future internet

MDPI

Article

Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids

Fouzi Harrou [1,*], Benamar Bouyeddou [2], Abdelkader Dairi [3,*] and Ying Sun [1]

[1] Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia; ying.sun@kaust.edu.sa
[2] LESM Laboratory, Department of Telecommunications, Faculty of Technology, University of Saida-Dr Moulay Tahar, Saida 20000, Algeria; benamar.bouyeddou@univ-saida.dz
[3] Computer Science Department, University of Science and Technology of Oran-Mohamed Boudiaf (USTO-MB), El Mnaouar, BP 1505, Oran 31000, Algeria
* Correspondence: fouzi.harrou@kaust.edu.sa (F.H.); abdelkader.dairi@univ-usto.dz (A.D.)

Abstract: The evolution of smart grids has led to technological advances and a demand for more efficient and sustainable energy systems. However, the deployment of communication systems in smart grids has increased the threat of cyberattacks, which can result in power outages and disruptions. This paper presents a semi-supervised hybrid deep learning model that combines a Gated Recurrent Unit (GRU)-based Stacked Autoencoder (AE-GRU) with anomaly detection algorithms, including Isolation Forest, Local Outlier Factor, One-Class SVM, and Elliptical Envelope. Using GRU units in both the encoder and decoder sides of the stacked autoencoder enables the effective capture of temporal patterns and dependencies, facilitating dimensionality reduction, feature extraction, and accurate reconstruction for enhanced anomaly detection in smart grids. The proposed approach utilizes unlabeled data to monitor network traffic and identify suspicious data flow. Specifically, the AE-GRU is performed for data reduction and extracting relevant features, and then the anomaly algorithms are applied to reveal potential cyberattacks. The proposed framework is evaluated using the widely adopted IEC 60870-5-104 traffic dataset. The experimental results demonstrate that the proposed approach outperforms standalone algorithms, with the AE-GRU-based LOF method achieving the highest detection rate. Thus, the proposed approach can potentially enhance the cybersecurity in smart grids by accurately detecting and preventing cyberattacks.

Keywords: cyberattack detection; protocol IEC 104; deep learning; semi-supervised methods; anomaly detection

Citation: Harrou, F.; Bouyeddou, B.; Dairi, A.; Sun, Y. Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids. *Future Internet* **2024**, *16*, 184. https://doi.org/10.3390/fi16060184

Academic Editors: Christos Tryfonopoulos and Nicholas Kolokotronis

Received: 3 May 2024
Revised: 17 May 2024
Accepted: 20 May 2024
Published: 22 May 2024

1. Introduction

With the rapid digitization of energy infrastructure, cybersecurity has become a critical concern for smart grids [1]. Due to their interconnected nature, the use of advanced communication and information technologies to enhance efficiency, reliability, and sustainability renders smart grids increasingly vulnerable to cyber threats. Smart grids, envisioned as the future of power grids, integrate advanced technologies such as sensors, automation, and communication systems for real-time monitoring and control [2,3]. They facilitate quicker problem identification and support demand response programs, renewable energy integration, and operation in diverse environments with adaptable technologies like Industrial Internet of Things (IIoT), cloud computing, and Software-Defined Networking (SDN). Components such as sensors, meters, controllers, and communication networks provide numerous entry points for potential attackers, leading to severe consequences such as power disruptions and the compromise of critical infrastructure. Ensuring the integrity and resilience of smart grid systems necessitates innovative cybersecurity measures tailored to the evolving threat landscape [4].

Nevertheless, the growing dependence on vulnerable advanced communication systems and highly connected devices has heightened smart grids' vulnerability to cyberattacks and malicious activities [5]. As a result, cyber attackers have a broadened attack surface within the smart grid ecosystem, targeting insecure communication networks, outdated software, weak authentication, and other vulnerabilities [3,5]. Indeed, a successful cyberattack on a smart grid can cause major disruptions to power generation and distribution, endangering public safety via widespread outages. Moreover, such attacks can compromise sensitive information's confidentiality, integrity, and availability, including customer data, financial records, and critical infrastructure data [6]. Various types of cyberattacks can be launched against smart grids, including Man-in-the-middle (MitM), False data injection, DoS/DDoS (Denial of Service/Distributed Denial of Service), Insider attacks, Phishing attacks, Malware attacks, and physically damaging or sabotaging smart grid components. For example, significant cyberattacks occurred in recent years, targeting Iran's nuclear centrifuges (2010), the Ukrainian power system (2015), the US power grid (2019), Energie de Portugal (2020), and a Ukrainian energy company (2022) [5,7].

Ensuring cybersecurity is essential for the successful deployment and operation of smart grids. This includes implementing security protocols, deploying intrusion detection and prevention systems, training personnel on cybersecurity best practices, and continuously monitoring and updating the smart grid systems. Consequently, machine learning (ML) has emerged as a popular method to detect and prevent cyberattacks in smart grids [8]. ML algorithms analyze vast amounts of operational data and identify unusual behaviors in network traffic, enabling them to detect potential security threats and alert the system administrators. As a result, ML plays a crucial role in maintaining the security and reliability of smart grid systems. Various ML-based approaches, including supervised, unsupervised, and semi-supervised learning, have been researched to defend against different types of cyberattacks. For example, An et al. [9] devised a detection approach using a deep-Q-network (DQN) to safeguard AC power systems against data integrity attacks (DIA). Their study showed that the DQN-based detection approach surpassed the standard methods in regard to accuracy and speed. Sakhnini et al. [10] examined three distinct algorithms—Artificial Neural Networks (ANNs), k-Nearest Neighbor (KNN), and Support Vector Machine (SVM)—incorporating various feature selection (FS) techniques, particularly the genetic algorithm (GA), which proved to be the most efficient FS method. Hink et al. [11] explored ML-based techniques to differentiate among regular operations, cyber-attacks, and natural disturbances in smart grids, evaluating algorithms like Random Forest (RF), Naïve Bayes (NB), SVM, and AdaBoost. Esmalifalak et al. [12] tackled stealthy false-data injection attacks using Principal Component Analysis (PCA)-based dimensionality reduction and SVM trained over labeled data for detection. Ahmed et al. [13] introduced an unsupervised Isolation Forest (iForest) algorithm for detecting covert data-integrity exploits using unlabeled historical data of State Estimation Measurement Features (SE-MF) and a PCA-based data reduction technique. Acosta et al. [14] addressed the detection of stealthy attacks in large-scale smart grid networks by applying Kernel PCA (KPCA) to solve the computational complexity issues. The output data from KPCA were fed into the Extra-Trees algorithm. Al-Qudah et al. [15] presented an integrated solution combining one-class classification (OCSVM) with PCA for the accurate detection of memory dump malware, including novel types. Menon et al. [16] proposed an unsupervised K-means-based model to identify Denial of Service (DoS) attacks, such as UDP and ICMP flood attacks, directed at the AMI network. The model, relying on unlabeled data, successfully clustered both normal and abnormal behaviors.

The evolution of smart grids has spurred technological advancements and an increasing demand for more efficient and sustainable energy systems. However, the integration of communication systems into smart grids has escalated the risk of cyberattacks, potentially leading to power outages and system disruptions. This paper introduces a semi-supervised approach for detecting malicious attacks in Industrial Control Systems (ICSs) and Supervisory Control and Data Acquisition (SCADA) networks. Unlike traditional supervised

learning, which relies on labeled data, this method utilizes only attack-free data for training. This eliminates the need for costly and time-consuming manual labeling, making it more practical and cost-effective for real-world deployment. By learning from attack-free data, the model can effectively identify deviations from normal behavior during testing, without the need for explicit labels. This approach simplifies the training process and reduces the risk of bias introduced by human labeling errors. The contributions of this study are summarized next.

- Firstly, a hybrid deep learning approach is proposed for detecting the cyberattacks in smart grids. Specifically, we introduce the Autoencoder (AE)-Gated Recurrent Unit (GRU) approach, integrating two stacked GRU layers into the AE model's encoder and decoder. By incorporating GRU units into both the encoder and decoder sides, the model learns compact representations of sequential smart grid data while ensuring minimal loss in data reconstruction. For cyberattack detection, the AE-GRU approach is combined with semi-supervised anomaly detection methods, including Isolation Forest (IF), Local Outlier Factor (LOF), OCSVM, and Elliptical Envelope (EE). Initially, the AE-GRU approach extracts pertinent features from the data, seamlessly integrated with semi-supervised techniques (IF, OCSVM, EE, and LOF) to detect anomalies effectively. Specifically, AE-GRU handles data reduction and feature extraction, followed by applying anomaly detection algorithms to identify potential cyberattacks.
- The effectiveness of these approaches was evaluated based on the IEC 60870-5-104 (IEC 104) control communication protocol, commonly used in SCADA networks to manage critical infrastructures such as power stations. The IEC 104 protocol is widely used in smart grid environments for the exchange of control and monitoring information between various devices and systems. This protocol facilitates the communication between different components of the power grid, including sensors, actuators, controllers, and SCADA systems. The proposed framework's effectiveness was assessed using the widely adopted IEC 60870-5-104 traffic dataset, which includes various types of malicious attacks such as DOS, Switch, Injection, ConnLoss, and Rogue Dev. We employed four statistical indices—accuracy, precision, F1-score, and the Area Under the Curve (AUC)—to compare the discrimination accuracy of the considered methods. The experimental results demonstrate that the proposed approach outperforms standalone algorithms, with the AE-GRU-based LOF method achieving the highest detection rate. This underscores the potential for the proposed approach to enhance the cybersecurity in smart grids by accurately detecting and mitigating cyber threats.

The remaining sections of this paper are structured as follows: Section 2 discusses the related works on deep learning-based detection approaches for cyberattacks in smart grids. Section 3 provides a detailed description of the proposed framework. The performance evaluation experiments and detection results are presented in Section 4. The paper concludes in Section 5, followed by an outline of future work.

2. Related Works

DL algorithms have proven effective across various domains, including image recognition, speech processing, and anomaly detection. DL effectively analyzes data from sensors, control systems, and communication networks within smart grids. Recent interest focuses on using DL for cyberattack detection in smart grids, with studies exploring its application [17–19]. This section provides an overview of DL-based attack detection in smart grids.

In [20], Haghshenas et al. introduced a Temporal Graph Neural Network (TGNN) architecture to detect FDI and ramp attacks. It constructs a temporal graph, utilizes a three-layer GNN with GRU units to learn normal behavior, and employs a graph attention mechanism for attack localization. However, the model's assumption of temporal sequencing in cyberattacks may not always hold, posing challenges for detection and localization. Khanna et al. [21] introduced an approach to detect compromised meters in smart grids using the KLD (Kullback–Leibler distance), ANNs (Artificial Neural Networks), and ELMs

(Extreme Learning Machines). The KLD quantifies the dissimilarity between historical and real-time measurements to identify anomalies that signal data integrity attacks. ANNs and ELMs accurately predict the current loads and identify compromised meters based on an error threshold. In [22], Karimipour et al. introduced an unsupervised model-free method based on Symbolic Dynamic Filtering (SDF) for feature extraction, a Dynamic Bayesian Network for transition probabilities, RBM for learning behavior patterns, and a Relative Entropy (RE) metric for anomaly detection. The accuracy of the framework may vary due to different symbolization methods for time series data. Qiu et al. [23] introduced the SG-FST-MCNN, a multi-view convolutional neural network (MCNN), for authenticating DSD (Distribution Synchrophasor Data) sources and detecting spoofing attacks. It utilizes Savitzky–Golay (SG) filter and fast S transform (FST) for feature extraction, followed by MCNN for classification without manual feature selection. However, an SG filter and FST assume linearity, which may limit their effectiveness with non-linear data. The study in [24] introduced a two-stage deep learning framework utilizing image recognition models to detect and locate attacks in multivariate time-series data. The framework converts data into 2D images using the Gramian Angular Field (GAF) and Recurrence Plot (RP) techniques and trains a multi-label CNN classifier for attack detection and localization. However, this approach is computationally demanding, presenting challenges for real-time detection.

Shan et al. [25] targeted DDOS attacks using the Autoencoder (AE) algorithm. They utilized a multi-level mixture of shallow and deep marginalized stacked denoising autoencoders (MSDA) for feature extraction. These features were projected into a kernel space, where the Multiple Kernel Learning for Dimensionality Reduction (MKLDR) algorithm trained the detection model. However, MKLDR faces challenges in selecting suitable kernels and has limited scalability for large or high-dimensional datasets. Dou et al. [26] proposed a detection method that combines Variational Mode Decomposition (VMD) and OS-Extreme Learning Machines (OSELMs) to identify abnormal power system states. This approach extracts multiscale modes and analyzes statistical features to assess irregular behaviors. An OSELM correlates these features with the power system security status and identifies abnormal states. However, the effectiveness of the F-test may be limited by assumptions, particularly the handling of outliers and non-normal data distributions in real-world settings. Lu et al. [27] focused on intrusion detection in Advanced Metering Infrastructure (AMI) using a Stacked Autoencoder (SAE) and Long Short-Term Memory (LSTM) models. A SAE reduced the input feature dimensionality, while the Bi-directional LSTM (BiLSTM) identified abnormal traffic patterns. An attention mechanism assigns weight coefficients to important features, enhancing the classification accuracy. Qi et al. [28] exploited Phasor Measurement Unit (PMU) data to detect cyberattacks by employing the deep autoencoder (DAE) and semi-supervised anomaly detection techniques. Such an approach may not be effective when changing the data distribution or when there is insufficient information in unlabeled data. Ferrag et al. [29] developed DeepCoin, integrating blockchain with a recurrent neural network (RNN) to secure smart grid transactions while preserving privacy. DeepCoin employs practical Byzantine fault tolerance for blockchain consensus and RNN to verify security requirements and prevent cyberattacks.

3. AE-GRU Anomaly Detection Framework

In this section, an overview of the materials needed to develop the proposed AE-GRU-based detection scheme is provided, including the Autoencoder, GRU, and semi-supervised anomaly detection methods.

3.1. Auto-Encoders

An autoencoder, a type of neural network architecture widely employed in tasks such as dimensionality reduction, feature learning, and data compression, is particularly valuable in cybersecurity applications [30]. An autoencoder comprises two main components: an encoder network and a decoder network (Figure 1). The encoder network compresses

input data into a latent space representation, whereas the decoder network reconstructs the original input based on this compressed representation.

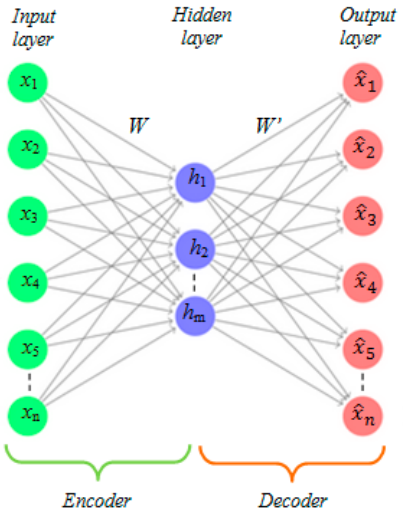

Figure 1. Fundamental structure of an autoencoder (AE).

The encoding stage of an autoencoder is pivotal in compressing input data, $x = \{x_1, x_2, \ldots, x_n\}$, into a lower-dimensional latent space representation, $h = \{h_1, h_2, \ldots, h_m\}$, which contains essential features and patterns for efficient reconstruction by the decoder stage. This transformation involves applying a linear transformation to the input, followed by a non-linear activation function, represented mathematically as [31]:

$$h = f(x) = A_f(Wx + b), \tag{1}$$

where W denotes the weight matrix, b represents the bias vector, and A_f is the activation function applied element-wise. In the decoding stage, the compressed representation h from the encoding stage is transformed back into the original input data space. This process involves applying a series of hidden layers to h, each involving a linear transformation followed by a non-linear activation function, represented mathematically as [31,32]:

$$\hat{x} = g(h) = A_g(W'h + b'), \tag{2}$$

where W' is the weight matrix, b' is the bias vector, and A_g is the activation function. The output of this transformation, $\hat{x} = \{\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n\}$, represents the reconstructed input data. The goal of the decoding stage is to generate a reconstruction that closely matches the original input data x, thereby capturing the essential features and patterns encoded in the compressed representation h.

During training, an AE adjusts the parameters such as weights and biases to minimize the difference between the input data and their reconstructed output. This iterative process utilizes optimization algorithms like the stochastic gradient descent (SGD) algorithm to update the parameters and minimize a chosen loss function. Cross-entropy is widely used as a loss function in autoencoders for its effectiveness in capturing the differences between the input and reconstructed data distributions. It is expressed as [32]:

$$L_{BCE} = \frac{1}{M}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[x_{j,i} log \hat{x}_{j,i} + (1 - x_{j,i}) log(1 - \hat{x}_{j,i})\right], \tag{3}$$

where M represents the number of training samples or instances, and $x_{j,i}$ denotes the j-th feature of the i-th training instance. In cybersecurity, autoencoders trained on normal data learn patterns and structures. Deviations from these learned patterns during inference can signal anomalies or cyber threats.

3.2. GRUs (Gated Reccurent Units)

A GRU is a type of recurrent neural network (RNN) designed to mitigate the vanishing gradient problem commonly encountered in traditional RNNs [33]. Introduced by Cho et al. in 2014, GRUs employ gating mechanisms to selectively control information flow, reducing the risk of gradient vanishing or exploding during training [34]. Specifically, GRUs consist of two main components: the update gate and the reset gate (Figure 2). The update gate determines how much of the previous hidden state to retain and how much of the new input to incorporate, while the reset gate determines how much of the previous hidden state to forget and how much of the new input to focus on [35].

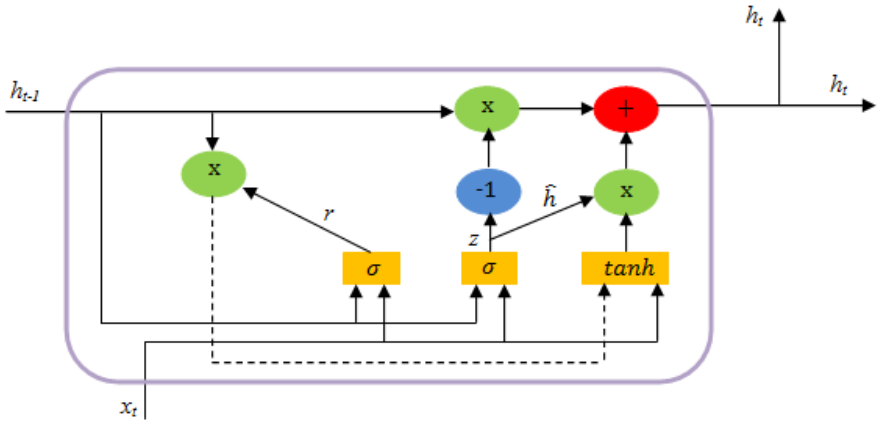

Figure 2. General representation of a GRU.

For the input data $x_t = \{x_1, x_2, \ldots, x_n\}$ and state $h_t = \{h_1, h_2, \ldots, h_m\}$ vectors at time t, the update gate z_t is computed as [36]:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z), \quad (4)$$

where W_z and U_z represent the weight matrix, and σ is the activation sigmoid function. The reset gate r_t in Equation (8) controls how much of the previous hidden state to forget [36].

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r), \quad (5)$$

These gates are combined using element-wise multiplication to determine the updated hidden state. The output of the GRU is then computed based on a combination of the current input and the updated hidden state [36]:

$$h_t = z_t \odot h_{t-1} + (1 - z_t) \odot \hat{h}_t, \quad (6)$$

$$\hat{h}_t = \tanh(W_h x_t + U_h(h_{t-1} \odot r_t)), \quad (7)$$

where h_t is the hidden state at time step *t* and $\hat{h}$ is the candidate hidden state, representing the proposed update to the current hidden state. GRUs typically provide similar capabilities to LSTM units but with fewer parameters, ensuring computational efficiency while effectively capturing the long-term dependencies in sequential data.

3.3. Hybrid AE-GRU

In this section, we introduce the hybrid AE-GRU model, which combines the advantages of AE and GRU architectures to improve the cybersecurity measures in smart grids. The AE-GRU model is designed to encode time-series data effectively, aiming to mitigate the potential cyber threats. The AE-GRU model integrates two stacked GRUs within both the encoder and decoder components (Figure 3). This configuration enables the model to capture the intricate temporal patterns and anomalies present in smart grid data. By leveraging the sequential nature of GRUs, the model can efficiently extract features from the

input data and reconstruct normal traffic patterns. The primary objective of the AE-GRU model is to minimize the reconstruction error, typically measured using metrics like Binary Cross-Entropy (BCE) [31]. This metric evaluates the dissimilarity between the original input data and the reconstructed output. By reducing the reconstruction error, the AE-GRU model enhances its ability to accurately capture and represent the underlying structure of the smart grid data.

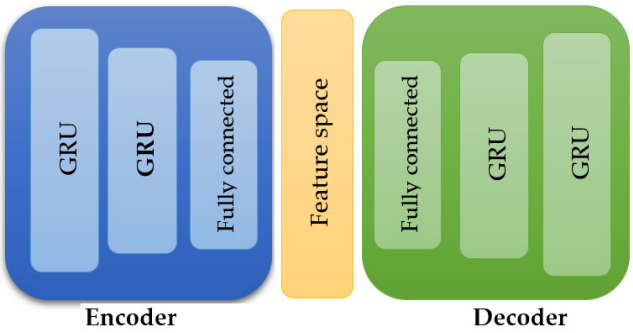

Figure 3. Architecture of the proposed hybrid AE-GRU model.

The integration of the AE-GRU model represents a proactive measure to enhance the cybersecurity in smart grids. By effectively encoding the time-series data, the model can be used in conjunction with semi-supervised anomaly detection methods to identify potential cyber threats, such as malicious attacks or anomalies in system behavior.

3.4. Semi-Supervised Algorithms

The primary objective of the detection stage is to differentiate between regular and unusual traffic routed in the smart grid. In this study, four semi-supervised anomaly detection techniques were explored: a One-Class Support Vector Machine (1SVM), Local Outlier Factor (LOF), Isolation Forest (iF), and Elliptic Envelope (EE). These methods are designed to detect the anomalies in data without requiring labeled instances of anomalies during training. In other words, these methods were developed using a semi-supervised training approach, which involves training only with normal data (i.e., attack-free data).

- A One-Class SVM is a machine learning algorithm used for anomaly detection, particularly in cases where only normal data are available for training. It works by constructing a hyperplane in a high-dimensional space that encapsulates the normal data points. This hyperplane should ideally separate the normal data from the rest of the feature space which contains anomalies [37,38]. During training, the algorithm learns to maximize the margin around the normal data points while minimizing the possibility of including anomalies within this margin. During inference, data points lying outside this margin are classified as anomalies [39].
- Isolation Forest (iF) is an ensemble learning method designed for outlier detection. It constructs a set of isolation trees, each of which partitions the feature space by randomly selecting a feature and a split value. Anomalies are expected to be isolated in fewer partitions compared to the normal data points [40]. Therefore, they require fewer splits to be separated from the majority of the data. The algorithm measures the average path length for each data point in the trees. The shorter average path lengths indicate anomalies, while the longer path lengths suggest normal data [41].
- An Elliptic Envelope (EE) is a statistical method used for multivariate outlier detection assuming that the normal data points are located within a tightly bound elliptical region. The algorithm fits an ellipse to the data using robust covariance estimation techniques [42]. Data points lying outside the ellipse are considered outliers, as they deviate significantly from the expected distribution of normal data. The EE method is particularly useful when the normal data follow a Gaussian distribution and when the dimensionality of the data is relatively low [41].

- The LOF method comprises a density-based anomaly detection algorithm that measures the local density deviation of a data point with respect to its neighbors. It operates under the assumption that anomalies have lower densities compared to their neighbors, resulting in higher LOF scores [43]. The LOF score of a data point is computed based on the ratio of the local density of the point to the average local density of its neighbors. Data points with significantly higher LOF scores compared to their neighbors are considered outliers.

Table 1 provides a concise overview of the characteristics of these four anomaly detection methods. These approaches offer different strategies for identifying the anomalies in data and can be applied depending on the specific characteristics of the dataset and the nature of the anomalies being targeted.

Table 1. Comparison of the four semi-supervised anomaly detection methods.

Approach	Basic Idea	Pros	Cons
1SVM	Constructs a hyperplane to encapsulate normal data and separates it from anomalies.	- Effective for high-dimensional data - Works well with small training data	- Sensitive to parameter tuning - Slow training on large datasets
LOF	Measures the local density deviation of a data point with respect to its neighbors.	- Robust to outliers and noise - Does not assume a specific data distribution	- The computational complexity increases with dataset size - Parameter selection can be challenging
Isolation Forest (iF)	Constructs isolation trees to isolate anomalies with fewer splits than normal data.	- Efficient for high-dimensional data - Fast training and inference	- Prone to overfitting with noisy data - Limited interpretability
Elliptic Envelope (EE)	Fits an ellipse to the data and detects outliers outside the ellipse.	- Robust to multivariate outliers - Effective for low-dimensional data	- Assumes a Gaussian distribution of normal data - Limited applicability to non-Gaussian data

3.5. The Proposed AE-GRU-Driven Anomaly Detection Framework

This section provides a brief overview of the proposed anomaly detection framework for detecting the cyberattacks in smart grids, specifically focusing on monitoring network traffic data, mainly focusing on the IEC 104 protocol communication. This protocol is commonly used for exchanging control and monitoring information between the devices in smart grids. By focusing on IEC 104 data, the framework specifically targets the communication within the smart grid control system, potentially leading to more accurate anomaly detection compared to analyzing general network traffic. To effectively model the distribution of normal traffic, it is imperative to capture the temporal data dependencies

inherent in data sequences and time-series data. The proposed deep learning model is designed to achieve this by integrating the AE with the GRU model, which is renowned for its ability to learn long-range dependencies, into its structure. Within this framework, the autoencoder (AE) plays a pivotal role, performing two critical tasks: feature extraction and dimensionality reduction. Through the training process, the deep AE constructs a compact representation of the data, incorporating the relevant features and reducing the dimensionality. By combining the robustness of deep autoencoders with the effectiveness of recurrent neural networks, the AE-GRU model can effectively capture lengthy time-period dependencies. Importantly, this method is agnostic to the communication standard employed in the smart grid network, allowing for versatility across various standards. For the purposes of this study, the proposed cyberattack detection procedure was evaluated using the IEC-104 standard. The process flow is depicted in Figure 4, illustrating the two phases: training and detection. Data preprocessing involves the removal of missing values and standardization of numeric features. Subsequently, during the training phase, the AE-GRU model and anomaly detection procedures are trained using attack-free data. The trained model is then evaluated using testing data to assess its performance.

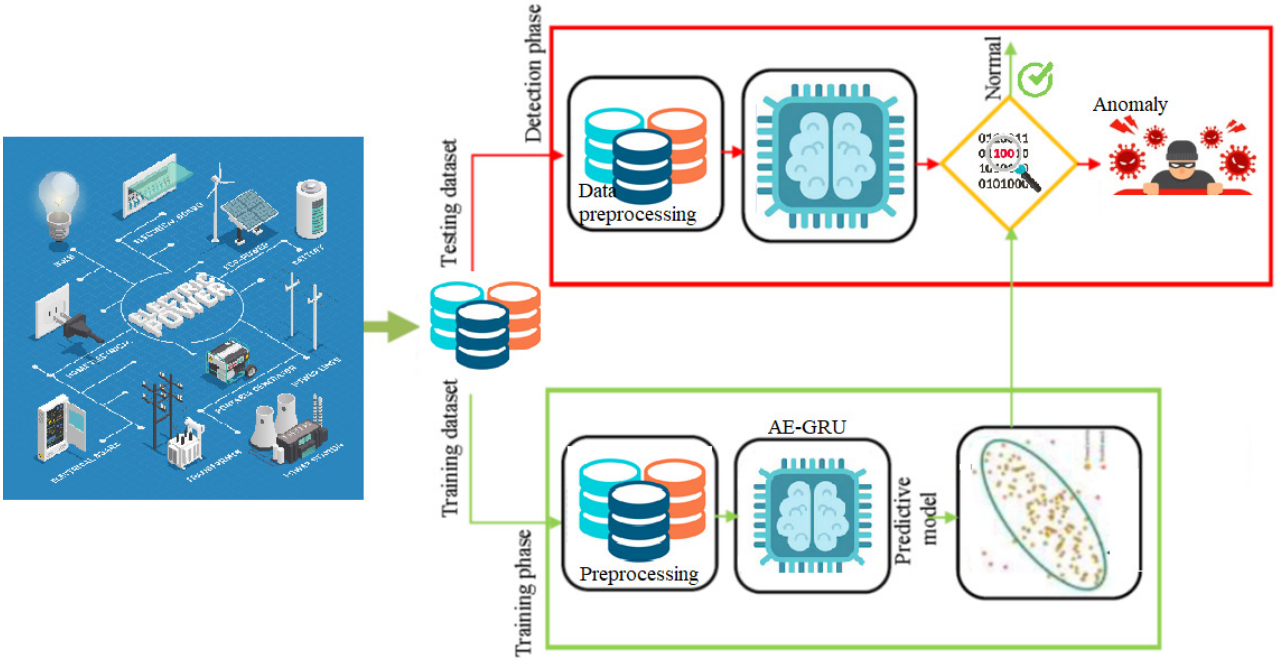

Figure 4. Flowchart of the AE-GRU based detection framework.

During the training stage, the data are normalized and organized into sequences of specific lengths. Encoding these sequences generates a compact representation containing the essential features, with the training process aiming to minimize the reconstruction error using the cross-entropy loss function. This iterative process continues until the model converges and the reconstruction error stabilizes. The resulting feature space contains normal traffic communications without any attacks, which is utilized to train the anomaly detection methods considered in this study.

The anomaly detection methods are trained on the feature space obtained from encoding the normal data. When a data sequence corresponds to a specific attack category, its numerical signature is encoded using the model parameters learned from the normal data. Consequently, any deviation from the encoding of the normal data can be detected by the anomaly detectors.

The performance of the designed framework was assessed using four widely used statistical metrics: Accuracy, Precision, Recall, and F1-score. In a binary detection scenario,

these metrics are calculated based on the number of true positives (TP), false positives (FP), false negatives (FN), and true negatives (TN).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}, \tag{8}$$

$$Recall = \frac{TP}{TP + FN}, \tag{9}$$

$$Precision = \frac{TP}{TP + FP}, \tag{10}$$

$$F1 - score = 2\frac{Precision - Recall}{Precison + Recall} = \frac{2TP}{2TP + FP + FN}, \tag{11}$$

Before presenting the results, the next section provides an overview of the IEC 608705-104 protocol and its significance in SCADA systems, particularly in smart grid networks.

3.6. An Overview of the IEC-60780-5-104 Protocol

The IEC 60870-5-104 (IEC 104) protocol is a fundamental component of SCADA networks, which is pivotal in managing and overseeing critical infrastructures such as power stations [44]. Designed to enable seamless communication between control centers and substations, IEC 104 facilitates real-time monitoring, control, and data acquisition within power grid systems. Its adoption has become widespread due to its ability to ensure the reliable and efficient transmission of data, essential for maintaining the stability and functionality of power distribution networks. Unlike its predecessor, the IEC 60870-5-101 protocol, IEC 104 operates at higher speeds, allowing for faster and more responsive communication between substations and control centers. This enhanced speed is crucial for meeting the demands of the modern power grid operations, where rapid decision-making and real-time data exchange are paramount.

The architecture of the IEC 104 protocol follows a client–server model, where substations act as servers and control centers act as clients. This structure enables bidirectional communication, facilitating the exchange of control commands, status information, and measurement data between the different components of the power grid infrastructure [45]. IEC 104 relies on standard networking protocols such as the Transmission Control Protocol (TCP) and Internet Protocol (IP) for data transmission. This reliance on widely accepted networking standards ensures the compatibility with the existing network infrastructure and simplifies the integration into modern communication networks. In addition to defining the communication procedures and data formats, the IEC 104 protocol also specifies various data types tailored to the specific requirements of power grid applications. These data types encompass a wide range of parameters, including analog values, binary states, and control commands, allowing for the comprehensive monitoring and control of the power grid operations.

While the IEC 104 protocol offers robust communication capabilities, it is not immune to cybersecurity threats [46]. As the power grid systems become increasingly interconnected and digitized, the protocol's vulnerabilities may be exploited by malicious actors seeking to disrupt operations or compromise the sensitive infrastructure. Therefore, understanding the intricacies of the IEC 104 protocol is essential for developing effective cybersecurity strategies and implementing robust anomaly detection techniques to safeguard the critical power grid assets against potential cyberattacks.

4. Threat Scenarios and Results

This section provides an overview of the utilized 4.1 BUT-IEC104-I Dataset, followed by presenting the detection results based on the AE-GRU-based methods and the considered standalone anomaly detection approaches.

4.1. BUT-IEC104-I Dataset

The BUT-IEC104-I dataset provides a valuable resource for cybersecurity research, particularly for assessing the anomaly detection methods within the context of the IEC 60870-5-104 (IEC 104) communication protocols. Developed by Matousek et al. [47,48] from Brno University of Technology, this dataset consists of network traffic traces collected from a real-world smart grid environment that conforms to the industrial network standard, IEC 608705-104. It simulates the realistic scenarios encountered in power grid operations. The traffic was monitored using an IPFIX sniffer, capturing IPFIX flow and application protocol headers. The dataset includes various traffic characteristics, such as IP addresses, ports, object IDs, as well as attributes like start and end times and data exchange quantity. Each line in the dataset captures a range of headers extracted from the IEC 104 packet, totaling 16 features. These include the timestamp (absolute time) and relative time (in seconds from the start of capturing), as well as source and destination IP addresses, ports, IP length (from the IP header), and APDU length (from the IEC 104 header). Additionally, features such as the APDU format type, u-format type (including start data transfer, stop data transfer, test frame activation, test frame confirmation, stop data transfer action, and stop data transfer confirmation), and ASDU type identification (e.g., single point information, interrogation command) are recorded. These headers provide detailed information on the ASDU packet, including the number of Information Objects within it, the cause of transmission (e.g., periodic, spontaneous), originator address, ASDU address field, and Information Object Address—a list of addresses of Information Objects present in the ASDU. It covers a range of benign and malicious activities, including denial-of-service (DoS) attacks, injection attacks, connloss attacks, and rogue device attacks. For further details about the BUT-IEC104-I dataset, see [47,48].

Each instance in the dataset consists of a sequence of network packets exchanged between the different components of the smart grid, such as substations and control centers, encoded according to the IEC 104 protocol standards. The packets contain information about the command and data exchanges, status updates, and control signals, reflecting the operational activities typical in power grid systems. To facilitate the evaluation of the anomaly detection methods, the dataset is annotated with labels indicating the presence or absence of malicious activity in each network traffic instance. This annotation enables researchers to assess the performance of the anomaly detection algorithms in accurately distinguishing between normal and malicious behaviors. Furthermore, the dataset includes metadata providing additional contextual information, such as timestamps, source and destination addresses, packet sizes, and communication patterns. This metadata enhances the understanding of the underlying network dynamics and aids in analyzing the detected anomalies. The dataset contains not only normal traffic but also various types of attack events, including DOS attacks, switching attacks, injection command attacks, and connection loss attacks.

All attacks were intentionally generated at the L7 layer, also known as the application layer, of the OSI (Open Systems Interconnection) model. The application layer is the topmost layer in the OSI model and provides network services directly to user applications. Attacks at this layer can exploit the vulnerabilities in the specific applications or protocols running on top of the network stack. By generating attacks at the application layer, the aim was to simulate realistic cyber threats that target smart grid networks. These attacks include various forms of malicious activities, such as denial-of-service (DoS) attacks, injection attacks, command blocking, switching attacks, and other network intrusions. Attacking the application layer allowed for the assessment of the effectiveness of the anomaly detection methods in detecting and mitigating these threats. It also enabled the evaluation of the robustness of the detection framework in identifying the anomalies within the application-level traffic of smart grid networks. The attack traces were generated during the Bonnet research project from 2019 to 2022. More details are available at https://www.fit.vut.cz/research/project/1303/ (accessed on 20 May 2024).

Overall, the BUT-IEC104-I dataset serves as a comprehensive and realistic benchmark for evaluating the efficacy of the anomaly detection techniques in safeguarding smart grid infrastructures against cyber threats. Its diverse composition and detailed annotations make it a valuable resource for advancing the research in power grid cybersecurity.

4.2. Detection Results

The anomaly detection methods were trained using normal IEC 104 communication data (attack-free data), which consisted of 58,930 packets collected over a period of 2 days, 19 h, and 55 min. This approach was chosen because the proposed methods are semi-supervised, eliminating the need for labeled data. From each traffic sample, 16 key attributes were extracted, including source and destination IP addresses, as well as port numbers. During the training, the parameters of each method were adjusted to minimize the cross-entropy of the reconstructed error, ensuring the optimal performance of the models.

The AE-GRU model is configured with nine input features and utilizes the ReLU activation and Cross-Entropy loss functions. The Rmsprop optimizer was employed during training, which consists of 300 epochs with a batch size of 250. Each input sequence has a length of 12 timesteps. The encoder comprises three layers, with the first layer containing a GRU with 128 units, followed by a GRU layer with 16 units, and finally, a dense layer with units equal to the number of features. On the other hand, the decoder comprises three layers: the first layer is a dense layer with the units equal to the number of features, followed by two GRU layers with 16 and 128 units, respectively. On the other hand, the standalone anomaly detection methods are configured with the specific parameters for their operation. Isolation Forest is set with a contamination rate of 0.01 and utilizes 150 estimators. The LOF method also has a contamination rate of 0.01 and is configured with the novelty set to TRUE. The EE method is configured with a contamination rate of 0.01 and a support fraction of 0.995. For the 1SVM method, the kernel used is the Radial Basis Function (RBF), with the parameters set as follows: $\nu = 0.0015$ and $\gamma = 0.25$.

- DOS attack: In this scenario, a DOS attack is directed at an IEC 104 control station, aiming to overload it and disrupt its functionality, thereby potentially causing grid failure. The attacker gains unauthorized access by utilizing a spoofed IP address and floods the victim with a significant volume of 1049 messages over a 30 min period. This onslaught overwhelms the control station's resources, rendering it unable to respond effectively to legitimate requests and ultimately leading to system instability or failure.

Figure 5 presents the heatmap illustrating the detection performance metrics attained by the AE-GRU-based and standalone anomaly detection methods during the DOS attack scenario. During the DOS attack scenario, Figure 5 shows that the AE-GRU-based anomaly detection methods demonstrated varying performance levels compared to the standalone models. Specifically, the AE-GRU-iForest method achieved an accuracy of 0.8875, exhibiting strong precision and F1-score values of 1 and 0.9052, respectively. This suggests that the AE-GRU-iForest method effectively detected anomalies with minimal false positives and achieved a balance between precision and recall. However, the AE-GRU-LOF method showed a lower accuracy of 0.65, indicating that it struggled to correctly classify instances during the attack. While it achieved perfect recall, its precision and F1-score were notably lower at 0.65 and 0.7879, respectively. Conversely, both the AE-GRU-1SVM and AE-GRU-EE methods demonstrated excellent performance, with accuracies exceeding 0.99 and perfect precision, recall, and F1-scores, indicating their robustness in detecting DOS attacks.

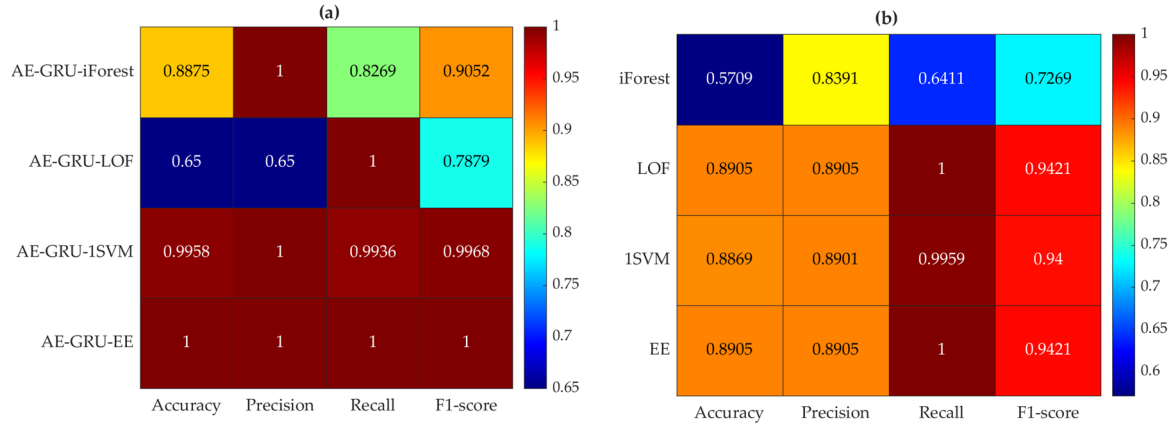

Figure 5. Detection performance comparison of (**a**) the AE-GRU-based and (**b**) standalone anomaly detection methods during the DOS attack scenario.

In comparison, the standalone anomaly detection methods exhibited different detection capabilities (Figure 5b). The iForest method achieved an accuracy of 0.5709, indicating a lower overall performance compared to the AE-GRU-based methods. Although it exhibited reasonable precision and F1-score values of 0.8391 and 0.7269, respectively, its recall was notably lower at 0.6411, indicating a higher rate of false negatives. On the other hand, the LOF and EE methods achieved an accuracy of 0.8905, with perfect precision, recall, and F1-scores, suggesting their effectiveness in detecting DOS attacks. However, the 1SVM method displayed a slightly lower accuracy of 0.8869, with precision, recall, and F1-score values of 0.8901, 0.9959, and 0.94, respectively, indicating its high recall but lower precision compared to the other methods.

Overall, the AE-GRU-based anomaly detection methods, particularly the AE-GRU-iForest and AE-GRU-1SVM methods, outperformed the standalone models in detecting DOS attacks, achieving higher accuracies and balanced precision–recall trade-offs. This highlights the effectiveness of leveraging deep learning techniques, such as the AE-GRU, for anomaly detection in smart grid cybersecurity applications.

- Switching attack: In a switching attack, malware is utilized to manipulate the targeted devices, turning them alternately on and off. This type of attack disrupts the normal operation of the devices and can potentially lead to system instability or malfunction. In this scenario, the switching attack persisted for 10 min, during which 72 packets were transmitted to the victim station. The attacker's objective is to disrupt the station's functionality by manipulating its operational status, which can have significant repercussions on the overall grid operation and stability. Figure 6 displays a heatmap comparing the detection performance metrics of the AE-GRU-based and standalone anomaly detection methods during the switching attack scenario. In the switching attack scenario, both the AE-GRU-based and standalone anomaly detection methods were evaluated. The AE-GRU-based methods, like the iForest and LOF methods, showed good accuracy and precision, with the iForest method achieving 0.8903 accuracy and 0.9856 precision, and the LOF method achieving 0.8945 accuracy and good precision (Figure 6a). However, the 1SVM model performed poorly with only 0.1181 accuracy and 0.0833 recall. The EE model had moderate accuracy at 0.8692 and precision at 0.9852. The standalone methods, especially the LOF and EE methods, demonstrated a strong performance, with accuracies of 0.9576 and perfect precision scores (Figure 6b). The 1SVM model also had high accuracy and precision, with scores of 0.9556 and 0.9575, respectively. Overall, while the AE-GRU-based methods like the iForest and LOF methods performed well, the standalone methods, particularly the LOF and EE methods, consistently showed a strong performance, suggesting their effectiveness in detecting the anomalies in the switching attack scenario.

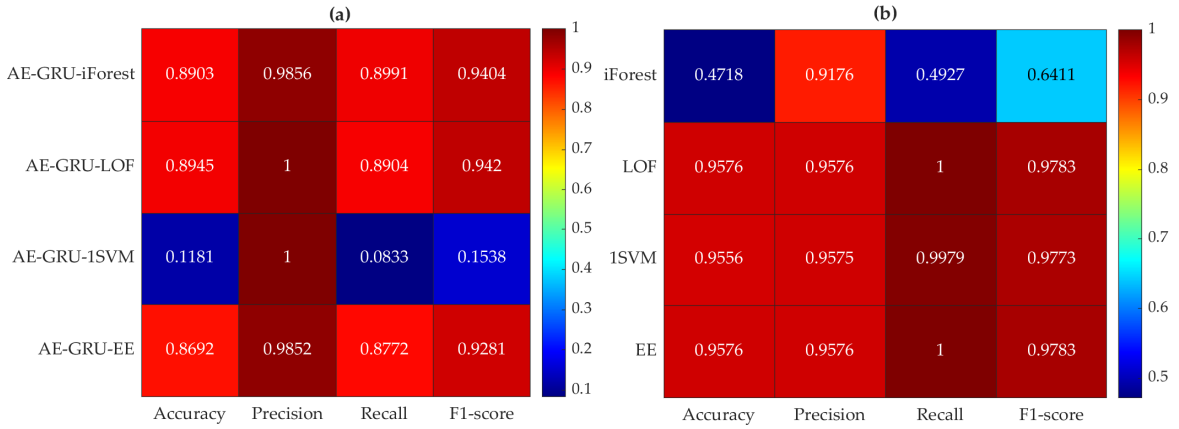

Figure 6. Detection performance comparison of (**a**) the AE-GRU-based and (**b**) standalone anomaly detection methods during the switching attack scenario.

- Injection command attacks: In injection command attacks, the attacker interferes with a connected device by modifying its configurations or introducing fraudulent commands, leading to abnormal behavior. This manipulation results in the generation of various anomalies within the system. The attack occurred in two distinct instances: the first lasted for 5 min and involved 83 packets, while the second persisted for 15 min and comprised 221 packets. The attacker aims to compromise the integrity and functionality of the targeted device, potentially causing disruptions or damage to the overall system. Such attacks pose significant risks to the security and reliability of the network, highlighting the importance of robust cybersecurity measures in safeguarding critical infrastructure like smart grids. Figure 7 illustrates the heatmap comparing the detection performance metrics of the AE-GRU-based and standalone anomaly detection methods during the injection attack scenario based on the testing data. In the injection attack scenario, both the AE-GRU-based and standalone anomaly detection methods achieved high accuracy, precision, and recall. The AE-GRU-based methods had accuracy values from 0.9619 to 0.9771, while the standalone methods ranged from 0.457 to 0.9275. All the methods had precision scores of 1, indicating near-perfect identification of attack instances. The AE-GRU-based methods showed recall values from 0.9616 to 1, while the standalone methods ranged from 0.4927 to 1. Overall, the AE-GRU-based methods consistently outperformed the standalone methods, demonstrating their superior detection capabilities for injection attacks.

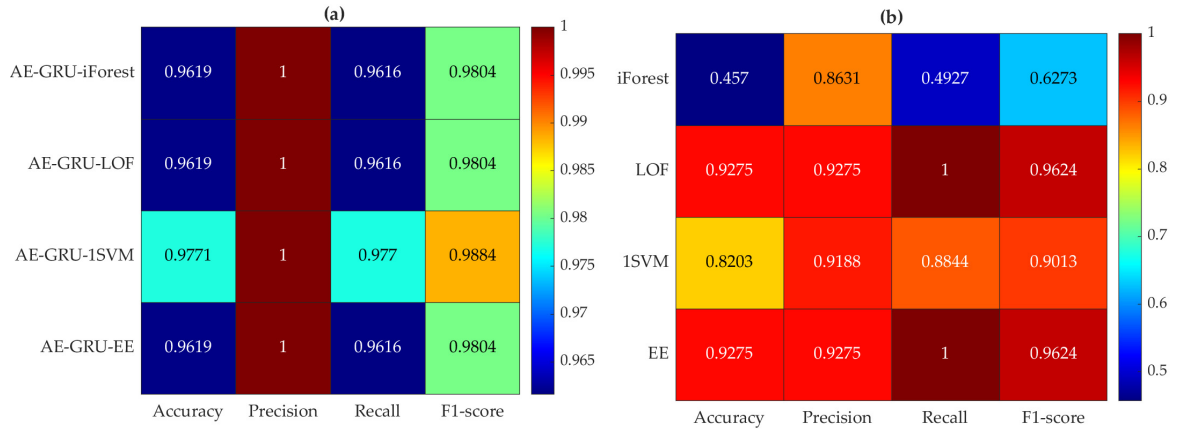

Figure 7. Detection performance comparison of (**a**) the AE-GRU-based and (**b**) standalone anomaly detection methods during the injection attack scenario.

- Connection loss attacks: In this category, the attacker attempts to interfere with specific devices, disrupting their interconnected communications. Two scenarios were simulated to replicate this interference. In the first scenario, a 10 min disconnection led to the loss of 146 packets. In the second scenario, the disconnection persisted for an hour, losing several packets. These attacks aim to disrupt the normal functioning of the targeted devices, potentially causing delays, malfunctions, or data loss. Such interference poses significant threats to the reliability and integrity of the communication network, underscoring the importance of robust cybersecurity measures in mitigating such risks.

Figure 8 shows a heatmap comparing the evaluation metrics of the AE-GRU and standalone anomaly detection methods during a connection loss attack scenario, based on the test data. From Figure 8, we observe that the AE-GRU-based methods, specifically the AE-GRU-LOF and AE-GRU-EE methods, exhibited a significantly higher detection performance compared to the standalone methods, with F1-score values of 94.93% and 96.43%, respectively. This signifies a balanced performance in precision and recall, crucial for accurate anomaly detection. Conversely, the standalone methods, including the iForest and 1SVM methods, demonstrated lower F1-scores, with the iForest method reaching 51.37% and the 1SVM method reaching 83.29%. This suggests that while the standalone methods might excel in certain aspects such as recall, their overall performance in terms of precision and recall balance is not as robust as the AE-GRU-based methods are. These differences in F1-score highlight the effectiveness of the AE-GRU-based methods in achieving a harmonious trade-off between precision and recall, thereby offering a more balanced approach to the anomaly detection during connection loss attacks. This balance is crucial in ensuring the accurate detection of anomalies while minimizing false positives, ultimately enhancing the cybersecurity of smart grid networks.

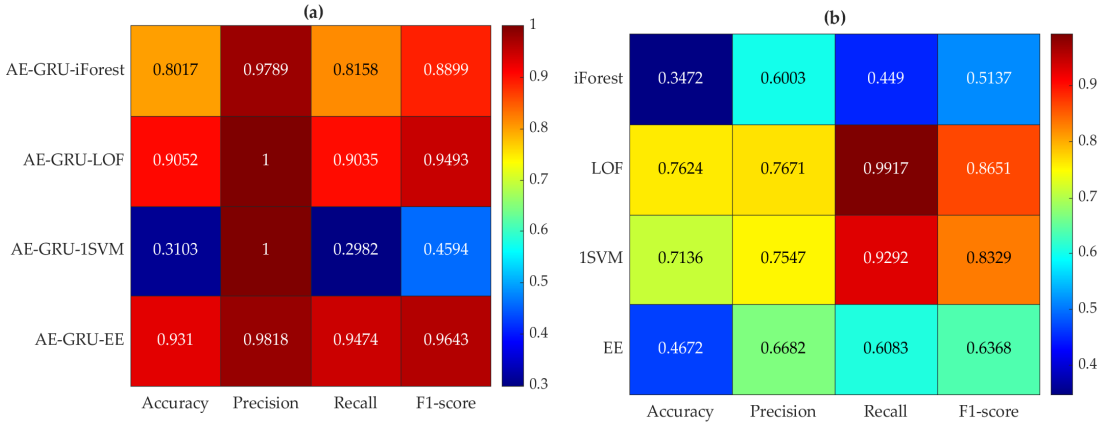

Figure 8. Detection performance comparison of (**a**) the AE-GRU-based and (**b**) standalone anomaly detection methods during the connection loss attack scenario.

- Rogue device attack: In this attack, the attacker gains unauthorized access to the communication network, allowing them to transmit arbitrary messages to authorized devices. These messages compel the devices to perform unauthorized activities, leading to irregular events and potentially harmful outcomes. In a 30 min attack, the attacker transmitted 417 abnormal messages, exploiting the network security protocol vulnerabilities. Such attacks can disrupt the network's normal operations, compromise its integrity, and pose significant risks to the overall cybersecurity posture of the system. It underscores the importance of robust security measures to prevent unauthorized access and mitigate the impact of such attacks on the network's functionality and reliability.

In the rogue device attack scenario, the AE-GRU-based anomaly detection methods outperformed the standalone methods (Figure 9a,b). The AE-GRU-based methods, such as

the iForest and LOF methods, achieved impressive F1-scores of 99.03%, indicating highly accurate detection with minimal false positives and negatives. On the other hand, the standalone methods showed a more varied performance. While the LOF method achieved a perfect F1-score, the iForest method exhibited a lower F1-score of 60.04%, indicating a less balanced detection performance. Figure 9b reveals that the 1SVM method achieved an F1-score of 86.95%, demonstrating relatively balanced precision and recall compared to the AE-GRU-based methods. However, it still fell short of the performance attained by the AE-GRU-based methods. These quantitative results highlight the superior performance of the AE-GRU-based anomaly detection methods in accurately identifying the rogue devices within smart grid networks. Leveraging deep learning and sequential data modeling, these methods offer a robust approach to enhancing the cybersecurity by effectively detecting anomalous behavior.

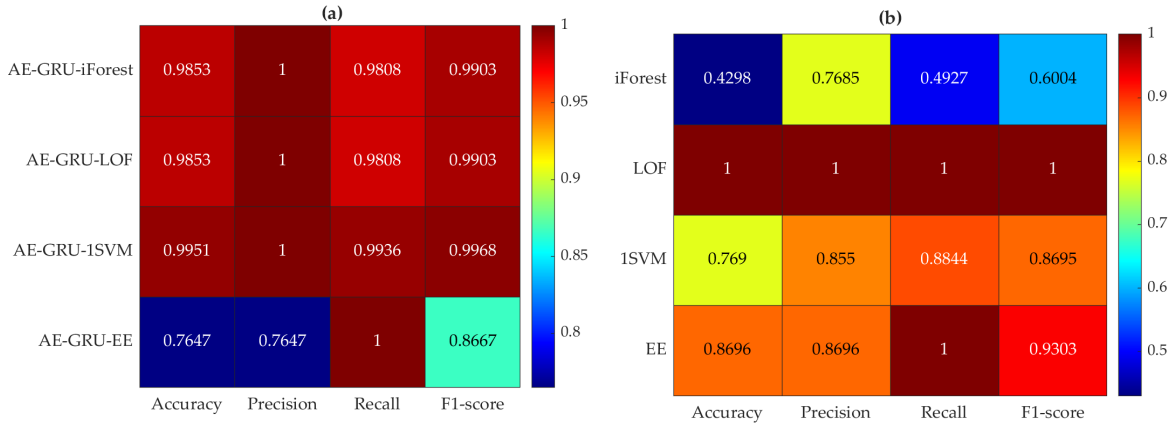

Figure 9. Detection performance comparison of (**a**) the AE-GRU-based and (**b**) standalone anomaly detection methods during the rogue device attack scenario.

While no single approach exhibited a superior performance across all the considered attacks, the AE-GRU-based anomaly detection methods consistently outperformed the standalone anomaly detection methods (LOF, EE, 1SVM, iForest) in detecting the various types of attacks in smart grid networks. This superiority can be attributed to several factors. Firstly, the AE-GRU-based methods leverage the power of deep learning architectures, specifically autoencoders and GRUs, to effectively model the complex temporal dependencies inherent in time-series data such as network traffic. This enables them to capture the subtle patterns and anomalies that may be missed by the standalone methods. Additionally, the AE-GRU models are capable of learning the high-level representations of data features through unsupervised learning, allowing them to create more informative and discriminative feature representations compared to the standalone methods.

Figure 10 depicts the average performance metrics of the anomaly detection methods considered. The benefit of evaluating the average performance metrics is providing a comprehensive assessment of each method's overall effectiveness across different types of attacks. By averaging the results over multiple scenarios, we gain insights into the methods' robustness and adaptability in detecting the anomalies commonly encountered in smart grid networks. We observe that the AE-GRU-based EE and LOF methods stand out as the top performers, achieving high accuracy and F1-scores of 0.91 and 0.95, respectively. These methods also demonstrate superior precision and recall, indicating their ability to effectively identify anomalies while minimizing false positives and false negatives. Furthermore, Figure 10 underscores the advantage of leveraging advanced techniques such as the AE-GRU-EE, which combines autoencoder-based feature extraction with a semi-supervised anomaly detection method, resulting in a superior detection performance. Similarly, the AE-GRU-LOF method, a density-based outlier detection method, proves highly effective in anomaly detection tasks.

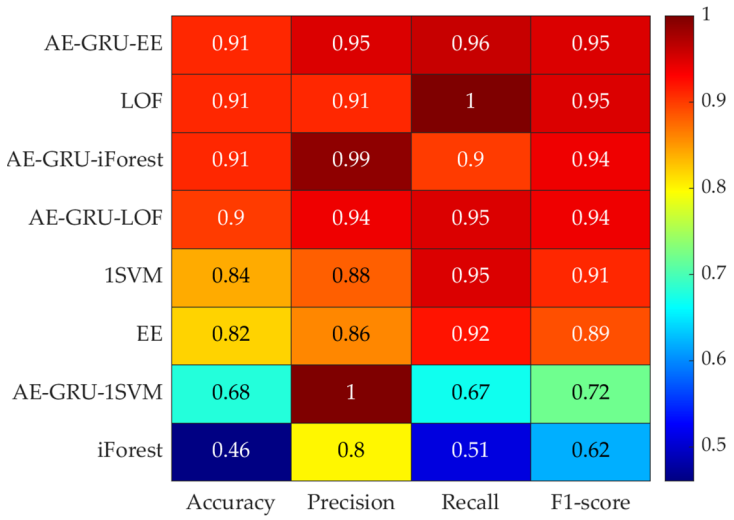

Figure 10. Average performance metrics of the considered anomaly detection methods.

5. Discussion and Conclusion

Protecting smart grids from cyberattacks is paramount in regard to ensuring the reliability and safety of grid operations. By deploying robust detection mechanisms and response strategies, operators can mitigate the impact of cyber threats and safeguard the grid infrastructure. The study demonstrates the effectiveness of the AE-GRU-based anomaly detection methods in enhancing the cybersecurity of smart grid networks using the BUT-IEC104-I dataset. The advantages of this approach include its ability to accurately detect the various types of anomalies, such as DOS attacks, switching attacks, injection command attacks, and connection loss attacks. The integration of the AE-GRU models with the semi-supervised anomaly detection methods, such as the EE and LOF methods, enhances the adaptability and robustness, resulting in an improved detection performance across the different attack scenarios. This highlights our framework's efficacy and the benefits of integrating the AE-GRU with semi-supervised anomaly detection to identify the cyber threats in smart grid traffic.

Despite the satisfactory detection performance, the study also has limitations that warrant attention. One limitation is the reliance on simulated attack scenarios, which may not fully capture the complexity and variability of real-world cyber threats. Additionally, the performance of the proposed framework may be influenced by factors such as the quality and quantity of training data, as well as the specific configurations of the smart grid network under consideration. Several potential solutions can be considered to enhance the performance of the proposed framework. Firstly, increasing the diversity and authenticity of the training data by incorporating real-world network traffic traces can improve the robustness of the AE-GRU models.

The encouraging outcomes (performance) of the presented cyberattack detection solution motivate further exploration and potential integration into the monitoring and intrusion detection systems across diverse industrial domains. Moreover, future investigations will be conducted by incorporating wavelet techniques to handle noisy data. Additionally, we intend to investigate the effectiveness of joining (merging) unsupervised deep learning with statistical monitoring charts, such as the Generalized Likelihood Ratio Test. Another potential line of improvement is to explore techniques such as transfer learning or domain adaptation that could help leverage the knowledge from the related domains to improve the generalization and adaptability of the AE-GRU models to diverse smart grid environments. Moreover, incorporating the ensemble learning approaches, where multiple models are combined to make predictions, could potentially improve the overall robustness and reliability of the anomaly detection system.

Author Contributions: F.H.: Writing—Review and editing, Formulation, Methodology, Investigation; Validation; B.B.: Writing, Review and editing, Conceptualization, Validation; A.D.: Writing—Review and editing, Methodology, Software, Formal analysis, Validation; Y.S.: Review and Editing, Formal analysis, Supervision, Visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in this study are available at https://ieee-dataport.org/documents/ics-dataset-smart-grid-anomaly-detection (accessed on 20 May 2024).

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

References

1. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of security advances in smart grid: A data driven approach. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 397–422. [CrossRef]
2. Khoei, T.T.; Slimane, H.O.; Kaabouch, N. A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. *arXiv* **2022**, arXiv:2207.07738.
3. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A survey on IoT-enabled smart grids: Emerging, applications, challenges, and outlook. *Energies* **2022**, *15*, 6984. [CrossRef]
4. Tang, D.; Fang, Y.P.; Zio, E. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods. *Reliab. Eng. Syst. Saf.* **2023**, *235*, 109212. [CrossRef]
5. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies* **2022**, *15*, 6799. [CrossRef]
6. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2023**, *6*, 103–123. [CrossRef]
7. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electron. Electr. Eng.* **2021**, *5*, 24–37.
8. Sahani, N.; Zhu, R.; Cho, J.H.; Liu, C.C. Machine learning-based intrusion detection for smart grid computing: A survey. *ACM Trans. Cyber-Phys. Syst.* **2023**, *7*, 1–31. [CrossRef]
9. An, D.; Yang, Q.; Liu, W.; Zhang, Y. Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach. *IEEE Access* **2019**, *7*, 110835–110845. [CrossRef]
10. Sakhnini, J.; Karimipour, H.; Dehghantanha, A. Smart grid cyber attacks detection using supervised learning and heuristic feature selection. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 108–112.
11. Hink, R.C.B.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyber-attack discrimination. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems (ISRCS) 2014, Denver, CO, USA, 19–21 August 2014; pp. 1–8.
12. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2014**, *11*, 1644–1652. [CrossRef]
13. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
14. Acosta, M.R.C.; Ahmed, S.; Garcia, C.E.; Koo, I. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks. *IEEE Access* **2020**, *8*, 19921–19933. [CrossRef]
15. Al-Qudah, M.; Ashi, Z.; Alnabhan, M.; Abu Al-Haija, Q. Effective one-class classifier model for memory dump malware detection. *J. Sens. Actuator Netw.* **2023**, *12*, 5. [CrossRef]
16. Menon, D.M.; Radhika, N. Anomaly detection in smart grid traffic data for home area network. In Proceedings of the 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 18–19 March 2016; pp. 1–4.
17. Al-Abassi, A.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access* **2020**, *8*, 83965–83973. [CrossRef]
18. Kundu, A.; Sahu, A.; Serpedin, E.; Davis, K. A3D: Attention-based auto-encoder anomaly detector for false data injection attacks. *Electr. Power Syst. Res.* **2020**, *189*, 106795. [CrossRef]
19. Tuor, A.; Kaplan, S.; Hutchinson, B.; Nichols, N.; Robinson, S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. In Proceedings of the Workshops at the Thirty-First AAAI Conference on Artificial Intelligence, San Francisco, CA, USA, 4–9 February 2017.
20. Haghshenas, S.H.; Hasnat, M.A.; Naeini, M. A temporal graph neural network for cyber attack detection and localization in smart grids. In Proceedings of the 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–19 January 2023; pp. 1–5.
21. Khanna, K.; Panigrahi, B.K.; Joshi, A. AI-based approach to identify compromised meters in data integrity attacks on smart grid. *IET Gener. Transm. Distrib.* **2018**, *12*, 1052–1066. [CrossRef]

22. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R.; Leung, H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access* **2019**, *7*, 80778–80788. [CrossRef]
23. Qiu, W.; Tang, Q.; Wang, Y.; Zhan, L.; Liu, Y.; Yao, W. Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors. *IEEE Trans. Smart Grid* **2020**, *11*, 3457–3468. [CrossRef]
24. Mohammadpourfard, M.; Genc, I.; Lakshminarayana, S.; Konstantinou, C. Attack detection and localization in smart grid with image-based deep learning. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 121–126.
25. Ali, S.; Li, Y. Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access* **2019**, *7*, 108647–108659. [CrossRef]
26. Dou, C.; Wu, D.; Yue, D.; Jin, B.; Xu, S. A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM. *CSEE J. Power Energy Syst.* **2020**, *8*, 1697–1707.
27. Lu, G.; Tian, X. An efficient communication intrusion detection scheme in AMI combining feature dimensionality reduction and improved LSTM. *Secur. Commun. Netw.* **2021**, *2021*, 6631075. [CrossRef]
28. Qi, R.; Rasband, C.; Zheng, J.; Longoria, R. Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning. *Information* **2021**, *12*, 328. [CrossRef]
29. Ferrag, M.A.; Maglaras, L. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1285–1297. [CrossRef]
30. Liu, W.; Wang, Z.; Liu, X.; Zeng, N.; Liu, Y.; Alsaadi, F.E. A survey of deep neural network architectures and their applications. *Neurocomputing* **2017**, *234*, 11–26. [CrossRef]
31. Zhang, G.; Liu, Y.; Jin, X. A survey of autoencoder-based recommender systems. *Front. Comput. Sci.* **2020**, *14*, 430–450. [CrossRef]
32. Michelucci, U. An introduction to autoencoders. *arXiv* **2022**, arXiv:2201.03898.
33. Dey, R.; Salem, F.M. Gate-variants of gated recurrent unit (GRU) neural networks. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1597–1600.
34. Cho, K.; Van Merriënboer, B.; Bahdanau, D.; Bengio, Y. On the properties of neural machine translation: Encoder-decoder approaches. *arXiv* **2014**, arXiv:1409.1259.
35. Kanai, S.; Fujiwara, Y.; Iwamura, S. Preventing gradient explosions in gated recurrent units. *Adv. Neural Inf. Process. Syst.* **2017**, *30*, 1–10.
36. Ravanelli, M.; Brakel, P.; Omologo, M.; Bengio, Y. Improving speech recognition by revising gated recurrent units. *arXiv* **2017**, arXiv:1710.00641.
37. Harrou, F.; Taghezouit, B.; Bouyeddou, B.; Sun, Y. Cybersecurity of photovoltaic systems: Challenges, threats, and mitigation strategies: A short survey. *Front. Energy Res.* **2023**, *11*, 1274451. [CrossRef]
38. Rabaoui, A.; Davy, M.; Rossignol, S.; Lachiri, Z.; Ellouze, N. Improved one-class SVM classifier for sounds classification. In Proceedings of the 2007 IEEE Conference on Advanced Video and Signal Based Surveillance, London, UK, 5–7 September 2007; pp. 117–122.
39. Kawi, O.; Clawson, K.; Dunn, P.; Knight, D.; Hodgson, J.; Peng, Y. Medical formulation recognition (MFR) using deep feature learning and one class SVM. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–7.
40. Liu, F.T.; Ting, K.M.; Zhou, Z.H. Isolation forest. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, Pisa, Italy, 15–19 December 2008; pp. 413–422.
41. McKinnon, C.; Carroll, J.; McDonald, A.; Koukoura, S.; Infield, D.; Soraghan, C. Comparison of new anomaly detection technique for wind turbine condition monitoring using gearbox SCADA data. *Energies* **2020**, *13*, 5152. [CrossRef]
42. Hubert, M.; Debruyne, M.; Rousseeuw, P.J. Minimum covariance determinant and extensions. *Wiley Interdiscip. Rev. Comput. Stat.* **2018**, *10*, e1421. [CrossRef]
43. Alghushairy, O.; Alsini, R.; Soule, T.; Ma, X. A review of local outlier factor algorithms for outlier detection in big data streams. *Big Data Cogn. Comput.* **2020**, *5*, 1. [CrossRef]
44. Lin, C.Y.; Nadjm-Tehrani, S. Understanding IEC-60870-5-104 traffic patterns in SCADA networks. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 4 June 2018; pp. 51–60.
45. Cherifi, T.; Hamami, L. A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol. *Int. J. Crit. Infrastruct. Prot.* **2018**, *20*, 68–84. [CrossRef]
46. Grammatikis, P.R.; Sarigiannidis, P.; Sarigiannidis, A.; Margounakis, D.; Tsiakalos, A.; Efstathopoulos, G. An anomaly detection mechanism for IEC 60870-5-104. In Proceedings of the 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 7–9 September 2020; pp. 1–4.

47. Matoušek, P.; Ryšavý, O.; Grégr, M.; Havlena, V. Flow based monitoring of ICS communication in the smart grid. *J. Inf. Secur. Appl.* **2020**, *54*, 102535.
48. Matoušek, P.; Havlena, V.; Holík, L. Efficient modelling of ICS communication for anomaly detection using probabilistic automata. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021; pp. 81–89.