CSS5), Prof. Jhanjhi has played a pivotal role in shaping the educational and research landscape at Taylor's University. His leadership has been instrumental in fostering a dynamic environment conducive to cutting-edge research and academic excellence. Prof. Jhanjhi's global recognition as one of the world's top 2underscores his exceptional contributions to the field. In Malaysia, he ranks among the top five computer science researchers, earning him the title of an Outstanding Faculty Member by MDEC Malaysia in 2022. His commitment to advancing knowledge is reflected in his highly indexed publications in prestigious journals such as SCIE/WoS/ISI/SCI/Scopus, boasting a collective research impact factor exceeding 900 points. Prof. Jhanjhi has made significant contributions to literature, editing/authoring over 45 research books published by esteemed publishers, including Springer, Taylor and Francis, Wiley, Intech Open, IGI Global USA, among others. In addition to his prolific publications, Prof. Jhanjhi has displayed outstanding mentorship, supervising and co-supervising a notable number of postgraduate students. Over 37 scholars have successfully graduated under his guidance, a testament to his commitment to nurturing the next generation of scholars. His expertise extends to serving as an external Ph.D./Master thesis examiner/evaluator for several universities worldwide, having evaluated over 60 theses. Prof. Jhanjhi's editorial roles in reputable journals, including Associate Editor and Editorial Assistant positions for journals like PeerJ Computer Science, CMC Computers, Materials Continua, CSSE, Frontier in Communication and Networks, reflect his standing in the academic community. Notably, he has been honored with the Outstanding Associate Editor award for IEEE ACCESS. Prof. Jhanjhi's commitment to advancing research is evident in his successful completion of more than 40 internationally funded research grants. As a sought-after keynote and invited speaker, he has shared his insights in over 60 international conferences and has chaired various conference sessions. With a rich academic background, including accreditation experience in ABET, NCAAA, and NCEAC for a decade.