A contrived dataset of substation automation for cybersecurity research in the smart grid networks based on IEC61850

John Edet Efiong[1], Jide Ebenezer Taiwo Akinsola[2], Bodunde Odunola Akinyemi[3], Emmanuel Ajayi Olajubu[4], Ganiyu Adesola Aderounmu[1]
[1]Cybersecurity Research Laboratory, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
[2]Department of Computer Sciences, First Technical University, Ibadan, Nigeria
[3]Autonomous Robot Laboratory, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
[4]Cysec Laboratory, Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria

Article Info

Article history:

Received Jan 23, 2024
Revised May 17, 2024
Accepted May 26, 2024

Keywords:

CyberGrid
Cybersecurity research
Datasets
Deep learning
IEC61850
Smart grid
Substation automation system

ABSTRACT

Relevant datasets that depict and/or emulate the smart grid networks (SGN) are key to developing cybersecurity models that can effectively provide security for mission-critical infrastructure. The difficulty in obtaining relevant SGN real-life datasets presents a considerable challenge for researchers in the field and, the existing datasets lack representation of the IEC61850 protocol for modelling substation automation processes for cybersecurity solutions. This paper presents a dataset simulated from a fully virtual testbed, intended to provide researchers with the necessary datasets for research and experiments that require massive amounts of data close to the real-world scenario. Experimentally, the dataset was used to develop an intrusion detection model based on gated recurrent unit (GRU), deep belief network (DBN), long-short term memory (LSTM), and evaluated using accuracy, precision, recall, F1-score, detection rate, false alarm rate (FAR), missed alarm rate (MAR), mean squared error (MSE), mean absolute error (MAE), and loss. Results show that the standalone deep learning (DL) algorithms outperformed the hybridized ones and are more suitable for developing models for securing substation automation systems that support generic object-oriented substation events (GOOSE), and manufacturing message specification (MMS) and run on IEC61850, distributed network protocol version 3 (DNP3), and Modbus-transmission control protocol (ModbusTCP).

Corresponding Author:

John Edet Efiong
Cybersecurity Research Laboratory, Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife, Nigeria
Email: jeediof@gmail.com

1. INTRODUCTION

In recent times, the energy infrastructure has increasingly become more interconnected and dependent on digital technologies and their associated cyber risks. This makes the need for effective, secure, and sustainable energy management very crucial. Smart grid research has, thus, presented itself as an essential process for addressing the ever-growing challenges in the domain, especially cybersecurity concerns. However, to advance the much-desired research, realistic datasets that emulate the dynamic and complex nature of smart grid systems are required. Particularly for the modern grid, such datasets are expected to have a proper mix of proprietary and modern communication protocols, represent the physical, communication, and application layers of the grid, and depict both the physical and cyber processes of cyber-physical systems [1]. Datasets serve as the foundation for testing, validating, and developing smart grid technologies, making them a critical asset for research and development in the energy business value chain [2].

A contrived dataset is a dataset intentionally created, simulated, synthesized, generated, or manufactured for a specific purpose, such as research, testing, or experimentation [3]. Unlike real-world datasets that are collected from actual observations or measurements, contrived datasets are synthetic and designed to meet certain criteria or mimic particular characteristics. These datasets are often used in various fields, including data science, machine learning, research, and testing, for a range of purposes [4]. Synthetic datasets are valuable because they offer a level of control and reproducibility that may not be achievable with real-world data. Researchers and practitioners can use such datasets to explore and experiment with different concepts, algorithms, and solutions without the limitations or complexities of real data. However, it is important to ensure that contrived datasets accurately represent the characteristics of the problem or domain they are intended to simulate to make their results and findings applicable to real-world scenarios. Many existing datasets for smart grid cybersecurity lack comprehensive, realistic, and up-to-date cybersecurity scenarios that accurately mimic the evolving threat landscape [5]. This paper presents a dataset designed to include a wide range of cybersecurity attack scenarios, helping researchers develop and test robust security solutions. Also, the existing datasets do not provide a sufficient level of detail or focus on the unique challenges and vulnerabilities present in substation automation systems. The presented contrived dataset provides well-documented ground truth data for evaluating intrusion detection systems (IDSs), security solutions, and incident response strategies. This is a significant gap in existing datasets, where ground truth data is often limited.

Furthermore, anomalies in smart grid network (SGN) traffic are often early indicators of cyber threats. The contrived dataset includes known anomalies and deviations from normal network behaviour, aiding in the development and evaluation of anomaly detection algorithms. Thus, the new dataset has been structured to support the training and testing of machine learning models for intrusion detection, network security, and threat prediction in smart grids. The dataset is specifically tailored for teaching and learning about substation automation security. In this paper, a contrived dataset which is a representation of the substation automation cyber-physical communications is evaluated using three deep learning (DL) algorithms, including the gated recurrent unit (GRU), deep belief network (DBN), and long-short term memory (LSTM). DL has been proven to outperform traditional machine learning algorithms in many respects when applied on cybersecurity problems [6]–[10]. The goal of this research was to address scientific questions that border on data integrity and authenticity, threat detection and anomaly detection/behaviour analysis, as: i) how effective are current cybersecurity measures in ensuring the integrity and authenticity of data exchanged within substation automation systems based on IEC61850 standards?; ii) how can a contrived dataset facilitate the development and testing of IDS?; and (iii) how can machine learning and data analytics techniques be applied to identify anomalous behaviour or deviations from normal operation within substation automation systems, using the contrived dataset as a benchmark for performance evaluation?.

By addressing these scientific questions, the paper aims to contribute to advancing the understanding of cybersecurity challenges and solutions in SGN, ultimately enhancing the resilience and security of critical energy infrastructure. The major contributions of this study are: i) introduce a contrived dataset that replicates the intricacies of real-world smart grid environments with respect to prevalent cyber attacks on critical infrastructure; ii) demonstrate a use case of the dataset in developing DL models for a binary classification intrusion detection problem; iii) provide experimental results of the use case to gain insights into the leverage of the datasets for developing cybersecurity solutions; and iv) ultimately contribute to the advancement of smart grid research, enabling researchers to experiment, innovate, and develop solutions for improved energy management. The rest of the paper is structured as: in section 2, related works are reviewed. Section 3 presents the methods used in generating the dataset and the experimental set up for demonstrating the use of the dataset for developing cybersecurity models. The results are presented and discussed in section 4. Section 5 is the conclusion.

2. RELATED WORKS

As observed earlier, cybersecurity research geared towards the smart grid requires reliable datasets for experiments and developing tools for the security of mission-critical infrastructure from varying degrees of cyber threats. Several datasets have been leveraged in the literature to address different aspects of cybersecurity in the sector. These range from synthetic datasets from cyber ranges to experimental datasets from laboratories, with very little from real-world systems [11]. For instance, the Geek Lounge Lab [12] generated datasets for electrical systems for the 4SICS conference. While this represents the power system dynamics, it did not depict the IEC61850 protocol or emulate the modern smart grid system. The electric power intelligent control (EPIC) testbed released datasets that showed features for the manufacturing message specification (MMS) which is required for communication with IEC61850 [5]. The EPIC datasets focused more on the physical processes of the electric grid, with very limited attention paid to the cyber components.

The work of [13] presented a dataset with a representation of generic object-oriented substation events (GOOSE) which ensures automation and secure communication in IEC61850. The generation scenarios did not consider the cybersecurity concerns of the substation. Similarly, [14], [15] had earlier leveraged GOOSE to develop datasets that could potentially reveal threats to the smart grid. They, however, failed to capture the cyber processes of the system and present threat models. To address the above limitations, [16] developed a synthetic dataset for cybersecurity research that focused on the IEC61850 substation automation system using GOOSE and presented threat and substation models to aid in cybersecurity research. Like others, the dataset was typically generated from physical systems, depicting physical perturbations in the electrical processes similar to EPIC. Recently, Radoglou-Grammatikis *et al*. [17] presented a dataset generated from a testbed of industrial systems in the smart grid that utilized the distributed network protocol version 3 (DNP3) communication protocol. Although the datasets were presented for developing an intrusion detection model, they are a representation of more of the physical processes. Furthermore, the authors presented another dataset for IEC 60870-5-104 protocol to mitigate attacks that happen on critical systems with such a protocol [18]. Similar to the previous, the physical processes of the systems were majorly covered. Owing to the fact that obtaining real-life datasets related to smart grid operations presents a considerable challenge for researchers in the field and the IEC61850 protocol that supports substation automation was not covered in most of the works presented, the CyberGrid was developed to address such limitations [19], [20]. The difficulty in accessing real-world datasets for which CyberGrid seeks to bridge emanates from several factors, such as: i) smart grid data often contains sensitive information related to power infrastructure, customer data, and operational details. Sharing such data raises significant privacy and security concerns, making it challenging to access real-world datasets; ii) smart grid systems commonly use a mix of proprietary and modern protocols for communication and control and access to proprietary protocols and data can be restricted, further limiting the availability of real-life datasets; and iii) public datasets that adequately emulate substation automation with a combination of proprietary and modern smart grid protocols are sparse, and the existing synthetic datasets may not represent the complexities.

3. METHOD

This section describes the methods used in generating the datasets, their characteristics, validation, and quality control, use cases and applications, and distribution of the datasets.

3.1. Dataset generation

The dataset was generated from a virtual testbed called CyberGrid [19]. Five types of attacks and twelve patterns were simulated and launched against CyberGrid, depicting 2,166,581 samples.

3.1.1. Methodology

The methodology for generating the dataset is summarized in Figure 1, which depicts a six-step process: testbed set-up, scenario definition, network traffic configuration, anomaly injection, data logging and capture, and data annotation. In setting up the testbed in step 1, the environment was designed to replicate the components of a smart grid as described in [19]. Where necessary, the testbed was scaled to different configurations to generate data representative of various substation automation scenarios [21]. The test scenarios in step 2 were defined according to the objectives of the research and the requirements of the dataset. The scenarios were patterned according to a random parameterized framework defined as interception, interruption, modification, and fabrication (I2MoF). Standard network simulation and traffic generation tools were used to create, craft, and send realistic network packets and generate traffic as necessary. In step 3, the different components were configured to generate network traffic that mimics real-world communication patterns, including protocols (DNP3, ModbusTCP, and IEC61850) used in substation automation, data exchange, and command and control traffic.

At the fourth level, anomalies were injected into the network to include security incidents and attack scenarios specifically targeting the open programmable logic controller (OpenPLC) server and runtime, the supervisory control and data acquisition (SCADA) and human-machine interface (HMI) control monitor, and the processes. These injections were aimed at causing communication disruptions, interruptions, data manipulation, false data injection, and various effects typical of the attack types and patterns simulated. To maintain control over the data generation parameters, including traffic volume, variability, and complexity, certain parameters were adjusted to meet the requirements for the test scenarios. Data logging mechanisms were implemented in step 5 within the attacker node to capture and log the flow for both normal and anomalous activities. Ideally, Wireshark was set in place for network capture and filtering. Variations in data were introduced to cater to varying network traffic patterns, device behaviours, and communication protocols as a way of emulating possible real-world conditions and challenges. Lastly, the captured data was annotated to provide information about the context, purpose, and characteristics of the network traffic. The annotation process included labelling the different data types, events, and potential security incidents using expert knowledge and established attack patterns of known threats and intrusions.

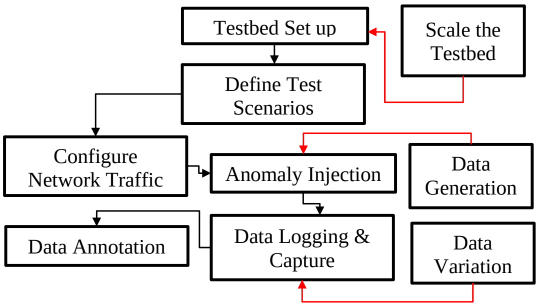

Figure 1. Data generation process

3.1.2. Overview of the substation automation testbed: CyberGrid

CyberGrid plays a pivotal role in the field of smart grid cybersecurity research [19]. Its primary purpose is to facilitate the simulation of cyberattacks specific to smart grid environments and generate high-quality datasets for the development, testing, and validation of cybersecurity solutions tailored to the power sector. This initiative acknowledges the critical need for robust security measures in the modern energy landscape and the growing importance of safeguarding smart grid infrastructure against cyber threats.

The research focused on intrusions in SCADA systems and PLCs which control and monitor power transmission and distribution in grids. The design of the testbed made three basic assumptions as: i) the network topologies of SCADA systems are fixed and the transactions between the nodes are repetitive and regular; ii) the outstations and control systems run on Modbus, DNP3, and IEC61850; and iii) the attacker has already gained access to the network.

The assumption of the static nature of SCADA network topologies makes it easy for IDSs to detect abnormal traffic and identify unusual attributes in supposing normal packets. This assumption is important because, by design, SCADA systems are intended to last for several years. That way, the network configuration would be predetermined and the communication behaviours could be pre-empted.

3.1.3. Structure and format of the dataset

With 2,166,581 samples, the dataset is of a significant size, which can be valuable for conducting extensive research, training machine learning models, and evaluating the performance of cybersecurity solutions. Figures 2 to 4 show the distributions of the datasets for training, testing, and validation respectively, and the attack patterns simulated. This large number of samples can provide a robust foundation for various experiments and analyses related to smart grid cybersecurity. Researchers can use this dataset to develop, test, and validate IDSs, anomaly detection algorithms, and other security solutions, and to gain insights into network behaviour and potential vulnerabilities in the smart grid. The dataset is available as a packet capture (PCAP) file and in comma-separated values (CSV) format, and was structured into three categories for each instance:

a. Network traffic information (NeTI): NeTI contains attributes related to the patterns of communication, including information such as length, time, duration, and the number of packets. These attributes help describe the overall flow and timing of network traffic.
b. Payload information (PI): PI provides hints about the nature of packets exchanged among nodes, including details like sequence numbers, transmission control protocol (TCP) segments, and other packet-specific information.
c. Network transaction labels (NeTLab): NeTLab contains attributes related to node identification, such as source internet protocol (IP) address, destination IP address, source port, destination port, protocol used, and more.

These attributes help identify the source and destination of network traffic. Additional features were computed based on NeTI, PI, and NeTLab, including attributes such as packet sequence, cumulative byte count, protocol number, transmission rates in both directions, packet counts in both directions, and sequence information (seq) as shown in Table 1.

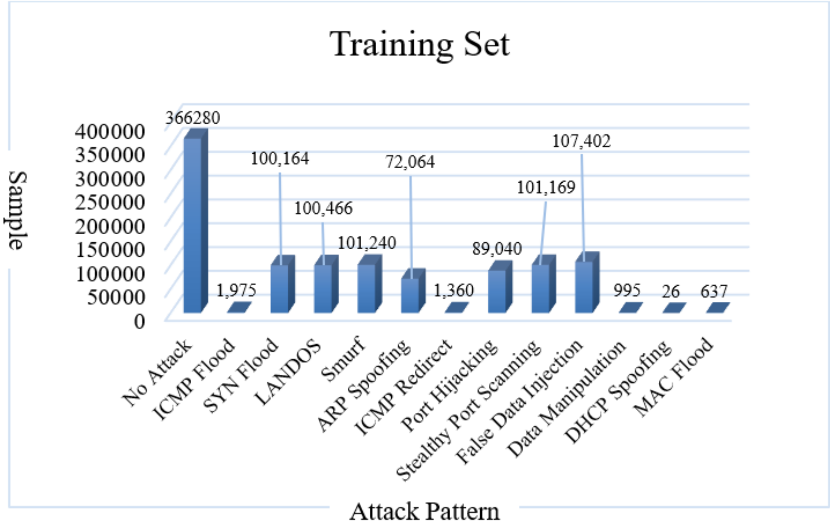

Figure 2. Training set

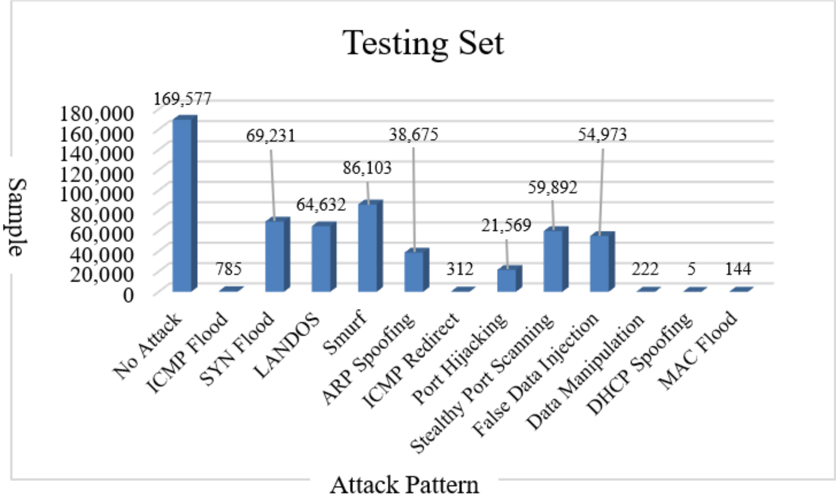

Figure 3. Testing set

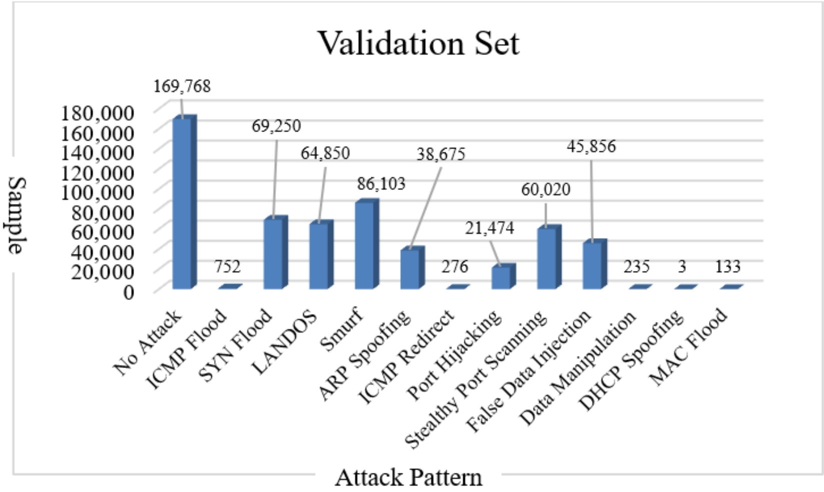

Figure 4. Validation set

Table 1. Attacks and patterns

AttackType	AttackPattern
Normal	No attack
DOS	ICMP flood | SYN flood | LANDOS | smurf
MiTM	ARP spoofing | ICMP redirect | port hijacking
Port scan	Stealthy port scanning
Interdiction	False data injection | data manipulation
Switching	DHCP spoofing | MAC flood

3.2. Features of dataset selected

The dataset used had 16 features, described as: packet sequence identification number (PktSeqID); packet arrival TimeStamp (time); packet size (length); (source port); destination port (SrcPort); cumulative bytes transmitted per packet in a network communication (CumByte); the time duration of a packet transmission or session (duration); packet's relative time with reference to the initial time (RelativeTime); protocol port numbers (ProtocolNo); the rate of data transmission, typically in bits per second in BPS (rate); source-to-destination transmission rate, representing the rate of data transmission from the source to the destination (srate); destination-to-source transmission rate, representing the rate of data transmission from the destination to the source (drate); the count of packets transmitted in a network communication (Pkts); destination-to-source packet count, representing the count of packets transmitted from the destination to the source (Dpkts); source-to-destination packet count, representing the count of packets transmitted from the source to the destination (Spkts) and sequence number. In TCP communication, sequence numbers are used to order and reassemble packets (Seq).

3.3. Data cleaning and preprocessing

A number of steps were followed to thoroughly clean and preprocess the network traffic data, ensuring that it is free from noise, irrelevant information, and inconsistencies. This began with data inspection and understanding of the structure and content of the dataset using expert knowledge, handling of missing data, data normalization and scaling, and feature selection. Categorical data were encoded into numerical values using techniques such as one-hot encoding and label encoding. The cleaning process makes the dataset more reliable and suitable for research, analysis, and the development of cybersecurity solutions.

3.4. Annotation and ground truth

The labeling of the dataset was based on expert knowledge and descriptive attack patterns found in the literature. This means that each instance in the dataset is associated with a label indicating whether it represents normal network behaviour or a specific type of attack. The dataset includes instances for various attack types and patterns, which were crafted and launched one after the other. This labeling approach simplifies the categorization of the datasets for use in research and experimentation.

3.5. Model development and performance evaluation

Preliminary experiments were conducted using three prominent DL algorithms: the GRU, the DBN, and LSTM. The significance of employing these models and combinations lies in their ability to capture complex temporal dependencies and patterns inherent in smart grid data; learn hierarchical representations of features for more effective detection of anomalies; adapt and generalize well to diverse and evolving cyber threats; provide interpretable results, aiding cybersecurity analysts in understanding and responding to detected intrusions and enhance the resilience and security posture of SGN by detecting and mitigating cyber threats in real-time [22], [23].

The dataset was preprocessed to extract relevant features and prepare the data for modeling. This involved normalization, encoding categorical variables, handling missing values, and splitting the data into training, validation, and testing sets. Each model architecture was designed based on its specific characteristics and capabilities. For example, GRU and LSTM are recurrent neural network (RNN) variants suitable for sequential data, while DBN is a DL model capable of learning hierarchical representations of features [24]. The models were trained using the prepared dataset, with hyperparameters tuned through techniques like grid search. The training involved optimizing the model parameters to minimize a chosen loss function. For this binary classification problem, the binary cross-entropy was selected [25]. The hyperparameters of the models, such as learning rate, batch size, number of layers, and activation functions were fine-tuned to achieve optimal performance. Regularization techniques, such as dropout or ridge regression (L2) regularization, may be applied to prevent overfitting and improve generalization. The performance of the models was evaluated using appropriate metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC). Additionally, the missed alarm rate (MAR) and false alarm rate (FAR) were utilized as the cost metrics for evaluating the performance of the models.

4. RESULTS AND DISCUSSION

The comprehensive analysis, as summarized in Table 2, provides a detailed snapshot of the performance outcomes for these classifiers. Firstly, the GRU model exhibited exceptional accuracy and precision, boasting an impressive 99% for both metrics. Furthermore, it excelled in terms of recall and detection rate, reaching a remarkable 99.7%. This level of precision and recall balance resulted in an F1-score of 93.3%, showcasing the model’s ability to achieve an equilibrium between minimizing false positives and false negatives. Additionally, the GRU model demonstrated a low FAR of 0.0299, signifying its capability to keep false alarms to a minimum. It also boasted a very low MAR of 0.0034, indicating that it effectively identified a vast majority of actual intrusion instances while avoiding overlooking them.

Similarly, the DBN exhibited an accuracy and precision of 99%. However, it displayed a slightly lower recall of 98.7%, indicating a slightly reduced strength to correctly identify positive samples compared to GRU. With the DBN, FAR was measured at 0.0091, signifying a somewhat lower rate of false alarms compared to GRU. The model’s MAR was slightly higher at 0.0130, suggesting that it may miss a few more intrusion instances compared to GRU. Moving beyond these metrics, the study extended the evaluation to include training and validation losses and the accuracies of both classifiers. Additionally, the analysis includes visual representations in the form of confusion matrices, loss-epoch plots, and accuracy-epoch plots. These figures further illuminate the behaviour and performance dynamics of the GRU and DBN models.

Table 2. Model performance results

Classifier	Performance metrics						
	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Detect rate (%)	FAR	MAR
GRU	99.0	99.0	99.7	93.3	99.7	0.0299	0.0034
DBN	99.0	99.7	98.7	99.2	99.7	0.0091	0.0130
LSTM	98.58	98.66	99.5	99.1	99.57	0.0411	0.0053

The LSTM recorded a high accuracy of 98.58%, indicating a strong classification performance and precision of 98.66% which suggests that the LSTM effectively minimized false positives. The remarkable recall rate of 99.47% signifies LSTM’s adeptness at capturing true positive cases, while an F1-score of 99.06% indicates a symbiotic equilibrium between precision and recall. This suggests that the LSTM missed identifying a substantial number of important instances. The data points were chronicled throughout 10 training epochs, which offer insights into the models learning trajectories as summarized in Table 3. The loss-epoch plot for the GRU, showcases the model’s learning process. Initially, the training loss was relatively high but experienced a rapid reduction. As the number of training epochs increased, the loss decreased gradually, with a slight surge observed after the eighth epoch. In contrast, the validation loss started lower and displayed some modulated fluctuations, with a sharp decline following the eighth epoch. Furthermore, Figure 5 provides the accuracy of the GRU pictorially across various epochs. It illustrates that both training and validation accuracy consistently improved as the number of epochs increased. The loss-epoch plot for the GRU, as depicted in Figure 6, showcases the model’s learning process. Initially, the training loss was relatively high but experienced a rapid reduction. As the number of training epochs increased, the loss decreased gradually, with a slight surge observed after the eighth epoch. In contrast, the validation loss started lower and displayed some modulated fluctuations, with a sharp decline following the eighth epoch.

Table 3. Model training and validation results

Classifier		Epoch									
		1	2	3	4	5	6	7	8	9	10
GRU	Train loss	0.0844	0.0551	0.0502	0.0477	0.0453	0.0456	0.0440	0.0448	0.0427	0.0506
	Valid loss	0.0560	0.0518	0.0494	0.0439	0.0489	0.0404	0.0445	0.0460	0.0502	0.0246
	Train acc	96.8%	98.1%	98.3%	98.4%	98.4%	98.5%	98.5%	98.5%	98.6%	98.5%
	Valid acc	98.1%	98.3%	98.3%	98.4%	98.3%	98.4%	98.5%	98.4%	98.5%	99.0%
DBN	Train loss	0.1604	0.1264	0.1197	0.1110	0.1041	0.0928	0.0835	0.0746	0.0653	0.0565
	Valid loss	0.1451	0.1176	0.1153	0.1036	0.0948	0.0832	0.0712	0.0794	0.0650	0.0518
	Train acc	92.1%	93.9%	94.4%	94.9 %	95.3%	95.9%	96.5%	97.0%	97.6%	98.0%
	Valid acc	93.3%	94.3%	95.00%	95.3%	95.7%	96.8%	97.2%	96.8%	96.9%	98.8%
LSTM	Train loss	0.0845	0.0562	0.0488	0.0472	0.0444	0.0467	0.0480	0.0532	0.0466	0.0454
	Valid loss	0.0702	0.0458	0.0623	0.0471	0.0481	0.0612	0.0752	0.0407	0.0443	0.0415
	Train acc	96.80%	98.10%	98.33%	98.41%	98.41%	98.41%	98.425	98.36%	98.49%	98.56%
	Valid acc	97.40%	98.32%	98.08%	98.36%	98.29%	98.36%	97.92%	98.54%	98.47%	98.58%

The loss-epoch plot, as illustrated in Figure 7, revealed a consistent and notable reduction in the loss metric as the number of epochs progressed. This trend remained consistent for both the training and validation phases of the algorithm's execution. Such a pattern indicates that the DBN model was effectively learning from the data, gradually improving its predictive capabilities over time. Figure 8 provides an insightful visualization of the accuracy across epochs for DBN. It depicted an upward trajectory in both training and validation accuracy as the number of epochs increased. This observation underscores the model's continuous learning and improvement throughout the training process. These results contribute to understanding the performance of the DBN. They signify the DBN's effectiveness in learning, predicting, and discriminating between data points, further validating its role in our multi-layered machine learning framework. The detection rate of 99.47% of the LSTM points to its effectiveness in identifying positive instances. The FAR of 0.0411 and MAR of 0.0053 indicate a controlled number of false alarms and effective minimization of missed intrusions respectively. LSTM showed a decreasing training loss, indicating its capability to learn and reduce errors over training epochs and the validation loss followed a similar decreasing trend, suggesting that LSTM generalized well according to Figure 9. The training accuracy showed incremental improvement, demonstrating its capacity to fit the training data effectively, and the validation accuracy generally increased, indicating LSTM's ability to generalize to unseen data as seen in Figure 10.

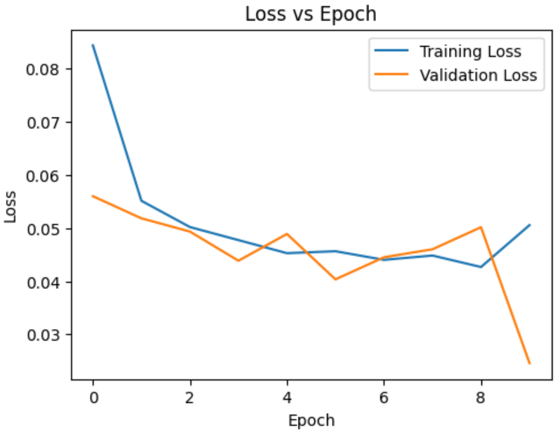

Figure 5. GRU loss-epoch

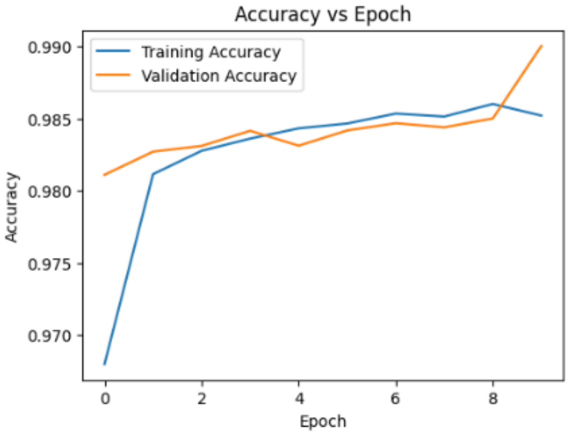

Figure 6. GRU accuracy-epoch

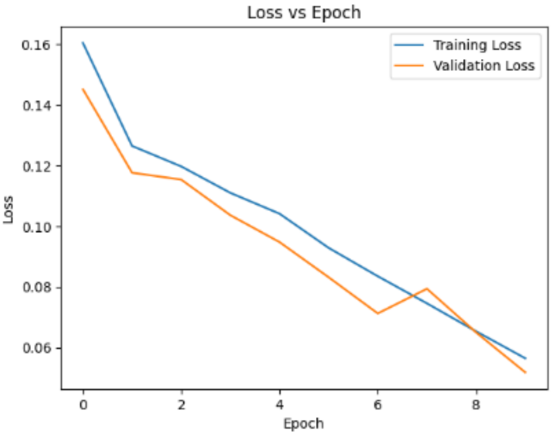

Figure 7. DBN loss-epoch

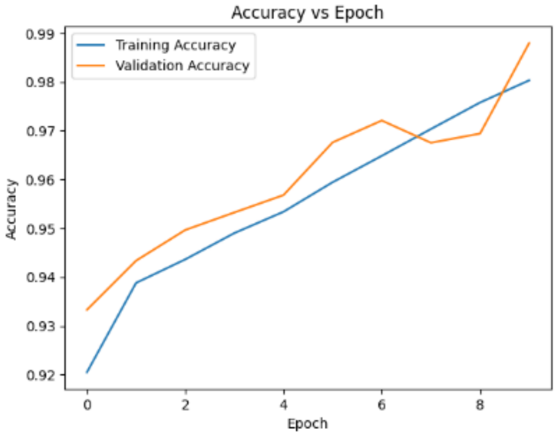

Figure 8. DBN accuracy-epoch

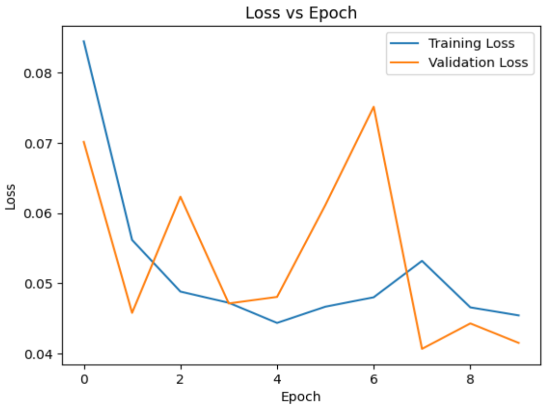

Figure 9. LSTM loss-epoch

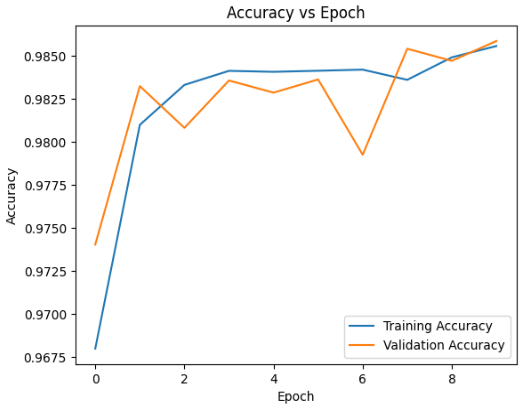

Figure 10. LSTM accuracy-epoch

5. CONCLUSION

The research highlights the crucial role of useful datasets in cybersecurity research, particularly as it applies to SGN. By leveraging a contrived dataset generated from CyberGrid, the paper showcases how such datasets can facilitate experimentation, evaluation, and development of cybersecurity solutions. The utilization of CyberGrid, a virtual testbed established by the Cybersecurity Research Lab at Obafemi Awolowo University, validates its effectiveness as a platform for simulating cyberattacks in substation automation systems. This validation enhances confidence in the accuracy and reliability of the dataset generated from the testbed. Consequently, the research evaluates DL algorithms, including GRU, DBN, and LSTM, for intrusion detection in SGN. By experimenting with these algorithms using the contrived dataset, the paper provides insights into their performance and suitability for addressing cybersecurity challenges in the smart grid domain. Specifically, the preference for GRU, DBN, and LSTM models underscores their potential for accurately detecting and classifying cyber threats in substation automation systems. These findings have practical implications for cybersecurity practitioners and researchers involved in securing SGN. They provide guidance on selecting appropriate DL algorithms and highlight the importance of utilizing relevant datasets for effective intrusion detection and cybersecurity strategy development. Overall, the research contributes to advancing the understanding and application of DL techniques in addressing cybersecurity challenges in the smart grid, while emphasizing the significance of curated datasets in facilitating meaningful research outcomes.

ACKNOWLEDGMENTS

The Research was supported by funding from the Digital Science and Technology Network (DSTN), France, through the Research Partnership programme with the OAU-Knowledge Pack, Africa Centre of Excellence, Obafemi Awolowo University, Ile-Ife, Nigeria.

REFERENCES

[1] J. E. Efiong, B. O. Akinyemi, E. A. Olajubu, I. A. Ibrahim, G. A. Aderounmu, and J. Degila, “Modelling smart grid instability against cyber attacks in SCADA system networks,” in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 180, 2023, pp. 239–250, doi: 10.1007/978-3-031-36115-9_23.
[2] A. Kenyon, L. Deka, and D. Elizondo, “Are public intrusion datasets fit for purpose characterising the state of the art in intrusion event datasets,” *Computers and Security*, vol. 99, p. 102022, Dec. 2020, doi: 10.1016/j.cose.2020.102022.
[3] E. Wescoat, S. Kerner, and L. Mears, “A comparative study of different algorithms using contrived failure data to detect robot anomalies,” *Procedia Computer Science*, vol. 200, pp. 669–678, 2022, doi: 10.1016/j.procs.2022.01.265.
[4] T. W. MacFarland and J. M. Yates, “Working with large and complex datasets,” in *Using R for Biostatistics*, Cham: Springer International Publishing, 2021, pp. 585–882, doi: 10.1007/978-3-030-62404-0_8
[5] H. Hindy *et al.*, “A taxonomy of network threats and the effect of current datasets on intrusion detection systems,” *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.
[6] R. Venkateswaran and A. Srinivasulu, “Enhancing cybersecurity through advanced threat detection: a deep learning approach with cnn for predictive analysis of ai-driven cybersecurity data,” *Journal of Research in Engineering and Computer Sciences*, vol. 1, no. 5, pp. 65–77, 2023.
[7] S. Yuan and X. Wu, “Deep learning for insider threat detection: review, challenges, and opportunities,” *Computers and Security*, vol. 104, p. 102221, May 2021, doi: 10.1016/j.cose.2021.102221.
[8] F. Rustam, M. F. Mushtaq, A. Hamza, M. S. Farooq, A. D. Jurcut, and I. Ashraf, “Denial of service attack classification using machine learning with multi-features,” *Electronics (Switzerland)*, vol. 11, no. 22, p. 3817, Nov. 2022, doi: 10.3390/electronics11223817.
[9] Y. An and Y. Eun, “Attak detection in RSU-OBU communication using deep neural network,” in *International Conference on*

Control, Automation and Systems, Oct. 2023, pp. 585–589, doi: 10.23919/ICCAS59377.2023.10316754.

[10] G. Megala, S. Prabu, and B. C. Liyanapathirana, "Detecting DDoS attack: a machine-learning-based approach," In *Applications of Artificial Intelligence for Smart Technology*, 2021, pp. 55–66, doi: 10.4018/978-1-7998-3335-2.ch004.

[11] D. Mashima, M. M. Roomi, B. Ng, Z. Kalberczyk, S. M. S. Hussain, and E.-C. Chang, "Towards Automated Generation of Smart Grid Cyber Range for Cybersecurity Experiments and Training," in *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, 2023, pp. 49–55, doi: 10.1109/DSN-S58398.2023.00024.

[12] Netresec, "Capture files from 4sics geek lounge," 2019.

[13] O. Hegazi, E. Hammad, A. Farraj, and D. Kundur, "IEC-61850 GOOSE traffic modeling and generation," in *2017 IEEE Global Conference on Signal and Information Processing*, Nov. 2018, vol. 2018-January, pp. 1100–1104, doi: 10.1109/GlobalSIP.2017.8309131.

[14] Y. Lopes, D. C. Muchaluat-Saade, N. C. Fernandes, and M. Z. Fortes, "Geese: a traffic generator for performance and security evaluation of IEC 61850 networks," in *IEEE International Symposium on Industrial Electronics*, Jun. 2015, vol. 2015-September, pp. 687–692, doi: 10.1109/ISIE.2015.7281552.

[15] S. M. Blair, F. Coffele, C. D. Booth, and G. M. Burt, "An open platform for rapid-prototyping protection and control schemes with IEC 61850," *IEEE Transactions on Power Delivery*, vol. 28, no. 2, pp. 1103–1110, Apr. 2013, doi: 10.1109/TPWRD.2012.2231099.

[16] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, 2019, doi: 10.1109/SmartGridComm.2019.8909783.

[17] P. Radoglou-Grammatikis, V. Kelli, T. Lagkas, V. Argyriou, and P. Sarigiannidis, "DNP3 intrusion detection dataset," *IEEE Dataport*, Nov. 2022, doi: 10.21227/s7h0-b081.

[18] P. Radoglou-Grammatikis, K. Rompolos, T. Lagkas, V. Argyriou, and P. Sarigiannidis, "IEC 60870-5-104 intrusion detection dataset. IEEE dataport," *IEEE Dataport*, Sep. 2022, doi: 10.21227/fj7s-f281.

[19] J. E. Efiong, A. Akinwale, B. O. Akinyemi, E. Olajubu, and S. Aderounmu, "CyberGrid: an IEC61850 protocol-based substation automation virtual cyber range for cybersecurity research in the smart grid," *Cyber-Physical Systems*, pp. 1–20, May 2024, doi: 10.1080/23335777.2024.2350004.

[20] M. M. Alani and T. Baker, "A Survey of smart grid intrusion detection datasets," *In Workshop Proceedings of the 19th International Conference on Intelligent Environments*, 2023, pp. 5-13, doi: 10.3233/AISE230004.

[21] Y. Yang *et al.*, "Cybersecurity test-bed for IEC 61850 based smart substations," in *2015 IEEE Power & Energy Society General Meeting*, 2015, pp. 1–5, doi: 10.1109/PESGM.2015.7286357.

[22] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[23] M. K. Putchala, "Deep learning approach for intrusion detection system (IDS) in the internet of things (IoT) network using gated recurrent neural networks (GRU)," *Wright State University*, p. 64, 2017.

[24] Nisha C. M and N. Thangarasu, "Deep learning algorithms and their relevance: a review," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 4, pp. 1–10, Nov. 2023, doi: 10.59461/ijdiic.v2i4.78.

[25] M. H. Vrejoiu, "Neural networks and deep learning in cyber security," *Romanian Cyber Security Journal*, vol. 1, no. 1, pp. 69–86, 2019.

BIOGRAPHIES OF AUTHORS

John Edet Efiong specializes in industrial cybersecurity. He is a research scholar of the Digital Science and Technology Network (DSTN), France, and a Young Researcher/Alumnus of the Heidelberg Laureate Forum Foundation (HLFF), Germany. He is currently the research team lead at the CyberSCADA/Cybersecurity Research Lab, Africa Center of Excellence, OAU ICT Knowledge-driven park at Obafemi Awolowo University, Ile-Ife, Nigeria. He is the researcher on the CyberSCADA project at OAK Park. He is a member of the Association for Computing Machinery (ACM), with interest covering Industrial Cybersecurity, Industrial Automation and Process Control, Cyber-Physical Systems, OT/IT Networks and IIoT. He can be contacted at email: jeediof@gmail.com.

Jide Ebenezer Taiwo Akinsola is a lecturer in the Department of Computer Sciences at the First Technical University, Ibadan, Nigeria. He is the Chief Operations Officer (COO) of AdunMart Limited and Director of ICT at the Institute of Business Administration and Knowledge Management. He holds a B.Sc., M.Sc., and Ph.D. in Computer Science (specialization in Artificial Intelligence and Data Security). He is a member of Nigerian Computer Society (NCS), Computer Professional Registration Council of Nigeria (CPN) and a fellow of the Institute of Business administration and Knowledge Management. He is an IT Systems and Security Professional and Blockchain Developer Mastery Award winner. He is an alumnus of MSM, Maastricht, The Netherlands and a Fellow of Netherlands Universities Foundation for International Cooperation (NUFIC), His research interests include AI, data security, blockchain technology, digital forensics, cloud security, cryptography, threat modelling, intelligent user interfaces, machine learning, and decision-making systems. He can be contacted at email: akinsolajet@gmail.com.

Bodunde Odunola Akinyemi holds a B.Tech (2005) in Computer Science from Ladoke Akintola University Ogbomosho, M.Sc (2011) and Ph.D (2014) in Computer Science from Obafemi Awolowo University Ile-Ife. She is currently an Associate Professor and member of the Communication Networks and CyberSCADA research groups in the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife. She is a member of the International Association Engineers, IEEE, Nigeria Computer Society (NCS) and Computer Professional Registration Council of Nigeria (CPN). Her major research areas are in data communication, network security and performance management, software development, and BlockChain technology. She can be contacted at email: bakinyemi@oauife.edu.ng.

Emmanuel Ajayi Olajubu is a Professor of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria where he obtained a BSc in Computer Science (with Economics), M.Sc and Ph.D in Computer Science. He is a member of the Nigerian Computer Society (NCS), Computer Professional Registration Council of Nigeria (CPN) and International Association of Engineers (IAENG). His research interests are in the areas of distributed systems, cyber-physical-system, and cybersecurity including network security. He was a former Acting Head of, the Department of Computer Science and Engineering at OAU. He can be contacted at email: emmolajubu@oauife.edu.ng.

Ganiyu Adesola Aderounmu is a Professor of Computer Science and Engineering with several years of research, teaching, leadership, and project funding experiences within and outside Nigeria. He has attracted several research grants and he is currently the Center Leader of the African Center of Excellence, OAU Knowledge-driven ICT park at Obafemi Awolowo University, Ile-Ife, Nigeria, and spearheads the partnership program of the Digital Science and Technology Network (DSTN) project for the OAK-Park, Nigeria and African Center of Excellence in Mathematics, Applications and Physical Sciences, (ACE-SMIA), University of Abomey-Calavi, Benin Republic. He is a former Acting Head of the Department of CSE; former Director of the Information Technology and Communications Unit at OAU. He is a member of the Screening and Monitoring sub-committee of the Tertiary Education Trust Fund (TETFUND) research fund. He served as a member of curriculum development for the National Open University of Nigeria, and a member of COREN, CPN, and NUC accreditation teams respectively to various universities in Nigeria. He is a visiting research fellow, University of Zululand, Republic of South Africa. He is the former National President of the Nigeria Computer Society. He can be contacted at email: gaderoun@oauife.edu.ng.