REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

SCEN-SCADA SECURITY: AN ENHANCED OSPREY OPTIMIZATION-BASED CYBER ATTACK DETECTION MODEL IN SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM USING SERIAL CASCADED ENSEMBLE NETWORK

Fatimah Yaseen Hashim ALZUBAIDI

Ph.D Thesis

Supervisor

Assoc. Prof. Dr. Sefer KURNAZ

İstanbul, 2025

SCEN-SCADA SECURITY: AN ENHANCED OSPREY OPTIMIZATION-BASED CYBER ATTACK DETECTION MODEL IN SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM USING SERIAL CASCADED ENSEMBLE NETWORK

Fatima Yaseen Hashim ALZUBAIDI

Electrical and Computer Engineering

Ph.D. Thesis

ALTINBAŞ UNIVERSITY

2025

The dissertation titled SCEN-SCADA SECURITY: AN ENHANCED OSPREY OPTIMIZATION-BASED CYBER ATTACK SELECTION MODEL IN SUPERVISORY CONTROL AND DATA AC9 VISITATION SYSTEM USING SERIAL CASCADED ENSEMBLE NETWORK prepared by FATIMAH YASEEN HASHIM AL-ZUBAIDI and submitted on 01/12/2025 has been **accepted unanimously** for the degree of Ph.D. in Electrical and Computer Engineering Department.

_____
Assoc. Prof. Dr. Sefer KURNAZ

Thesis Defense Committee Members:

Assoc. Prof. Dr. Sefer KURNAZ	Department of Computer Engineering Altınbaş University	_____
Prof. Dr. Osman Nuri UÇAN	Department of Electrical-Electronic Engineering Altınbaş University	_____
Assoc. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Software Engineering Altınbaş University	_____
Asst. Prof. Dr. Zeynep ALTAN	Department of Software Engineering İstanbul Beykent University	_____
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering İstanbul Arel University	_____

I hereby declare that this dissertation meets all format and submission requirements for a PhD thesis.

I hereby state that all data and material offered in this capstone project were acquired in complete line with ethical standards and scholastic regulations. I further affirm that, in accordance with the aforementioned standards of academic integrity, all borrowed ideas, arguments, and its findings, as well as all the sources indicated in the Reference List, have been correctly cited in the text.

Fatimah Yaseen Hashim AL- ZUBAIDI

Singture

DEDICATION

To my late father, whose memory continues to guide my steps. I am profoundly proud to honor your name through this achievement. Your values, strength, and love remain alive in my heart.

ABSTRACT

SECURITY: AN ENHANCED OSPREY OPTIMIZATION-BASED CYBER ATTACK DETECTION MODEL IN SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM USING SERIAL CASCADED ENSEMBLE NETWORK

AL- ZUBAIDI, Fatimah Yaseen Hashim
M.Sc., Electrical and Computer Engineering, Altınbaş University,
Supervisor: Assoc. Prof. Dr. Sefer KURNAZ

Date: 12 / 2025

Pages: 73

A significant role of Supervisory Control and Data Acquisition (SCADA) systems is supporting power system operation, where Information and Communication Technology (ICT) is adopted to interconnect the devices, and it increases system complexity. Because of the interconnection of SCADA systems, the complexity is increased, and there is a chance of cyber security vulnerabilities. In addition, the SCADA networks with legacy devices are affected by inbuilt cyber security deliberation that has provided severe cyber security vulnerable points. With the adoption of local-area networks and Internet Protocol (IP)-driven proprietary, malicious or unauthorized user accesses the information from outside sources, and hence, the SCADA systems are weakened by the elaborate attacks. SCADA systems need to deliberate the Denial of Service (DoS) and catastrophic failure as well as maloperation, which may subsequently compromise the stability and safety of the operations in the power system. Therefore, the pertinent priority in SCADA is to strengthen cyber security for guaranteeing reliable operation and also, the system stability is governed with respect to communications integrity. The smart grid features are used in the conventional Machine learning approaches for identifying cyber-attacks. Hence, implementing an efficient and accurate cyber-attack detection approach with less computational overhead is still a crucial research problem in SCADA. So, a novel and secure model for cyber-attack detection in the SCADA system using advanced deep learning techniques together with the

heuristic algorithm is executed in this research work. The SCADA data are collected from various power grids. The features from these data are optimally selected and fused with the optimal weights in order to obtain the weighted optimal features. The weighted optimal feature selection is done with the aid of the Enhanced Osprey Optimization Algorithm (EOOA). These optimally selected weighted features are given to the Serial Cascaded Ensemble Network (SCEN) to obtain the final detection output. The developed SCEN is made with the cascading of Autoencoder, Dilated Bidirectional Long Short Term Memory (Bi-LSTM), and Bayesian classifier. The parameters in the SCEN are tuned using the executed IOOA. The final detection of the presence or absence of a cyber attack is evaluated by this SCEN. The performance and the effectiveness of the developed model are verified and contrasted by conducting various experiments.

Keywords: Supervisory Control and Data Acquisition System, Cyber Attack Detection Model, Serial Cascaded Ensemble Network, Enhanced Osprey Optimization Algorithm, SCEN.

TABLE OF CONTENTS

Pages

ABSTRACT vi

LIST OF TABLES..... xi

LIST OF FIGURES..... xii

1. INTRODUCTION..... 1

1.1 BACKGROUND……1

1.2 RESEARCH CONTRIBUTION……3

1.3 OBJECTIVE……...4

1.4 RESEARCH GAPS……4

1.5 PROBLEM STATEMENT…… 4

1.6 RESEARCH MOTIVATION…….7

1.7 THESIS ORGANIZATION……11

2. LITATURE RIVEW..... 14

2.1 OVERVIEW……14

2.2 NEED FOR ADVANCED CYBER ATTACK DETECTION MODELS 14

2.3 RELATED WORK……...15

2.4 CHALLENGES IN SCADA SECURITY……... 18

2.4.1 Legacy Systems……18

2.4.2 Lack of Encryption in Communication Protocols……18

2.4.3 Limited Authentication and Authorization Mechanisms…… 19

2.4.4 Real-Time Operational Requirements……..19

2.4.5 Remote Access and Interconnectivity Vulnerabilities…… 20

2.4.6 Insider Threats……..20

2.4.7 Summary…….. 21

3. METRIAL AND METHODS..... 22

3.1 LAYERED ARCHITECTURE OF SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM WITH DESCRIPTION OF CYBER ATTACK DATASET……...……22

3.2 ARCHITECTURE OF SCADA SYSTEM……..22

3.3 DATA ACQUITISION……... 23

3.4 PROPOSED CYBER ATTACK DETECTION MODEL IN SCADA…….. 24

3.5 SELECTION OF OPTIMAL FEATURES AND WEIGHTS USING ENHANCED OPTIMIZATION STRATEGY FOR DETECTING CYBER ATTACKS IN SCADA…… 26

3.6 TRADITIONAL OOA…….. 26

3.7 PRESENTED EOOA…….. 29

3.8 OPTIMAL WEIGHTED FEATURE SELECTION……... 33

3.9 DETECTION OF CYBER ATTACKS IN SCADA USING DEVELOPED SERIAL CASCADED ENSEMBLE NETWORK WITH OPTIMAL TUNING OF HYPERPARAMETERS……. 34

3.10 BASIC AUTOENCODER……... 34

3.11 BASIC DILATED BILSTM……. 34

3.12 BASIC BAYESIAN CLASSIFIER……. 36

3.13 SCEN-BASED CYBER ATTACK DETECTION…….. 36

4. RESULTS AND DISCUSSION..... 39

4.1 EXPERIMENTAL SETUP …… 39

4.2 PERFORMANCE MEASURES…… 39

4.3 PERFORMANCE VALIDATION IN TERMS OF THE CONFUSION MATRIX ……..40

4.4 CONVERGENCE EXAMINATION…….. 41

4.5 ANALYSIS OVER BASELINE WORKS…….. 48

4.6 PERFORMANCE VERIFICATION AMONG ALGORITHMS AND PREVIOUS TECHNIQUES……52

4.7 STATISTICAL ANALYSIS ON HEURISTIC ALGORITHMS……55

5. RESULTS AND DISCUSSION..... 56

5.1 CONCLUSION……56

5.2 FUTURE WORK……56

REFRENCES..... 58

LIST OF TABLES

Pages

Table 1.1: Merits and Challenges of Conventional Cyber Attack Detection System In SCADA..... 6

Table 3.1: Dataset Representation Of The Collected Scada Data From Wind Turbines. .. 23

Table 4.1: Validation Of Performance On Developed Cyber Attack Detection Model Among Various Algorithms. 53

Table 4.2: Validation of Performance on Developed Cyber Attack Detection Model Among Various Techniques. 54

Table 4.3: Statistical Evaluation on Developed Cyber Attack Detection Scheme Among Various Heuristic Algorithms..... 55

LIST OF FIGURES

Pages

Figure 3.1: Structrural View of SCADA Systems in ICS Networks. 23

Figure 3.2: Developed Cyber Attack Detection Model in SCADA Systems Using Serial Cascaded Ensemble Network. 25

Figure 3.3: Step by Step Chart of Proposed EOOA. 32

Figure 3.4: Schematic Depiction of Proposed Cyber Attack Detection Using SCEN. 38

Figure 4.1: Confusion Matrix Examination On Proposed SCEN-based Cyber-Attack Detection Model Regarding for Dataset 1. 40

Figure 4.2: Confusion Matrix Examination on Proposed SCEN-based Cyber Attack Detection Model Regarding for Dataset2 41

Figure 4.3: Cost Function Estimation of the Proposed SCEN-based Cyber Attack Detection Model According to Dataset 1. 42

Figure 4.4: Cost Function Estimation Of The Proposed SCEN-based Cyber Attack Detection Model According to Dataset 2. 42

Figure 4.5: Detection Performance of the Implemented SCEN-Based Cyber Attack Detection Model Regarding (A) Accuracy For Dataset 1. 43

Figure 4.6: Detection Performance of The Implemented SCEN-Based Cyber Attack Detection Model Regarding FPR For Dataset 1. 44

Figure 4.7: Detection Performance of the Implemented SCEN-based Cyber Attack Detection Model Regarding Percision for Dataset 1. 44

Figure 4.8: Detection Performance of the Implemented SCEN-Based Cyber Attack Detection Model Regarding NPV for Dataset 1. 45

Figure 4.9: The Detection Performance of The Recommended SCEN-based Cyber Attack Detection Framework Regarding for Dataset 2. 46

Figure 4.10: The Detection Performance of the Recommended SCEN-based Cyber Attack Detection Framework Regarding FPR for dataset 2. 46

Figure 4.11: The Detection Performance of the Recommended SCEN-based Cyber Attack Detection Framework Regarding Precision for Dataset 2. 47

Figure 4.12: The Detection Performance of the Recommended SCEN-Based Cyber Attack Detection Framework Regarding NPV for dataset 2. 47

Figure 4.13: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding (a) Accuracy (b) FPR (b) Precision (b) NPV for Dataset 1. 48

Figure 4.14: Detection Performance of the offered SCEN-based Cyber Attack Detection Model Regarding FPR. 49

Figure 4.15: Detection Performance of the offered SCEN-based Cyber Attack Detection Model Regarding Precision for Dataset 1. 49

Figure 4.16: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding NPV for Dataset 1. 50

Figure 4.17: Detection Performance of the offered SCEN-based Cyber Attack Detection Model Regarding Accuracy for Dataset 2. 50

Figure 4.18: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding FPR for Dataset 2. 51

Figure 4.19: Detection Performance of the offered SCEN-based Cyber Attack Detection Model Regarding Percision for Dataset 2. 51

Figure 4.20: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding NPV for Dataset 2. 52

ABBREVIATIONS

AI	:	Artificial Intelligence
ANN		Artificial Neural Networks
CFS	:	Correlation-based Feature Selection
CNN	:	Convolutional Neural Network
CPS	:	cyber–Physical System
DCNN	:	Deep Convolutional-Recurrent Neural Network
DCS	:	Distributed Control Systems
DG	:	Distributed Generation
DL	:	Deep Learning
GEO	:	Geography Optimization
HMI	:	Human Machine Interface
HMM		Hidden Markov Models
IBL	:	Instance-Based Learning
ICS	:	Industrial Control System
IDS	:	Intrusion Detection Systems
ITS	:	Information Technology System
MCC	:	Mathews Correlation Coefficient
MITM	:	Man in the Middle
MTU	:	Master Terminal Unit
PLC	:	Programmable Logical Controllers

RTU	:	Remote Terminal Units
SCADA	:	Supervisory Control and Data Acquisition
SVM	:	Support Vector Machine
TSA	:	Tuna Swarm Algorithm

1. INTRODUCTION

1.1 BACKGROUND

Risk management requirements, performance requirements, and communication are various kinds of aspects considered between an Industrial Control System (ICS) and an Information Technology System (ITS) [1]. The ICS network is time-critical, and fault tolerance is highly important in ICS.

The safety of humans is also essential in ICS networks [2]. In ICS, several proprietary communication protocols are utilized that does not require certification of IDs, timestamp, and encryption encouraged by various vendors [13]. The addressed fault and information reveals, as well as delay in these protocols, are caused by some attacks like “Replay and Zero-day attacks, DoS and Man in the Middle (MITM)” in ICS [4].

These types of attacks in ICS systems can engender huge damage and information revealed into the physical infrastructure [5]. Therefore, cyber security in Supervisory Control and Data Acquisition (SCADA) systems is currently a vital part, and it is broadly used in ICS for ensuring controlled process security. Furthermore, the intelligent manufacturer is comprised of highly secured SCADA that includes important key components such as the protection of controlled processes and physical infrastructures, asset management, and communication protocols [6]. In this system, the network equipment, Programmable Logical Controllers (PLC), Distributed Control Systems (DCS), Remote Terminal Units (RTU), computers, servers, and also the supporting software like Human Machine Interface (HMI) are considered as the significant key elements [7].

The SCADA systems are no connections to the outside world because they are completely isolated [8]. But, this has been modified nowadays, and the ICS networks are constructed with the help of various commodity components that are interlinked to the Internet or external networks. This result in the ICS networks being highly exposed to cyber-attacks, and this gives a chance for attackers to steal the data and damage physical processes [9].

The major aspect considered during the designing of security solutions in ICS networks poses that the resource constraint components used in the ICS networks cannot be easily

reconfigured and updated, and the ICS networks have functioned without any longer interruptions [10]. Because of these hiders, the host-based deployed security solutions build in other environments. Therefore, the monitoring of communication between different ICS equipment present in the system is needed without any changes in the network that has been accomplished with the help of Intrusion Detection Systems (IDS) [11].

The developed IDS approaches functioned on three different levels such as (a) the flooding attacks in the network are identified by monitoring the general behaviors of host and ICS network, (b) the malformed messages or the abnormal messages are effectively identified by monitoring the details of the exchanged message among the field services and control servers (iii) the IDS approach is designed to be process aware that describes the monitoring the physical process interpretation should be supervised by the ICS networks [12]. The significant benefit of using this IDS approach is it does not need any physical process knowledge. But, they do not have the ability to detect the attacks designed for damaging the physical process [13].

The process-aware IDS is important to provide higher security against various attacks in SCADA networks. The process designer is used to provide the specification about the behavior state of the physical process in specification-based IDS [14]. This technique is well-suitable for processes with formal specifications available in the networks and it could be monitored easily. But, the traditional ICS networks should not contain the digital twin or the formal specification. In this situation, the IDS has been implemented with the consideration of learning the specifications from the historical data [15].

In the learned predicted models, if the variation among the measured and predicted observations is higher than the threshold value, the IDS raises the alert message during the prediction of process variables. But, it is not suitable for the noisy nature of actual sensors, which makes comparing values more crucial while detecting attacks. In addition, the selection of threshold values is very important, and there are no formal algorithms for preferring threshold factors. Invariant rules-based algorithms are utilized to identify the attacks. But, the important disadvantage of these invariant-based IDS is that they consider the behavior of the physical process without notifying time evolution [16].

This crucial type of cyber Physical System (CPS) is a smart grid and it incorporates various

transmission proficiencies of smart equipment to the grid. This has facilitated the control and remote operation of power systems. This integration of smart devices has resulted in potential violations of security contributions in smart grids. Changing firmware, stealing sensitive information, and injecting function codes on the smart grid via appropriate devices are considered examples of realizable attacks in SCADA [17].

Hence, it is crucial to identify the cyber attacks very earlier on the grid to conserve it from serious activities. Traditionally, machine learning approaches are helpful for identifying cyber attacks via the extraction of features from SCADA. However, implementing an accurate and effective high cyber attack detection is needed with decreased computational overload. Preventing cyber attacks in its earlier stage is a very challenging research problem in SCADA. Hence, a new ensemble machine learning-based cyber attack detection scheme to provide security is developed in SCADA.

1.2 RESEARCH CONTRIBUTION

The major contribution of our work will be as follows.

a. To design an advanced and enhanced heuristic algorithm assisted deep learning-based cyber attack detection framework in SCADA in order to prevent the data theft and manipulation of data in the SCADA attacks by means of cyber attacks as well as physical attacks in the power system.
b. To deploy an improved deep learning model called Serial Cascaded Ensemble Network (SCEN) which is constructed by cascading the Autoencoder, Dilated Bidirectional Long Short-Term Memory (Bi-LSTM), and Bayesian classifier to classify the presence or absence of cyber attacks in SCADA system.
c. To implement an Improved Osprey Optimization Algorithm (OOA) for optimizing the parameters in the developed SCEN classifier to detect the cyber attacks in SCADA with less computational complexity and processing time.
d. To execute the developed heuristic-aided deep learning cyber attack detection framework using real-time dataset, and to compare its performance with conventional classifiers, and existing traditional optimization algorithms.

1.3 OBJECTIVE

The main objective of this work will be to implement an advance deep learning-based cyber-attack detection framework in SCADA system with the assistance of optimization algorithm in order to prevent the data manipulation and data theft in the power system.

1.4 RESEARCH GAPS

a. The major reasons for executing the efficient cyber attack detection system in SCADA are provided below:
b. Since most of the existing SCADA system doesn't have an active monitoring system for frequently observing the suspicious activities in the SCADA system, the detection of the cyber attack in a continuous manner remains a difficult task.
c. The attributes like the SCADA bit count, reference number, data, and data of the register are not considered in existing machine learning-based cyber attack detection system in SCADA which results in inadequate detection.
d. The detection outcomes produced by the conventional deep learning-based cyber attack detection system are inaccurate because of processing a huge volume of data.
e. Since the SCADA system is inter-connected with various Internet Protocols (IP), the computational overload is high in the existing cyber attack detection models.
f. Existing works can able to detect the attack in the cyber field but does not consider the physical attacks in the SCADA system which may lead to inefficient detection results.

1.5 PROBLEM STATEMENT

The complexity and the interconnectivity of the SCADA system in the power system make the power system more vulnerable to cyber-attacks. The cyber attack protection system aims to prevent only the attacks in the cyber field but does not consider the physical attacks in the SCADA system. The existing IDS are not process-aware. Hence, efficient cyber as well as physical attack-resistant systems have to be developed. The features and the challenges of the conventional cyber attack detection systems in SCADA are provided in Table I. CFS and KNN [18] method minimizes the computational overload as well as enhances the precision of the smart grids. This method also decreases the features required for performing the classification, improves the accuracy of detection, and reduces the cost and time required for the detection of cyber attacks. But, this method is unable to handle different-sized data of

huge volumes. The efficiency of the detection technique is not as per the requirement. HMM and ANN [19] are used to identify legitimate anomalies as they consider time as a factor. The use of the simple feature extraction method also results in enhanced accuracy. But, this method does not consider the contextual features, which results in inadequate detection accuracy. The factors such as reference number, bit count, data of the register, data, and the written data of the MODBUS are not considered, which may lead to inadequate detection of anomalies in the PLC system. The false alarm rate in this method is high as the PLC's IP address is not taken into consideration. The instances of the classes are not labeled in this method as unsupervised learning methods are adopted. SCADA-IDS [20] are highly beneficial in addressing cyber attacks in digital substations and provide more security to smart grids. However, the physical attacks are not detected by this method. The installation cost is high, and it is not supported by all the software and hardware components. SVM, NHFC, and fuzzy classifier [21] can able to detect the zero-day attack, MITM attacks, buffer overflow, DoS, and reply attacks in physical and cyber fields in the SCADA network. Yet, the location at which the attack is happening and the type in which the attack belongs to is not known by this method. This method is not able to protect against manufacturing process attacks. RNN [22] prevents the hacking of the metering system. The detection rate provided by this method is high, and the false alarms are reduced in this method. But, the training process of this method is more difficult. Large sequence data is not able to be processed. The time required for processing the data is high and the computational process is highly complicated. Supervised and semi-supervised algorithm [23] is able to identify the time-dependent characteristics of the SCADA system and can learn the automaton for indicating the time-dependent behaviors of the system. But, it is not able to deal with complex tasks, and the computational time taken is more. SCADA-IDS [24] can protect the modern substation from electrical infrastructure-based cyber attacks. But, the data regarding the operation of these substations are not considered in this method. Time-based IDS [25] has the ability to learn temporal characteristics of the physical process in the ICT system, thus enhancing detection accuracy. This method is quick, and it relies on a few configuration variables. But, the temporal relationship between various processing parameters is not taken into account. An efficient cyber attack prevention and detection system is therefore implemented to overcome and tackle all these challenges using heuristic-assisted deep learning methods.

Table 1.1: Merits and Challenges of Conventional Cyber Attack Detection System In SCADA.

Author [citation]	**Methodology**	**Features**	**Challenges**
Gumaei*et al.* [18]	CFS and KNN	• This method minimizes the computational overload as well as enhances the precision of the smart grids. • This method also decreases the features required for performing the classification, improves the accuracy of detection, and reduces the cost and time required for the detection of cyber attacks.	• This method is unable to handle different-sized data of huge volumes. • The efficiency of the detection technique is not as per the requirement.
Kalech [19]	HMM and ANN	• This method is used to identify legitimate anomalies as it considers time as a factor. • The use of the simple feature extraction method also results in enhanced accuracy.	• This method does not consider the contextual features, which results in inadequate detection accuracy. • The factors such as reference number, bit count, data of the register, data, and the written data of the MODBUS are not considered, which may lead to inadequate detection of anomalies in the PLC system. • The false alarm rate in this method is high as the PLC's IP address is not taken into consideration. • The instances of the classes are not labeled in this method as unsupervised learning methods are adopted.

Table 1.1: Merits and Challenges of Conventional Cyber Attack Detection System In SCADA "Table Continued".

Yang *et al.* [20]	SCADA-IDS	• This method is highly beneficial in addressing cyber attacks in digital substations and provides more security to smart grids.	• The physical attacks are not detected by this method. • The installation cost is high, and it is not supported by all the software and hardware components.
Qian *et al.* [21]	SVM, NHFC, and fuzzy classifier	• It can able to identify the zero-day attack, MITM attacks, buffer overflow, DoS, and reply attacks in physical and cyber fields in the SCADA network.	• The location at which the attack is happening and the type to which the attack belongs is not known by this method. • This method is not able to protect against manufacturing process attacks.
Ismail *et al.* [22]	RNN	• The hacking of the metering system is prevented by this method. • The detection rate provided by this method is high, and the false alarms are reduced in this method.	• The training process of this method is more difficult. • Large sequence data is not able to be processed. The time required for processing the data is high, and the computational process is highly complicated.
Shlomo*et al.* [23]	Supervised and semi-supervised algorithm	• It is able to detect the time-dependent characteristics of the SCADA system and can learn the automaton for indicating the time-dependent behaviors of the system.	• It is not able to deal with complex tasks, and the computational time taken is more.
Yang *et al.* [25]	SCADA-IDS	• It can protect the modern substation from electrical infrastructure-based cyber attacks.	• The data regarding the operation of these substations are not considered in this method.

1.6 RESEARCH MOTIVATION

As motivations for this research, we consider the ever-rising trend of both the number of events as well as their level of sophistication of cyber attacks on critical infrastructure

SCADA systems. Against this background of the evolving cyber threat landscape, Supervisory Control and Data Acquisition (SCADA) systems become an invaluable component of the current information technology environment in the following ways. The role of modern SCADA systems has become critical in supporting the efficient operation of critical infrastructure facilities like electricity production, processing of drinking water, oil, as well as natural gas. The IT-OT convergence environment, which encompasses modern SCADA systems, has been exposed to the same cyber threats as conventional IT environment settings [26], [27].

The cyber community has experienced the rise of various cyber attacks in the course of the previous decade, which prove critical weaknesses of SCADA systems. The Stuxnet virus, which occurred in the year 2010, BlackEnergy in 2014, Industroyer in 2016, Triton in 2017, among others, show how state-sponsored actors with sophisticated strategies can exploit the use of industrial control systems (ICSs) in order to maliciously cause destruction of various industrial processes [28][29]. The cyber attacks will continue to pose significant impacts on various countries in the event that the actors continue using sophisticated strategies. The attacks will tend to focus on multi-staged strategies that will leave less of an impact until its activation.

Classical rule-based intrusion detection and signature-based firewall approaches, which perform well on known threats, fail to provide an effective means of coping with modern cyber attacks [30].

The specified attacks' signature or rule criteria lack adaptability concerning the evolving cyber attacks. As a consequence, an intense need has arisen for intelligent cyber attack discovery approaches that can dynamically adapt themselves according to evolving cyber attacks in real time without impeding SCADA performance or reliability.

The fusion of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) into the cybersecurity field opens promising avenues of improvement in existing SCADA protection methodologies. The use of machine learning-driven intrusion detection systems (ML-IDSs) has proved promising in detecting unusual network traffic patterns through data modeling [31].

The disadvantage of such intrusion detection approaches encompasses a number of ambiguities, including redundancy of features, complexity of calculations, or lack of compatibility with SCADA scaled systems. As an intrinsic step of data preprocessing, feature selection plays an important role in resolving ambiguities of intrusion detection methodologies by discerning the most informative data characteristics leading to proper classification [32].

Recently, there has been interest in the use of metaheuristic optimization algorithms as efficient tools for feature selection and optimization of parameters of machine learning models [33]. Among various optimization algorithms, the Osprey Optimization Algorithm (OOA), which is a bio-inspired algorithm, has been found promising. The OOA is inspired by the hunting behavior of ospreys, which are hunting birds that demonstrate adaptability of decisions, awareness, and position adjustments during hunting [34].

The adaptability in hunting by the osprey can be translated into computational optimization in terms of an efficient trade-off between global and local searches. This trade-off plays a key role in efficiently resolving optimization problems of larger dimensions, as encountered in SCADA cybersecurity.

Through the incorporation of OOA into the feature selection technique used in the SCADA attack detection task, the proposed research seeks to improve the accuracy of the classification task, alleviate the computation costs, as well as ensure optimal generalization. OOA's flexibility allows it to dynamically traverse highly complex spaces concerning features, thus identifying the most influential features leading to the separation of normal from malicious network activities. This will ensure optimal functioning of the detection system, even with unknown attacks. Also, the removal of redundancy in features will ensure the inclusion of real-time detection, which is important in preventing large-scale disruptions.

To complement OOA, this work proposes a Serial Cascaded Ensemble Network (SCEN), which is a hybrid ensemble approach that ensures the highest level of classification accuracy. Contrary to conventional ensemble methods, which use a Bagging or Boosting approach in a parallel fashion, SCEN uses an iterative or stage-by-stage design, where the output of one classification stage serves as the enhanced input for the next [35]. As a result, multiple classification models can compensate for the mistakes of their predecessors, thus improving

detection accuracy while minimizing false positives. Ensemble learning, which uses optimal sets of features, has been demonstrated to enhance immunity from adversarial examples and noise [36], [37].

The rationale of carrying out the SCEN-OOA combination is based on reaching a synergistic level of intelligent feature selection and learning by ensembles. The OOA is instrumental in making sure that the most informative or discriminative features are kept, while SCEN ensures that classification is done on the consensus among various models. The proposed combination seems most appropriate in the SCADA domain, which requires real-time processing, reliability, and low false alarm rates. For mission-critical domains like SCADA, there can be significant losses in case of a detection delay or a false alarm. Therefore, the proposed combination will provide an optimal tradebetween accuracy and speed of processing. Furthermore, this work is driven by the need for cyber resilience in the current Industry 4.0 and Industrial Internet of Things (IIoT) environment. The current practice of linking smart sensors, cloud computing, and control devices has resulted in a larger attack surface area, which has led to various security issues [38].

The task of ensuring cyber resilience in an SCADA system involves learning continuously, staying aware of the environment, and adapting quickly to threats, which can be perfectly achieved by AI-optimized detection models. Through the use of the powers of both OOA and SCEN, the proposed work will help develop a self-learning cybersecurity system that can protect critical infrastructure from sophisticated cyber threats. Third, the relevance of this research does not stop there. There is an immense need or application of this research not only from an intellectual or exploratory pursuit, but it is an acute necessity. The aftereffect of cyber attacks on an SCADA system can be profoundly dangerous. The destruction can include blackouts in global powers, along with Environmental disasters like oil spills that can affect humanity globally. The design of an efficient cyber safety system can not only be an intellectual or technological challenge, it can also become an issue of humanity. The authors of this research hope that this can be achieved by the design of the SCEN-SCADA Security Framework by Osprey Optimization.

1.7 THESIS ORGANIZATION

This work will be divided into five main chapters, each of which will tackle a particular issue relating to the research. The design will ensure that there is a logical order of approaches, from explaining the significance of the problem with an introduction, then going into the literature review, the methodology, the results, and ending with the conclusions.

a. The first chapter introduces the research topic and its relevance. The chapter opens with background information of Supervisory Control and Data Acquisition (SCADA) systems. The introduction brings into focus the importance of SCADA systems in the overseeing of critical infrastructure like the electrical grid, water utilities, or industrial automation. The use of SCADA started in an isolated environment, meaning it was not connected. However, this has led to the rise of cybersecurity threats.

The research gaps in the current models of cybersecurity, including the challenge of conventional intrusion detection systems (IDS) in the SCADA scenario, will be identified in this chapter. The identified gaps will help address the problem statement, which pertains to the need for an intelligent, adaptive, and efficient cyber attack detection model specific to SCADA.

Moreover, it can be seen that the research motivation section discusses in more depth the threat landscape, which encompasses the sophistication of current cyber attacks, including Advanced Persistent Threats (APTs), ransomware attacks, and nation-state attacks. The motivation section introduces the use of optimization algorithms in general, including Osprey Optimization Algorithm (OOA), as well as the Serial Cascaded Ensemble Network (SCEN), which provides more accurate detection. The research chapter ends by discussing the scope, objective, and contribution of this research.

b. Chapter 2 provides a comprehensive review of existing literature. The chapter begins with an introduction on how the security of SCADA systems is of paramount importance, along with the need for efficient models capable of protecting the system from cyber attacks.

The section on related work examines various strategies pursued by researchers in recent years to improve the state of cybersecurity in SCADA. The approaches covered encompass

the use of machine learning, deep learning, or optimization techniques. The methodologies, merits, and demerits of the strategies form the basis of the current research.

The largest portion of this chapter will be dedicated to discussing the challenges in SCADA security, which include vulnerability in legacy systems, the use of unencrypted communication protocols, authentication, authorization, real-time operations, remote access, and insider threats. Each of the subsections (2.4.1–2.4.6) of this chapter will discuss every challenge in depth, focusing on how each of them inhibits the use of effective cybersecurity practices. The discussion of the research gap will be summarized at the end of this chapter, which will help determine the findings from the literature review that will be used as the motivation of the proposed methodology of the next chapter.

c. Chapter 3: Materials and Methods This chapter represents the essence of the thesis, dealing with the proposed methodology and its technical foundation. The first section of this chapter will describe the architecture of SCADA systems, as well as the characteristics of the cyber attack datasets.

The architecture of the SCADA system is expounded upon, detailing the communications layers, data acquiring processes, as well as the control elements. The data acquiring subsection talks about how data is preprocessed and prepared for use in training and testing.

The chapter then presents the proposed cyber attack detection method, which combines feature selection, optimization, and a machine learning approach. The proposed method utilizes an Enhanced Osprey Optimization Algorithm (EOOA) that optimizes the process of selecting key features or weights in classification.

Subsections 3.6 through 3.8 discuss how the transformation from the conventional OOA evolved into the improved EOOA, explaining the changes that enhanced faster convergence, exploration-exploitation tradeoff, and efficient computation. The optimal weighted feature selection is then introduced as an important step in reaching an accurate lightweight model.

The second half of this chapter (Sections 3.9-3.13) relies on the Serial Cascaded Ensemble Network (SCEN), which is a multi-level learning system involving various classification models (Autoencoder, Dilated BiLSTM, Bayesian Classifier) that make use of an ensemble

learning approach in order to effectively identify cyber attacks. There is a detailed description of every single element of this network.

d. Chapter 4: Results and Discussion provides the experimental results, followed by a detailed discussion of the findings. The description of experimental setup introduces the hardware and software environment, datasets, as well as parameters used in testing the proposed approach.

The section on performance measures describes how measures of detection performance are calculated using accuracy, precision, recall, F1 measure, and detection rate. The confusion matrix analysis will be used to give an insight into the classification of various attack classes.

The following discussion will continue with the convergence characteristics of the algorithms, which will demonstrate how EOOA optimizes better than conventional metaheuristics. The comparison of the proposed work with existing ones will show the effectiveness of the SCEN-EOOA model.

The section on performance verification compares the proposed method with other state-of-the-art algorithms and approaches. The effectiveness of the proposed method is then validated by carrying out rigorous experiments. Finally, the statistical analysis of heuristic algorithms is performed.

e. Chapter 5: Conclusion and Future Work, The final chapter concludes the thesis by summarizing the key findings and contributions of the research. It reiterates how the proposed Enhanced Osprey Optimization Algorithm (EOOA) and Serial Cascaded Ensemble Network (SCEN) synergistically improve the detection of cyber attacks in SCADA systems.

The conclusion highlights the major outcomes, including enhanced detection accuracy, optimized feature selection, and reduced computational complexity. The future work section outlines possible extensions of this research, such as real-time deployment in industrial control systems, the use of hybrid optimization methods, and adaptation to other critical infrastructure sectors. This chapter closes the thesis by emphasizing the broader implications of the study and its contribution to the evolving field of industrial cybersecurity.

2. LITATURE RIVEW

2.1 OVERVIEW

Supervisory Control and Data Acquisition (SCADA) plays an indispensable role in the field of industrial control system (ICS) infrastructure. The role of SCADA in various industries like energy, drinking water, manufacturing, and transportation is not only useful for monitoring industrial operations, acquiring data, or supervising industrial infrastructure remotely in real-time, but it also focuses on the efficient operation of an industry. The entire SCADA infrastructure comprises various modules like sensors, programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs), and data transmission networks.

The rise in the use of SCADA technology in automating various processes has resulted in efficiency gains, cost reductions, and enhanced decision-making. However, the increased connectivity of SCADA with information technology (IT) and the Internet of Things (IoT) has resulted in SCADA becoming more susceptible to various cyber attacks. The challenge posed by the association of SCADA with different technological developments needs to be tackled in order to avoid possible disruptions.

2.2 NEED FOR ADVANCED CYBER ATTACK DETECTION MODELS

Owing to the aforementioned issues, conventional cybersecurity tools like firewalls and anti-virus software alone cannot provide adequate protection from cyber attacks on SCADA systems. As an alternative solution, Intrusion Detection System (IDS), Machine Learning (ML)-based security approaches offer immense promise. However, most of the existing machine learning approaches face issues regarding high false positives, ineffectiveness in handling zero-day attacks, as well as scalability.

To fill this gap, this research proposed an Enhanced Osprey Optimization Based Cyber Attack Detection Model with an incorporation of the Serial Cascaded Ensemble Network (SCEN), which can bolster the security of SCADA. The proposed methodology uses approaches of nature-inspired optimization to increase the efficiency of feature selection as well as classification.

2.3 RELATED WORK

In 2020, Gumaei *et al.* [1] have proposed an effective and efficient approach for providing security on the smart grid. The security over the smart grid has been given by detecting cyber security attacks. In this cyber attack detection framework, the feature reduction and detection approaches were merged to decrease the huge amount of features and accomplish a greater cyber attack detection rate. Finally, the cyber attack detection rate has been highly improved. Consequently, the irrelevant features have been eliminated with the help of using the Correlation-based Feature Selection (CFS) approach in order to improve detection efficiency. Then, the normal and events with cyber attacks have been classified through the Instance-Based Learning (IBL) procedure via the adoption of selected optimal features. Lastly, a set of experiments have been performed among public datasets gathered from a SCADA smart grid power system. Here, the 10-fold cross-validation method has been used for conducting the experiments. Results findings show that the developed model accomplished a greater attack detection rate on the basis of fewer amount of features taken from SCADA.

In 2019, Kalech [2] has proposed a temporal pattern recognition-related cyber-attack identification approach in SCADA. The usage of temporal pattern recognition as did not only search for the anomalies when the data was forwarded by the components of SCADA through the smart grid network. In addition, the developed model searched the anomalies that were aroused due to the misused legitimate commands, which were drawn by unauthorized and incorrect time intervals among the users. The unauthorized access was detected through “Hidden Markov Models (HMM) and Artificial Neural Networks (ANN)” with less computational power. The real-world SCADA data has been considered for the evaluation of performance among five different feature extraction methods, and the experimental findings proved its effectiveness when contrasted to the traditional cyber attack detection models in SCADA.

In 2014, Yang *et al.* [3] have offered a novel intrusion detection scheme for a future generation of SCADA-specific smart grid systems. In this proposed scheme, the comprehensive solution has been attained by analyzing the multiple attributes which has the ability to eliminate cyber-attack threats. In addition, the behavior-based concept and a heterogeneous white list concept were exhibited in the multi-attribute intrusion detection

system to make the SCADA cyber systems more secure. The SCADA cyber security in smart grids has been provided with the utilization of a multilayer cyber-security framework with respect to the intrusion detection system without compromising the normal data availability. The simulated attacks have been investigated to ensure the detection efficiency of implemented approach regarding some validation metrics.

In 2020, Qian *et al.* [4] have proposed a security system in SCADA system by detecting the MITM attack and Replay attacks in both physical way and cyber way. The malicious behaviors in the network have been detected with the help of the validation of process states for preventing the damage of physical components that occurred due to the "Zero-day attacks, Replay, and MITM". The branching-shaped data has been realized by using the nonparallel hyperplane-based fuzzy classifier that was very complicated to categorize in SCADA systems. In addition, the DoS and other attacks in the system were detected by employing Support Vector Machine (SVM) with two parallel hyperplanes in the cyber field. This developed algorithm has been tested through Modbus/TCP traffic data, and the validation part was tested via the simulation process states. The performance of the developed hybrid cyber attack detection scheme was high when analyzed through traditional algorithms.

In 2020, Ismail *et al.* [5] have investigated the electricity thefts that occurred in SCADA systems in Distributed Generation (DG) domain. In this model, the smart meter monitoring has been hacked by malicious customers based on renewable DG units for manipulating their readings in order to claim higher supplied energy. Therefore, the falsely overcharged energy has been displayed as the outcome in the company. The malicious behavior has been detected by using the deep machine learning algorithm. To deal with the issues, they revealed the investigation with the integration of meteorological reports, several data from the SCADA metering points and DG smart meters while training and the developed Deep Convolutional-Recurrent Neural Network (DCNN) has offered the lowest false alarm rate and highest detection rate.

In 2021, Shlomo *et al.* [6] have recommended a novel cyber attack detection scheme by adopting two machine learning procedures. Initially, the supervised algorithm was developed for finding the frequently considered temporal sequences, and then the data payload of the SCADA transmission protocols was adopted for recognizing these patterns.

After recognizing these patterns, several features were attained, and it was applied to the classification algorithm. Secondly, the unsupervised algorithm was utilized for automation learning in order to summarize the temporal behavior. By analyzing the temporal behaviors, the detected unknown events or states during runtime were declared as malicious activities. Lastly, the real datasets have been considered for the evaluation of performance, where the initially utilized supervised in regards to the frequent temporal patterns provided efficient outcomes rather than baseline algorithms. The secondly utilized unsupervised algorithm has given even better results than the first one.

In 2017, Yang *et al.* [7] have proposed an efficient intrusion detection approach in IEC 61850-based substations to provide cyber security. The effective and comprehensive solution has been accomplished with the help of integrating protocol specifications, physical knowledge, and logical behaviors for mitigating various types of cyber security attacks. In addition, the developed intrusion detection model comprised protocol whitelisting, multi-parameter-based, model-based and access control–based detection. Finally, the comprehensive and realistic datasets have been considered for validating the performance of the proposed SCADA-specific IDS with respect to the data from an actual 500 kV smart substation.

In 2022, Ndonda and Sadre [8] have proposed a time-related process-aware IDS to detect attacks as opposed to physical processes. This has been accomplished by leveraging its temporal properties and regular nature. In this developed IDS, the temporal characteristics of the process attributes were effectively learned for identifying the attack vulnerabilities. Here, the effectiveness of the developed IDS model has been validated with the consideration of the public SCADA dataset while concerning the two traditional process-aware IDS. The experimental outcome was shown that the obtained solution has the ability to detect attacks very effectively.

2.4 CHALLENGES IN SCADA SECURITY

Supervisory Control and Data Acquisition (SCADA) plays an important role in monitoring as well as controlling critical infrastructure sectors like electricity production, drinking water supply, oil & gas pipelines, as well as transportation. However, despite their use significance, SCADAs still experience various issues concerning their security. The issue of SCADA security is of particular importance as SCADAs were initially operated in an isolated environment, which was proprietary. However, nowadays SCADAs operate in an interconnected environment using standard communications techniques and Internet communications. The following subsections give a clear description of the challenges encountered in SCADA security.

2.4.1 Legacy Systems

Legacy systems pose one of the biggest challenges in SCADA security. Legacy SCADA systems date back to a time when cybersecurity was not a key issue. Legacy SCADA systems will often fail to incorporate current security measures such as encryption, proper authentication, or intrusion detection. Legacy SCADA systems stand defined by design decades ago. Cybersecurity does not form part of legacy SCADA system design [39][40].

The issue of modernizing or replacing legacy SCADA system modules provides significant obstacles. The fact is that, in most industrial settings, legacy SCADA systems are deeply embedded in physical processes that cannot be interrupted or slowed down. Closing down critical infrastructure in order to repair or upgrade it can lead to significant losses. Moreover, it is often too expensive to perform an update or replacement of legacy hardware or software, most of which is customized [41]. There is a tendency, therefore, on the part of organizations to continue using legacy SCADA systems that have expired, thus making them susceptible to all forms of cyber threats. Cyberattackers can take advantage of software bugs that have not been fixed.

2.4.2 Lack of Encryption in Communication Protocols

The other significant problem is the lack of encryption in conventional SCADA communication protocols like Modbus, DNP3, or IEC 60870-5-104. The afore-mentioned conventional SCADA communication protocols lack focus on security. Originally, they are

capable of sending messages in plain text [42]. As a result, malicious entities able to tap into the network traffic can easily intercept, modify, or create malicious messages. This makes SCADA communications prone to eavesdropping, man-in-the-middle attacks, or malicious data modifications.

Although newer secure variants of the protocol, including Modbus Secure and DNP3 Secure Authentication, do exist, there has been a degree of reluctance on the parts of various organizations in adopting them. This has been owing not only to the restrictions imposed by outdated infrastructure, which could result in an overall slowdown in speed resulting from the use of encryption, among other issues. Other vendors of industrial controls still make use of proprietary versions of the protocol that lack encryption [43]. The vendors consider that by making the SCADA system physically distinct, they will not be vulnerable since this is referred to as "security by obscurity." However, this hypothesis is accurate nowadays.

2.4.3 Limited Authentication and Authorization Mechanisms

Lack of authentication can be an important weakness found in SCADA systems. Legacy systems often lack proper authentication tools or make use of only simple username/password authentication or do not use authentication altogether [44]. As a result, it becomes simpler for an unauthorized user, both internal or external, to gain access to the control interfaces and data. Lack of proper authorization controls can make this problem worse by granting users unnecessary levels of access [45].

The lack of role-based access controls or multifactor authentication mechanisms in most industrial control systems provides an environment where an attacker with compromised credentials can laterally move across the entire network. The lack of granular controls is particularly concerning in multi-vendor SCADA networks where all the different parts of the network will seamlessly communicate with each other, often following different security standards. Applying modern authentication concepts will help address this problem, though this entails a tremendous re-architecture of the network.

2.4.4 Real-Time Operational Requirements

The SCADA system is built to handle very tight real-time constraints. For example, sensor or actuator data has to be responded to in milliseconds. Otherwise, system failures can occur.

For instance, if there is a delay in the transmission of signals in an electricity grid, it can lead to an unstable electricity grid or an interrupted industrial process [46].

Due to the real-time constraints, it becomes difficult to execute conventional cybersecurity tools that incorporate computational or communications delays. For example, servers that perform encryption, deep packet inspection, or behavior anomaly detection often incur additional processing or latency [47]. As a result, cybersecurity tools often compromise on reliability in favor of overall system functionality. This enables an attacker to successfully execute an attack based on the premise that processing delays will preclude its defeat.

There is a need for a balanced solution that can incorporate lightweight security tools in a manner that enables real-time processing while ensuring safety from cyber attacks. Research on real-time cryptographic algorithms, hardware-assisted encryption processing, or edge anomaly detection has been promising in this regard.

2.4.5 Remote Access and Interconnectivity Vulnerabilities

The rise in the need for remote monitoring and control has completely changed the threat scenario in the world of SCADA. The traditional concept of SCADA was an ‘air-gapped’ network, which was inaccessible. The rise in the use of remote access, the cloud, and IIoT concepts has increased an OT environment’s connectivity with the IT infrastructure [48].

Even though this interconnected world of SCADA systems can increase efficiency levels by carrying out predictive maintenance, this increased connectivity also broadens the attack surface [49] . Backdoor channels, VPNs, or third-party connections can quickly become entry points if not properly protected. However, it was seen in various SCADA attacks that misconfigured firewalls, bad passwords, or vulnerable remote desktop servers led to malicious attacks. The Stuxnet incident of 2010 showed how malicious actors can gain entry into the control network by means of compromised remote access or updates [50] . This makes protecting remote access a challenge that can be accomplished by network segmenting, monitoring, or implementing zero-trust models.

2.4.6 Insider Threats

Insider threats, both malicious or accidental, rank among the most complex issues in terms of detection and prevention in an SCADA environment. As insiders, engineers, operation

personnel, or maintenance personnel enjoy legitimate access to the critical system, which allows malicious or accidental insiders to compromise network security [51]. While malicious insiders can disable alarms, modify process parameters, or release sensitive operation information from the system either by force or by financial benefit, accidental insiders can pose vulnerabilities by connecting unauthorized devices or not following security policies.

Insider attacks can be difficult to identify, given that legitimate users' behavior can be similar to normal system behavior. Legacy boundary security tools can be inadequate against insiders who already have valid authentication. Today, this problem can be tackled by adopting an overall approach that combines technological tools, which may include behavior-focused monitoring, user activity analysis, or access recording, with organizational measures like training, security auditing, and overall accountability [52].

2.4.7 Summary

Securing SCADA communications is a complex task influenced by technical, operational, and human issues. Legacy infrastructure, the absence of encryption, lack of authentication, real-time constraints, remote access issues, and insider threats make it difficult to increase the resilience of SCADA networks. This can be overcome by implementing a broad cybersecurity approach involving modernizing legacy infrastructure, implementing secure communication protocols, multi-layered access controls, real-time monitoring solutions, and a culture of awareness. Until then, it will be difficult for SCADA networks to be efficient as well as resilient to current cyber threats.

3. METRIAL AND METHODS

3.1 LAYERED ARCHITECTURE OF SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM WITH DESCRIPTION OF CYBER ATTACK DATASET

3.2 ARCHITECTURE OF SCADA SYSTEM

ICS are the systems used to manage and control the industrial processes aroused in industrial facilities such as plants, factories, and water treatment facilities. It typically consists of SCADA that includes distributed controller devices and Master Terminal Unit (MTU). The controlling and monitoring of physical processes are done with the help of MTS because it is a type of server in the plant. The status data and sensor data are collected by the MTU from field devices and then take proper decisions based on certain events happen. After, the commands related to the events are sent by them. The field devices are RTU or PLC that are interconnected to the actual sensors like pressure sensors and temperature sensors and also the actuators like valves and engines. IP-based network with some protocols is utilized for communicating the field devices and MTU in modern ICS.

The SCADA system includes three levels in processing data during communication that are supervisory level, control level and management level. In the control level, a huge amount of data is gathered from sensors to the PLCs. The collected data will be transferred to the station of the operator in supervisory level. This data will be analyzed with the PLC's set points and PLC's make decision that instruction will be forwarded to the actuators. This has been done in control level. The instructions to the actuators and the data from the sensors are monitored in the supervisory level. The attacks on the PLC's tamper the information collected by the sensors and hence there is a possibility to make false decision by the controllers. Therefore, the cyber attack detection methodologies are needed in SCADA system to provide higher security during decision making. The structural view of SCADA in ICS is given in below Fig. 1.

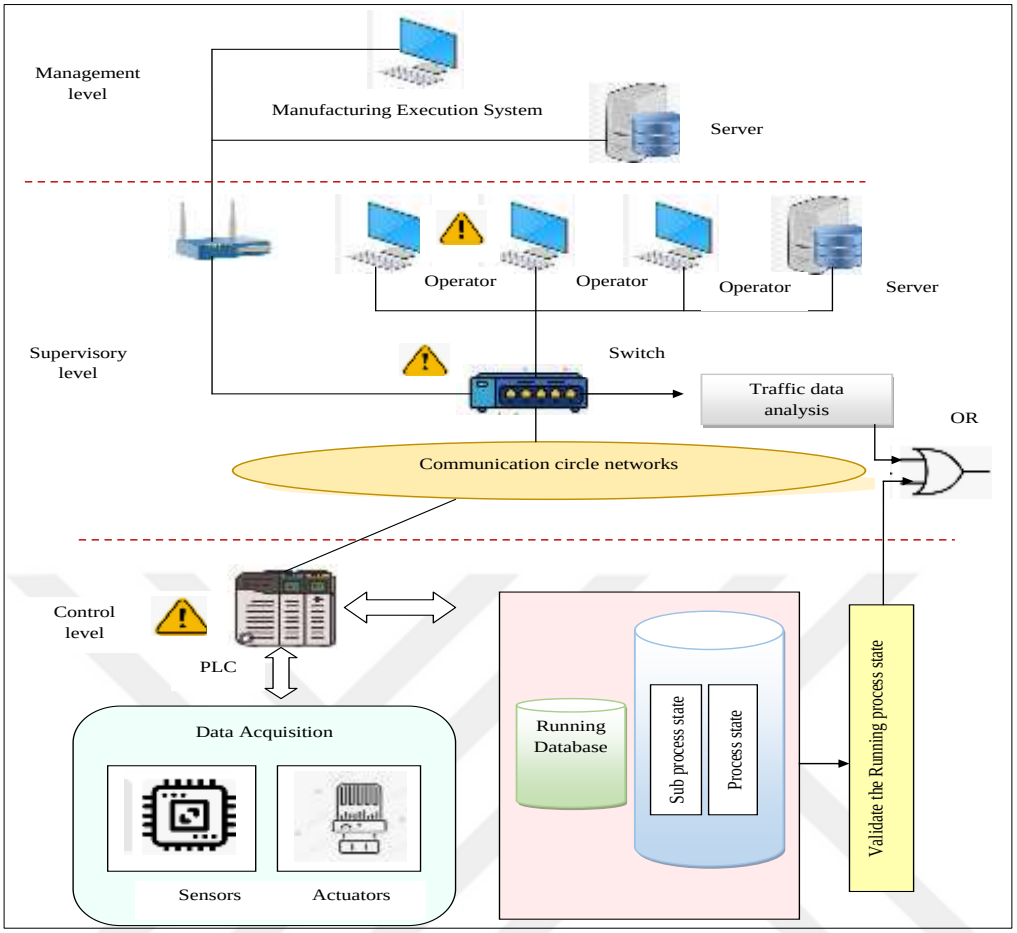

Figure 3.1: Structrural View of SCADA Systems in ICS Networks.

3.3 DATA ACQUITISION

The dataset used for deploying and executing the developed deep learning based cyber-attack detecting model along with its description is provided Table 3.1.

Table 3.1: Dataset Representation Of The Collected Scada Data From Wind Turbines.

Sl o.	Dataset Name	Dataset Link	Dataset Description
1)	Wind Turbine SCADA Dataset	"https://www.kaggle.com/datasets/berkerisen/wind-turbine-scada-dataset access date: 2023-03-31"	This data set is available in Kaggle website. This dataset consists of information gathered from the SCADA system in wind turbine. The attributes like velocity of the wind, direction of the wind flow, power generated from the wind turbine, etc, are provided in this dataset. The active SCADA system in a wind turbine in Turkey provides these resources for this dataset. The data are grouped in 5 files in 5 columns date/time, active power, wind speed, theoretical power curve, and the direction of the wind.

Table 3.1: Dataset Representation Of The Collected Scada Data From Wind Turbines "Table Continued"

2)	Operation SCADA Dataset of an Urban Small Wind Turbine in São Paulo, Brazil	"https://zenodo.org/record/7348454#.ZCaoi3ZBxPZ access date: 2023-03-31"	This dataset contains the electrical and mechanical operational parameters of a rooftop installed a small wind turbine at the University of Sao Paulo, Brazil. The data in this dataset were recorded in the year 2017 to 2022. The electrical attributes like energy, voltage, current, and frequency and the mechanical attributes like rotation, and direction of the wind turbine along with common attributes like temperature, alarms, DC bus voltage, etc, are provided in this dataset.

The obtained raw data from the wind turbines are signified by RW_a^{Tur}, where $a = 1,2,3\ldots,A$ indicates the amount of collected data.

3.4 PROPOSED CYBER ATTACK DETECTION MODEL IN SCADA

An efficient cyber attack detection approach is developed to identify the cyber attack vulnerabilities and malicious activities for providing higher security in SCADA systems using a serial cascaded ensemble network. The data required for mitigating the cyber attack vulnerabilities are gathered from traditional online databases of wind turbines. From the raw data, the weights optimization takes place with the help of EOOA and the most helpful features from the data are also selected via the developed EOOA. From these optimally tuned weights and selected features, the optimally weighted features are attained by concatenating these weights with the features. This optimally weighted feature improves the cyber attack detection performance in terms of maximized variance and minimized correlation coefficient. The optimal weighted features are applied to the classification process, where the serial cascaded ensemble network is adopted to classify the features. The SCEN is formulated by serially connecting the networks like an autoencoder, dilated BilSTM and Bayesian classifier to detect the cyber-attack vulnerabilities. The hidden neurons and epochs from autoencoder and also hidden neuron count, as well as steps per epochs from BiLSTM and Bayesian networks, are optimized through the proposed EOOA to increase the detection efficiency regarding with the metrics like "accuracy, precision, Mathews Correlation Coefficient (MCC) and False Positive Rate (FPR)". The malicious activities in SCADA are detected using the proposed SCEN very effectively, and high security is provided. The

experimental outcome is ensured with the baseline cyber attack detection approaches in terms of several validation metrics to guarantee the security of SCADA systems. The diagrammatic illustration of the proposed cyber attack detection approach in SCADA to provide security is showcased on Fig.3.2.

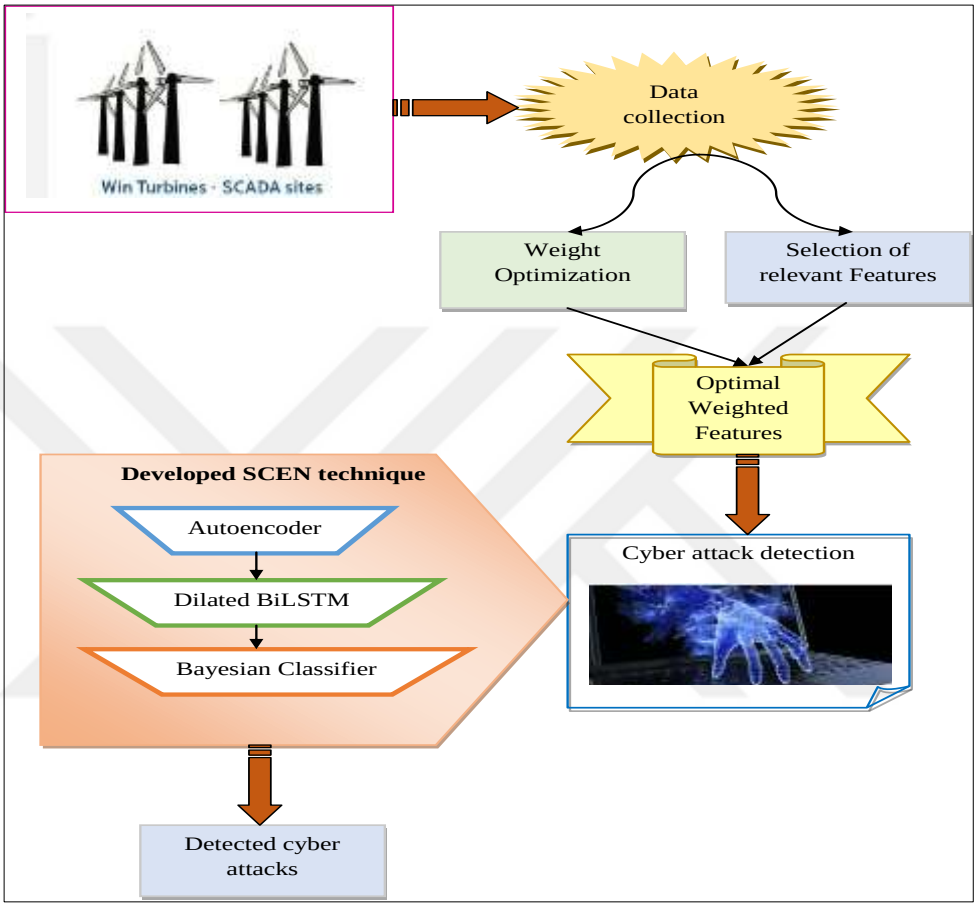

Figure 3.2: Developed Cyber Attack Detection Model in SCADA Systems Using Serial Cascaded Ensemble Network.

3.5 SELECTION OF OPTIMAL FEATURES AND WEIGHTS USING ENHANCED OPTIMIZATION STRATEGY FOR DETECTING CYBER ATTACKS IN SCADA

3.6 TRADITIONAL OOA

OOA [26] is a metaheuristic algorithm that imitates the characteristics of Osprey in nature. The hunting behavior of Osprey is the inspiration for OOA. In addition, the simulation behavior of ospreys is demonstrated in two phases' exploration and exploitation while hunting. The other name for ospreys is river hawk, fish hawk, and sea hawk. The most apparent Osprey behavior is listed below.

a. The color of the upper parts is deep-glossy brown and the underparts are shown in pure white color.

b. The head color of the Osprey is white with a black mask beyond the eyes.

c. The eye's irises are seen in white with black talons and the tails of the Osprey are short or long.

The ospreys update their position in the exploration and exploration phases on the basis of simulation behaviour.

Initialization phase: In the problem-solving phase, the ospreys provide a solution with respect to the searching power of the population candidates. The value of the problem variable is calculated by each Osprey in the OOA population on the basis of the position in the solution space. Each Osprey in OOA it is expressed using a vector. The Osprey's position in the problem-solving space is expressed in Eq. (3.1).

$$y_{u,v} = LRB_v + rd_{u,v} \cdot (URB_v - LRB_v),$$
$$u = 1,2,\ldots,V, v = 1,2,\ldots,U \tag{3:1}$$

Here, the term$Y$defines the population matrix of the location of the prey, $y_{u,v}$defines the dimension of$v$in problem space,$Y_u$represents theu^{th}Osprey, the osprey number is denoted

by$U$, the number of problem variable is indicated by$V$, the lower bound as well as the upper bound are indicated byLRB_vandLRB_v, respectively and also the random number between$[0,1]$is denoted by$rd_{u,v}$. The objective function of the vector is indicated by the termFn, where the u^{th}Osprey's objective function is denoted asFn_u. The ospreys' has the ability to determine the fish from underwater by using their strong eyesight. The ospreys attack the prey after finding the position of the Osprey. This natural behavior of the prey is considered for the updating of position in OOA. In underwater, the updating of position in problem space is the better objective function and the set of Osprey is specified in Eq. (3.2).

$$Fn_u = \{Y_l | l \in \{1,2,\ldots,U\} \wedge Fn_l < Fn_u\} \cup \{Y_{BST}\} \tag{3:2}$$

The position set ofu^{th}Osprey is indicated by$Fn_u$and the best candidate position is signified asY_{BST}. The ospreys randomly detect the location of the prey to hunt it. On the basis of the simulation of the ospreys' movement toward the fish, and then a new location is estimated, that is given in Eq. (3.4-3.5). Then, the objective function is increased by using the new position updated.

$$y_{u,v}^{z_1} = y_{u,v} + rd_{u,v} \cdot \left(dm_{u,v} - J_{u,v} \cdot y_{u,v}\right), \tag{3:3}$$

$$y_{u,v}^{z_1} = \begin{cases} y_{u,v}^{z_1}, & LRB_v \le y_{u,v}^{z_1} \le URB_v \\ LRB_v, & y_{u,v}^{z_1} < LRB_v \\ URB_v, & y_{u,v}^{z_1} > URB_v \end{cases} \tag{3:4}$$

$$Y_u = \begin{cases} Y_u^{z_1}, & Fn_u^{z_1} < Fn_u \\ Y_u, & else \end{cases} \tag{3: 5}$$

The new position of u^{th}Osprey is denoted $Y_u^{z_1}$on the basis of the initial position and$dm_{u,v}$gives the preferred fish inv^{th}dimension. The ransom numbers from the set are indicated by $J_{u,v}$and the objective function value is denoted as$Fn_u^{z_1}$. The random parameter$rd_{u,v}$is selected in the interval of$[0,1]$and$v^{th}$the dimension of Osprey is signified as$y_{u,v}^{z_1}$.

After hunting the fish, the ospreys it carries to a suitable position to eat. This behavior is considered for the simulation of the exploitation phase. When the ospreys carry the fish in

new positions in search space, there are small changes in its position and give better solutions.

The suitable position of ospreys is given in Eq. (3.6-3.8). The previous position of the Osprey is modified based on the lower and upper bound.

$$y_{u,v}^{z_2} = \frac{y_{u,v} + rd_{u,v} \cdot (URB_v - LRB_v)}{e}, \tag{3:6}$$

Here, the terms$u, v$and$e$are distributed in the interval of$u = 1,2,\ldots,V, v = 1,2,\ldots,U, e = 1,2,\ldots,E$. The position of the Osprey inv^{th}dimension is noted by$y_{u,v}^{z_1}$.

$$y_{u,v}^{z_2} = \begin{cases} y_{u,v}^{z_2}, & LRB_v \le y_{u,v}^{z_2} \le URB_v \\ LRB_v, & y_{u,v}^{z_2} < LRB_v \\ URB_v, & y_{u,v}^{z_2} > URB_v \end{cases} \tag{3:7}$$

$$Y_u = \begin{cases} Y_u^{z_2}, & Fn_u^{z_2} < Fn_u \\ Y_u, & else \end{cases} \tag{3.8}$$

The new position ofu^{th}Osprey is denoted by$Y_u^{z_2}$the new objective function value is denoted as$Fn_u^{z_2}$. The random attribute$rd_{u,v}$is chosen in the range between$[0,1]$, the iteration number of this algorithm is signified as$e$and the total count of iterations is noted by$E$. The position updating process is carried out until it reaches the last iteration count. The pseudocode of the OOA is represented in Algorithm 1.

Algorithm 1: OOA
Start OOA
Initialize the problem information attributes
Initialize the number of iterations and size of the population.
Create the initial population matrix.
Estimation of the objective function using Eq. (2).
For$e = 1 to E$
For$u = 1 to U$
Identification of position and hunting fish
Fish set position updating using Eq. (4).
Check the boundary condition of the new Osprey.
Carrying the hunted fish to the appropriate position
Estimate the position of the new Osprey using Eq. (7).
Check the boundary condition of the new Osprey.
Save the best candidate solution.
End for
End for
Stop the termination criteria.
End

3.7 PRESENTED EOOA

The EOOA is used in the cyber attack detection scheme in SCADA systems to boost

detection performance by optimally tuning the parameters. The weights from the collected data are optimally tuned, and the features from the data are preferred using EOOA, and these are given to the feature concatenation process. This optimally weighted feature improves the "variance and correlation coefficient". In addition, the hidden neuron and epoch count from autoencoder and also the hidden neuron, as well as steps per epoch from Dilated BiLSTM and Bayesian classifier, are optimally tuned for maximizing the accuracy and precision with less false positive error. The OOA algorithm is utilized in the cyber attack detection model because of its simplicity in structure and good convergence rate. In addition, it requires fewer parameters in search space to get the optimal solution. Yet, it lacks scalability issues. Hence, to address these issues EOOA algorithm is implemented with a modified random parameter concept based on the fitness function. The random attribute $rd_{u,v}$ is impoverished in regards to best and worst fitness functions. In the conventional OOA, the random attribute $rd_{u,v}$is chosen at random in the range between$[0,1]$, which does not provide the efficient optimal solution over huge dimensional data. But, the upgraded random parameter provides the better optimal solution, which is given in Eq. (3.9).

$$rd_{u,v} = \left(\frac{(BestFit \wedge 1.5)}{(WorsttFit \wedge 1.5)}\right) \quad (3: 9)$$

The term$rd_{u,v}$gives the randomly distributed attribute used for the updating of position in OOA. The best fitness of the solution is represented by$BestFit$and the worst fitness of the solution is indicated by$WorstFit$. The appropriate balancing of exploitation and exploration abilities is provided by using this developed EOOA during the search for the best optimal solution in the search space. The pseudocode of the proposed EOOA is depicted in Algorithm 2. The step-by-step diagram of implemented EOOA is depicted in Fig. 3.

Algorithm 2: EOOA
Start OOA
Initialize the problem information variables in the solution space
Fix the number of iterations and size of the population

Create the initial population matrix
Initialize the random parameter. $rd_{u,v}$
Update the random parameter$rd_{u,v}$using the newly developed concept
For$e = 1toE$
For$u = 1toU$
Identification of position and hunting fish
Fish set position updating using Eq. (4).
Check the boundary condition of the new Osprey.
Carrying the hunted fish to the appropriate position
Estimate the position of the new Osprey using Eq. (7).
Check the boundary condition of the new Osprey
Save the best candidate solution
End for
End for
Return
End

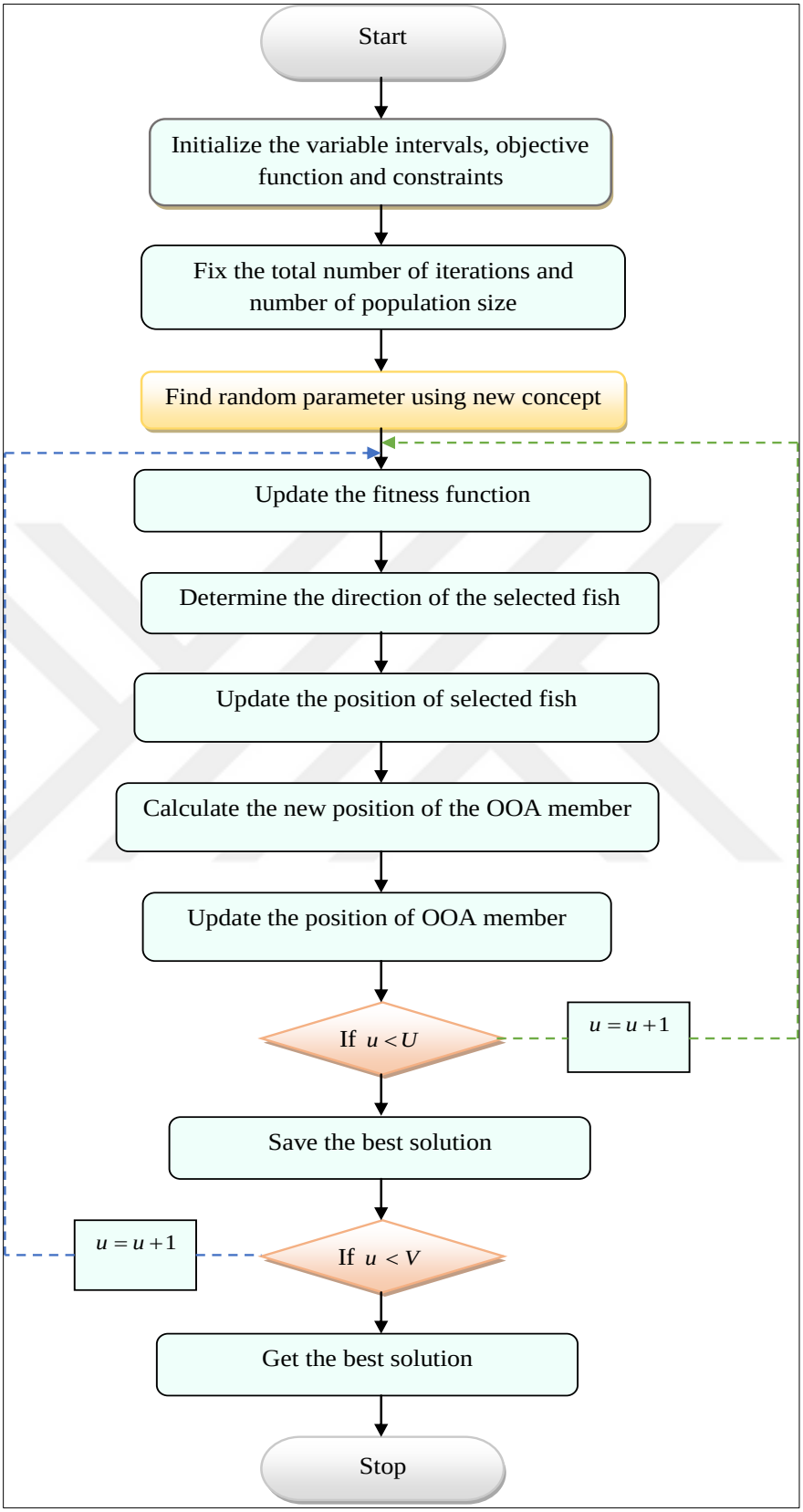

Figure 3.3: Step by Step Chart of Proposed EOOA.

3.8 OPTIMAL WEIGHTED FEATURE SELECTION

The collected raw data are RW_a^{Tur} given to the optimal weighted feature selection stage to make the classification process very easier. The weights from the raw data are optimally tuned and the features from the wind turbine data are optimally selected using the developed EOOA to decrease the dimensionality problem and computational burden. The optimally tuned weights are denoted by the term WE_d^{Raw}, and the optimally selected features from the data are represented as FS_e^{Raw}, these weights and features are multiplied to get the optimally weighted features. These features make the classification or detection very easier and it overcomes the problem of time consumption during the classification of the huge volume of data. The finally attained optimal weighted features are indicated by the term OW_{a*}^{Eo}.

The objective function of the optimal weighted feature is expressed in Eq. (3.10).

$$B_1 = \underset{\{WE_d^{Raw}, FS_e^{Raw}\}}{\arg\min} \left(\frac{1}{VR + CC} \right) \tag{3:10}$$

The variance is indicated by VR and the correlation coefficient is signified as CC during the selection of optimal weighted features. The optimally tuned weights are denoted by WE_d^{Raw} and also the optimally selected features are indicated by FS_e^{Raw}. The weights are tuned in the range between $[0.001, 0.09]$ and the features are optimized in the interval of $[1, 100]$. The formula for variance and correlation coefficient is expressed below in Eq. (3.11) and Eq. (3.12).

$$VR = \frac{\sum (e_i - \bar{e}_i)^2}{N-1} \tag{3:11}$$

The elements in the sample are denoted as e_i the mean of the sample is denoted as $\bar{e}_i$ and the size of the sample is indicated by N.

$$CC = \frac{\sum (e_i - \bar{e}_i)(f_i - \bar{f}_i)}{\sqrt{\sum (e_i - \bar{e}_i)^2 (f_i - \bar{f}_i)^2}} \tag{3.12}$$

The term e_i is the sample of e variable, f_i is the sample of f variable, $\bar{e}_i$ is the mean of e variable and $\bar{f}_i$ is the mean of f variable.

3.9 DETECTION OF CYBER ATTACKS IN SCADA USING DEVELOPED SERIAL CASCADED ENSEMBLE NETWORK WITH OPTIMAL TUNING OF HYPERPARAMETERS

3.10 BASIC AUTOENCODER

The autoencoder are used for identifying the cyber attacks in SCADA smart grid systems. The autoencoder [30] compresses the input data in multi-dimension that is done in hidden space and hence it is named an unsymmetrical symmetrical neural network. After, the data has been reconstructed from the compressed original data in the same hidden space. The autoencoder is comprised of the input layer, a hidden layer, a reconstruction layer and one activation function layer.

The activation function is any nonlinear function and it is denoted by the termAf. The formulation of the activation function is formulated in Eq. (3.13).

$$Af(t) = \frac{1}{1+exp^{-t}} \tag{3:13}$$

The encoding layer is the layer between the input and hidden layer, where the hidden layer is the latent space resemblance. The multi-dimensional data is highly decreased to a smaller size. The decoding layer is the layer among hidden and output layers. The compressed hidden space layer size is increased to reconstruct the input data by the decoding layer.

The set of input instances of $i$is denoted by the termγ. The autoencoder has the ability to reduce the data reconstruction error. The loss function of the autoencoder is represented by the squared error. The autoencoder with loss function is illustrated in Eq. (3.14).

$$Ls(\gamma) = \sum_{i\in\gamma} \|i - \hat{\imath}\|^2 \tag{3:14}$$

Here, the term$\hat{\imath}$is indicated as the reconstructed input instance$i$. Finally, an attack prediction score is obtained from this autoencoder structure.

3.11 BASIC DILATED BILSTM

The Dilated BiLSTM [31] is used in the developed model for cyber attack detection to improve security over SCADA. The casual convolution layer is introduced in between the input layer and convolution filter that is fed to the overlapping regions of the series

sequentially. The size of the input context window is increased with the usage of more model parameters that consume huge memory size and also, the long-range memory capacity is largely saturated. The dilation factor is introduced in the dilation convolution and it is responsible for creating the space between the value masks. The 3×3 mask with dilation factor and5×5receptive field is used in this dilated convolution. Totally nine model parameters are presented in the dilated convolution with the same receptive field. Hence, the wider field of view is delivered in the dilated convolution with the same computational cost. The dilated convolution among the input data and mask is given in Eq. (3.15).

$$G(i) = (h * cs)_i = \sum_{\vartheta=0}^{p-1} h_\vartheta \cdot s_i - c_\vartheta \tag{3:15}$$

The dilation factor is indicated by$c$, and the filter size is represented by$p$. From the long history data, the local trends of patterns are extracted by using this dilated convolution.

The BiLSTM network consists of forward and backward propagation with a forward LSTM layer. With respect to the back LSTM, the forward LSTM reverse the input data. The past and future information is considered in the output layer during the training of the LSTM layer. Hence, the past and future information are simultaneously attained via the hidden cells. The cost of computation regarding forward and reverse layers in BiLSTM is the same. In the hidden states of data, the direction of propagation is reversed for getting the sequential type of data. Evaluation of forward and reverse layers in the BiLSTM network is given in Eq. (3.16) and Eq. (3.17), correspondingly.

$$H_s = s(W_{s1} \cdot z_s + W_{s2} \cdot H_{i-1}) \tag{3:16}$$

$$H_B = s(W_{B1} \cdot z_i + W_{B2} \cdot H_{i+1}) \tag{3:17}$$

The output of forward and reverse LSTM are indicated by the terms$H_s$andH_B, respectively. The final output from the BiLSTM layer is estimated through Eq. (3.18).

$$O_P = l\big(W_{y1} * H_s + W_{y2} * H_B\big) \tag{3:18}$$

From the above expression, the weight values are indicated by the terms W_{y1}andW_{y2},

respectively. The cyber-attack prediction score is obtained at the output of Dilated BiLSTM network.

3.12 BASIC BAYESIAN CLASSIFIER

The Bayesian classifier [32], known as the belief network, is generally an augmented directed cyclic graph. The graph is signified by$Gr(U, D)$, where$U$is a vertices set and$D$is directed edges set, which joins vertices. For any length, no loops of the Bayes network are allowed. The name of a random variable is contained in each vertex$U$and the probability distribution table is maintained in the Bayesian classifier. This table indicates the probability of values variables depends on the possible combination of all parental values.

Several procedures are followed during the construction of the Bayesian classifier, which is summarized as follows.

a. From the training dataset, select a set of relevant variables.

b. Select the order for the variables.

c. Assume the order is in the format of$R_1, R_2, \ldots, R_n$, where the first order is denoted by$R_1$and the second order is indicated byR_2.

d. For $i = 1 to n$

i. Add the new node$R_i$to the network.

ii. With a minimal subset$\{R_1, R_2, \ldots, R_{i-1}\}$, the parents$R_i$are set to the network and these parents have conditional independence.

iii. Then, the probability of the table is defined as is $Pb(R_i = l|Parentsassignment(R_i)))$

Finally, the cyber attack detection score is attained at the output of the Bayesian classifier.

3.13 SCEN-BASED CYBER ATTACK DETECTION

The cyber security vulnerabilities present in the SCADA networks are detected through the developed SCEN model. Here, the machine learning classifiers like autoencoder, dilated

BilSTM and Bayesian classifier are serially connected to develop SCEN. The developed EOOA algorithm is adopted in the proposed cyber security attack detection framework to optimally select the hyperparameters from the proposed SCEN. The hidden neuron and epoch count from the autoencoder classifier are optimized, the hidden neuron count and steps per epoch from Dilated BiLSTM are optimally tuned and also the hidden neuron as well as steps per epoch from Bayesian classifier is optimally tuned via EOOA to increase the accuracy, MCC, precision, and decrease FPR. The learning ability of SCEN-based cyber security attack detection is also high when contrasted to the previous machine learning models. The objective functions of using the EOOA algorithm in SCEN during the detection of cyber attack vulnerabilities are expressed in Eq. (3.19).

$$B_2 = \underset{\left\{\substack{Hi_u^{AE}, Eh_v^{AE} Hi_w^{LSTM}, \\ ST_x^{LSTM} Hi_y^{BC}, STz_z^{BC}}\right\}}{\arg\min} \left(\frac{1}{Ar + Pn + MCC} + FPR \right) \tag{3:19}$$

The optimized hidden neuron from autoencoder in the interval of $[5,255]$is denoted by the termHi_u^{AE}, the epoch from autoencoder in the interval of$[5,50]$is indicated byEh_v^{AE}, the tuned hidden neuron from Dilated BiLSTM and Bayesian classifier in the range of$[5,255]$is denoted byHi_w^{LSTM}andHi_y^{BC}, respectively and also the steps per epochs from Dilated BiLSTM and Bayesian classifier in the range of $[5,50]$is signified asST_x^{LSTM}andSTz_z^{BC}, correspondingly. The accuracy measure is denoted asAr and it is estimated through Eq. (20).

$$Ar = \frac{T_r P + T_r N}{T_r P + T_r N + F_l P + F_l N}, \tag{3:20}$$

The termPnrepresents the precision and it is estimated via Eq. (21).

$$Pn = \frac{T_r P}{T_r P + F_l N} \tag{3:21}$$

The MCC measure is noted by $MCC$and it is illustrated in Eq. (22).

$$MCC = \frac{T_r P + T_r N - F_l P + F_l N}{\sqrt{\substack{(T_r P + F_l P)(T_r P + F_l N) \\ (T_r N + F_l P)(T_r N + F_l N)}}} \tag{3:22}$$

The FPR is evaluated through Eq. (23).

$$FPR = \frac{F_l P}{(T_r N + F_l P)} \quad (3:23)$$

The diagrammatic illustration of the proposed cyber-attack detection scheme in SCADA over ICS networks using SCEN is depicted in Fig. 3.4.

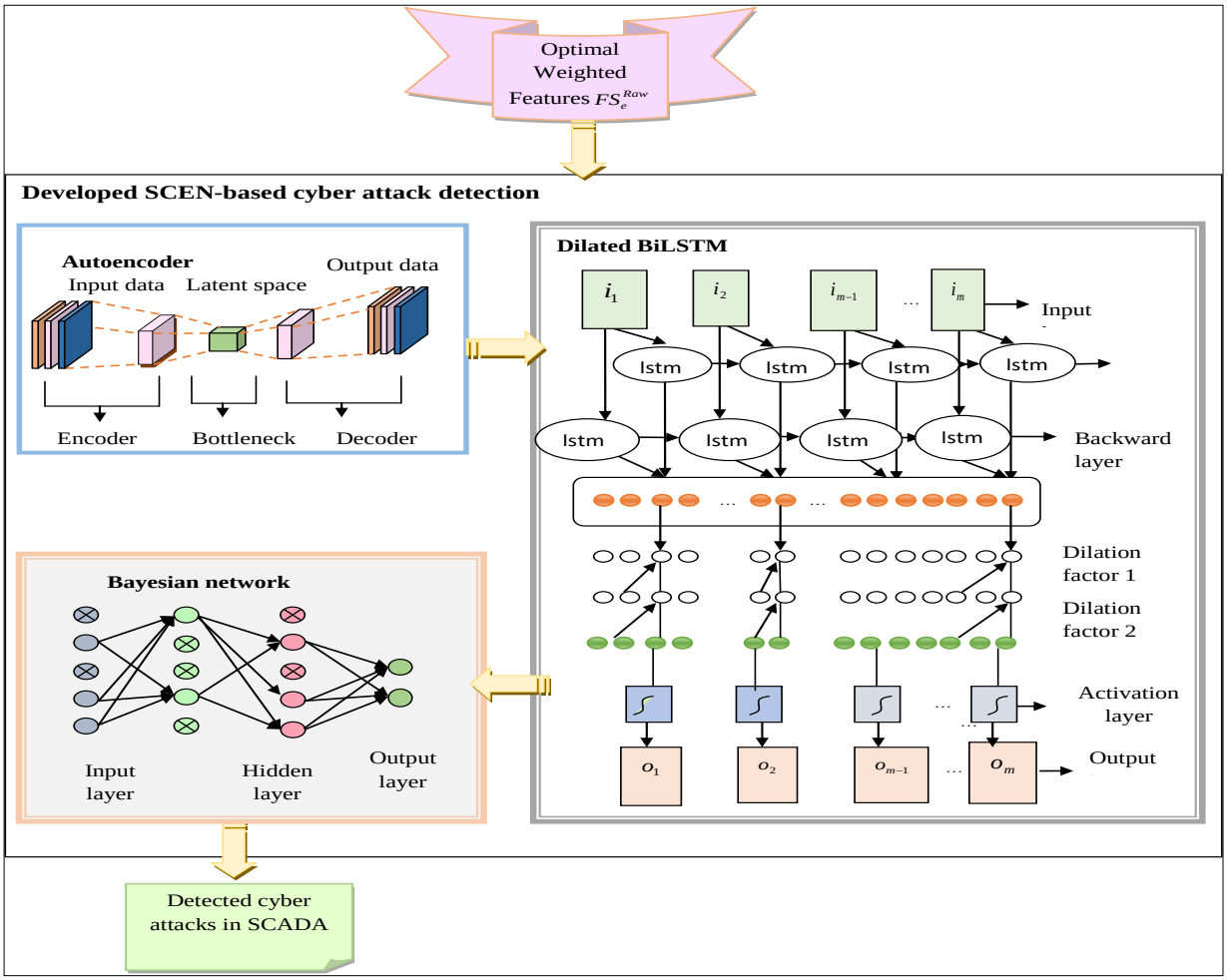

Figure 3.4: Schematic Depiction of Proposed Cyber Attack Detection Using SCEN.

4. RESULTS AND DISCUSSION

4.1 EXPERIMENTAL SETUP

The MATLAB 2020a software paradigm was used for the implementation of the proposed cyber-attack detection framework in SCADA systems. Experimental validation has been done to verify the detection efficiency of the proposed cyber-attack detection approach. To conduct the experimental analysis, the population count was set as 10 and the maximum count of iteration to be taken as 50. In addition, the chromosome length required for the implementation to be considered as 2*25. The traditional algorithms such as Tuna Swarm Algorithm (TSA) [27], Horse Herd Optimization [28], Geography Optimization (GEO) [29] and OOA [26] were considered for validating the detection performance in regard with various measures in the proposed scheme. The conventional attack detection models such as autoencoder [30], BiLSTM [31], Bayesian classifier [32] and Ensemble [33] networks were considered for the validation of performance to ensure the attack detection efficiency of the implemented scheme.

4.2 PERFORMANCE MEASURES

The positive measures as well as the negative measures, are used for validating the detection efficiency of the proposed cyber attack identification scheme in SCADA systems. The expression of these positive and negative measures is illustrated in the following Eqs.

$$Sensitivity = \frac{T_r P}{(T_r P + F_l N)} \tag{4:1}$$

$$Specificity = \frac{T_r N}{(T_r N + F_l P)} \tag{4:2}$$

$$F - score = 2 \times \frac{Pn \times Re\,call}{Pn + Re\,call} \tag{4:3}$$

$$NPV = \frac{T_r N}{(T_r N + F_l N)} \tag{4:4}$$

4.3 PERFORMANCE VALIDATION IN TERMS OF THE CONFUSION MATRIX

In the fig.4.1 and fig.4.2 gives the confusion matrix analysis of the suggested EOOA-SCEN-based cyber-attack detection approach in SCADA in regards with the predicted and actual label. This confusion matrix is used for analyzing the detection performance of the offered model while concerning with true positive and true negative observation measure. The accuracy over the detection of cyber-attacks is examined through this confusion matrix.

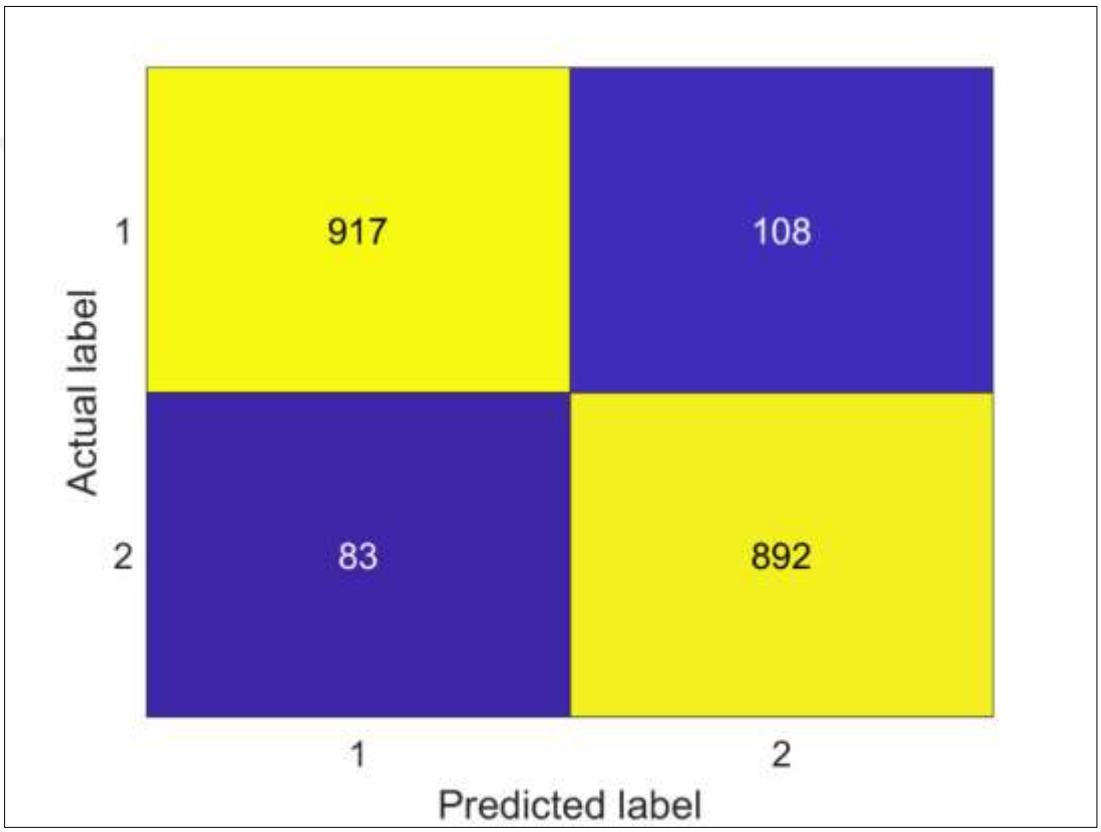

Figure 4.1: Confusion Matrix Examination On Proposed SCEN-based Cyber-Attack Detection Model Regarding for Dataset 1.

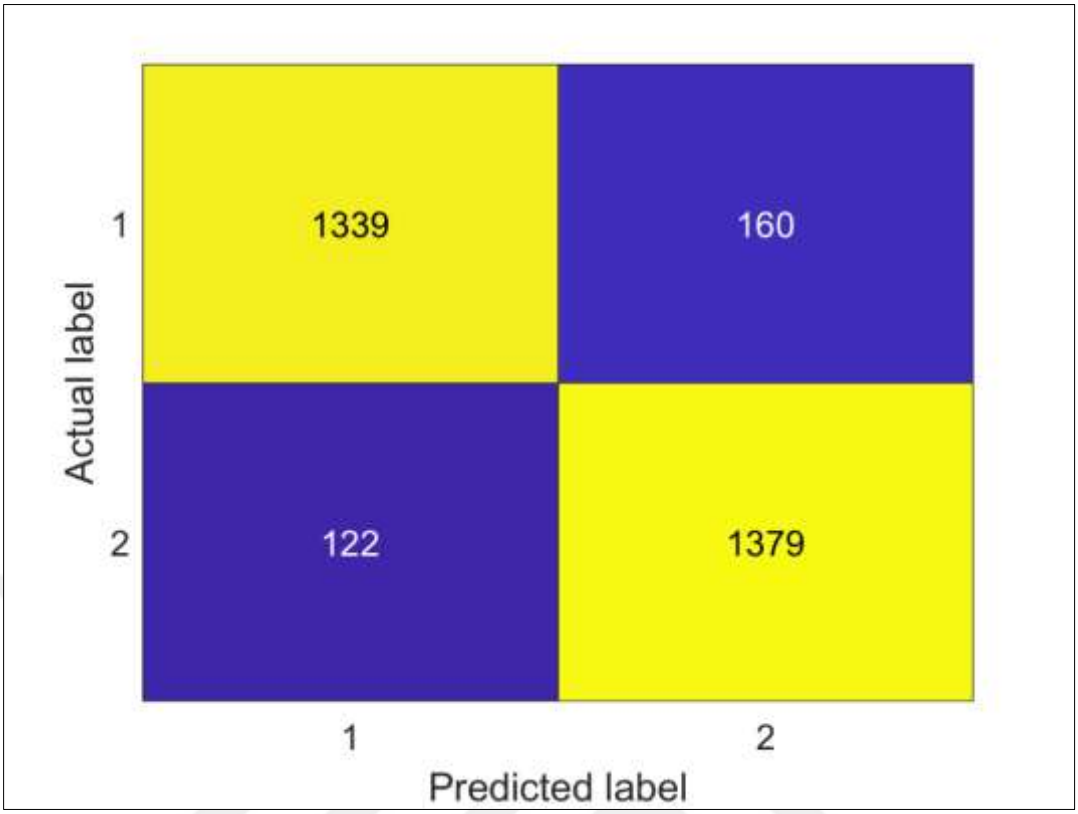

Figure 4.2: Confusion Matrix Examination on Proposed SCEN-based Cyber Attack Detection Model Regarding for Dataset2

4.4 CONVERGENCE EXAMINATION

Fig. 4.3 and fig 4.4 illustrates the convergence examination of the implemented cyber-attack detection model with respect to cost function among divergent algorithms. The iteration value is adjusted for analyzing the performance of the model in regard with a cost function. While analyzing the cost function, the effectiveness of the proposed cyber-attack detection scheme was high when compared to other algorithms. After the 30^{th} iteration, the cost function of the presented scheme produces more extensive outcomes than the traditional algorithms for both dataset 1 and dataset 2.

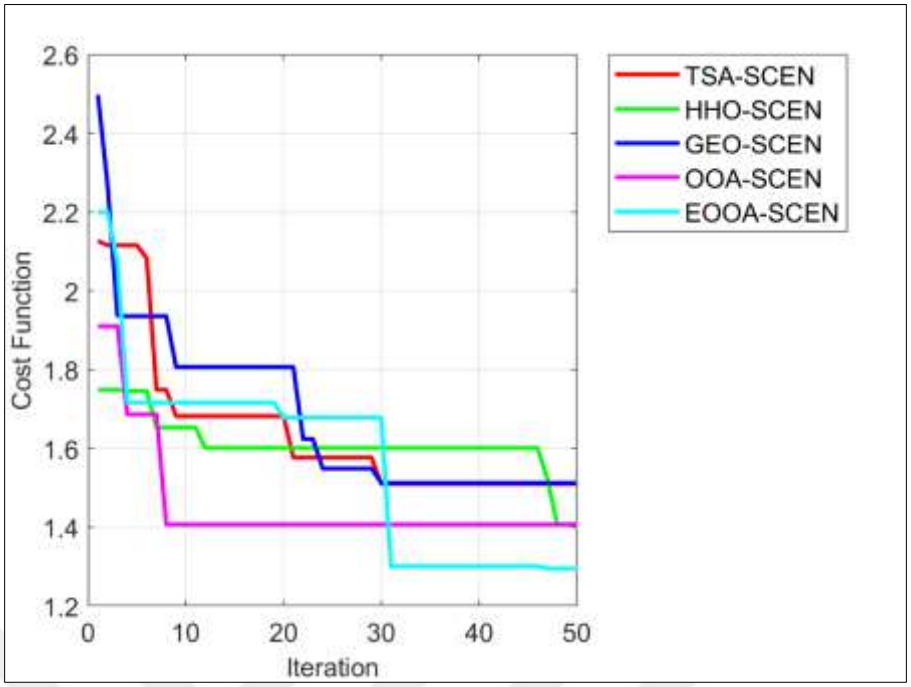

Figure 4.3: Cost Function Estimation of the Proposed SCEN-based Cyber Attack Detection Model According to Dataset 1.

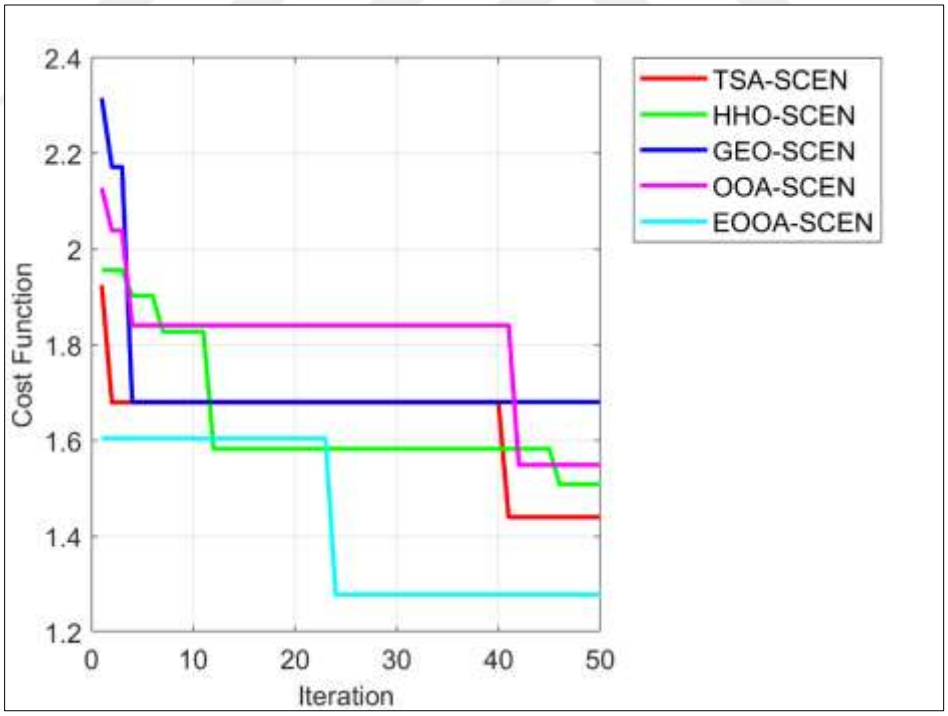

Figure 4.4: Cost Function Estimation Of The Proposed SCEN-based Cyber Attack Detection Model According to Dataset 2.

The conventional optimization strategies are considered for the analysis of performance

with respect to several validation metrics to validate the proposed cyber attack detection model. Fig. 4.5 depicts the performance validation among dataset 1 and Fig. 4.4 gives the performance validation with respect to dataset 2. The activation functions are considered here for giving the best validation outcome during the experiments. The NPV rate of the developed EOOA-SCEN-based cyber attack detection model is greater than 5.43%, 3.63%, 3.30%, and 2.64% with respect to the traditional algorithms like TSA-SCEN, HHO-SCEN, GEO-SCEN, and OOA-SCEN for considering dataset 1 at sigmoid activation function. All the performance measures are provided extensive outcomes when analyzed to the traditional algorithms for both dataset 1 provided extensive outcomes when analyzed to the traditional

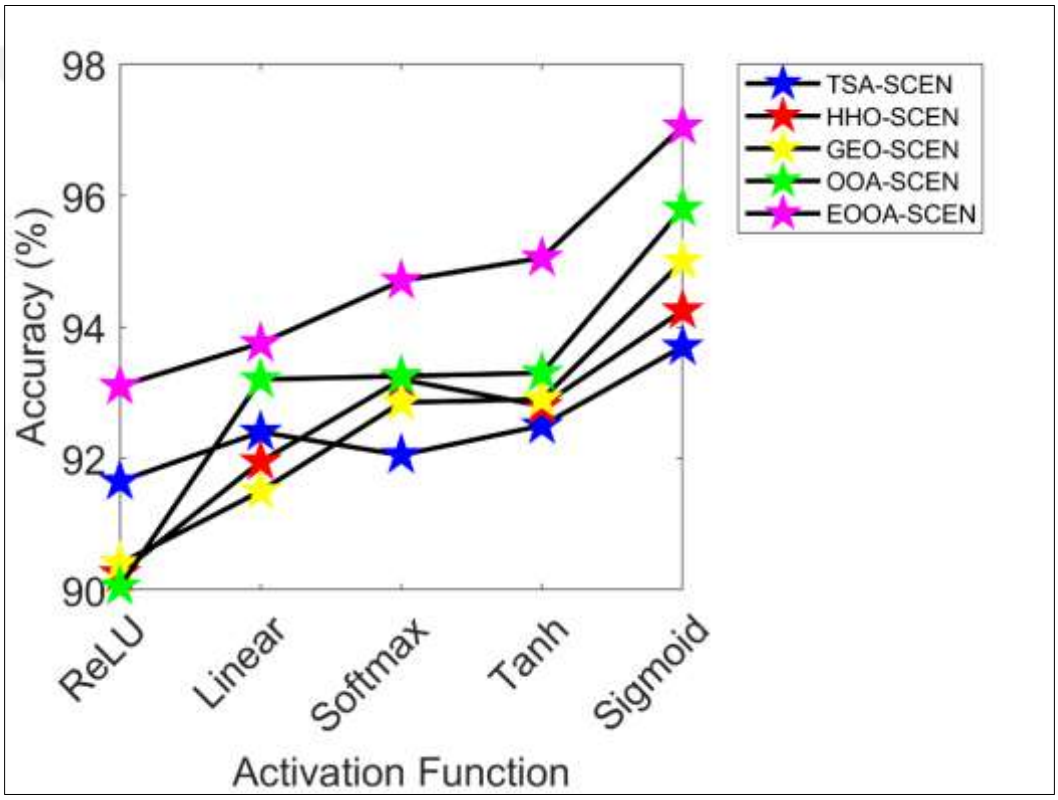

Figure 4.5: Detection Performance of the Implemented SCEN-Based Cyber Attack Detection Model Regarding (A) Accuracy For Dataset 1.

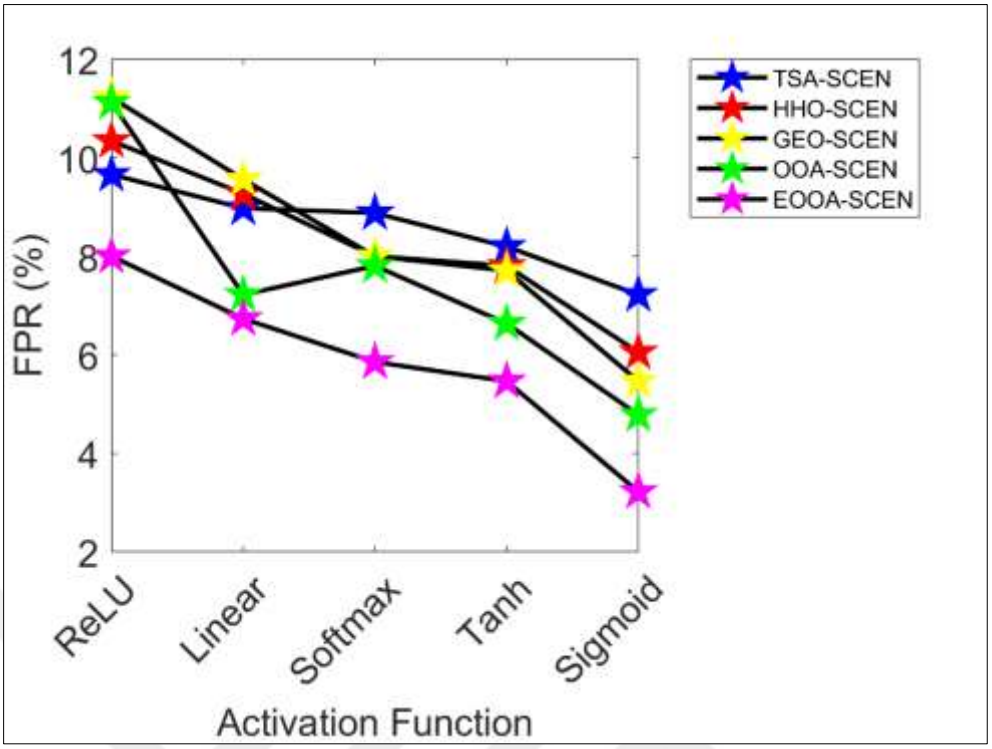

Figure 4.6: Detection Performance of The Implemented SCEN-Based Cyber Attack Detection Model Regarding FPR For Dataset 1.

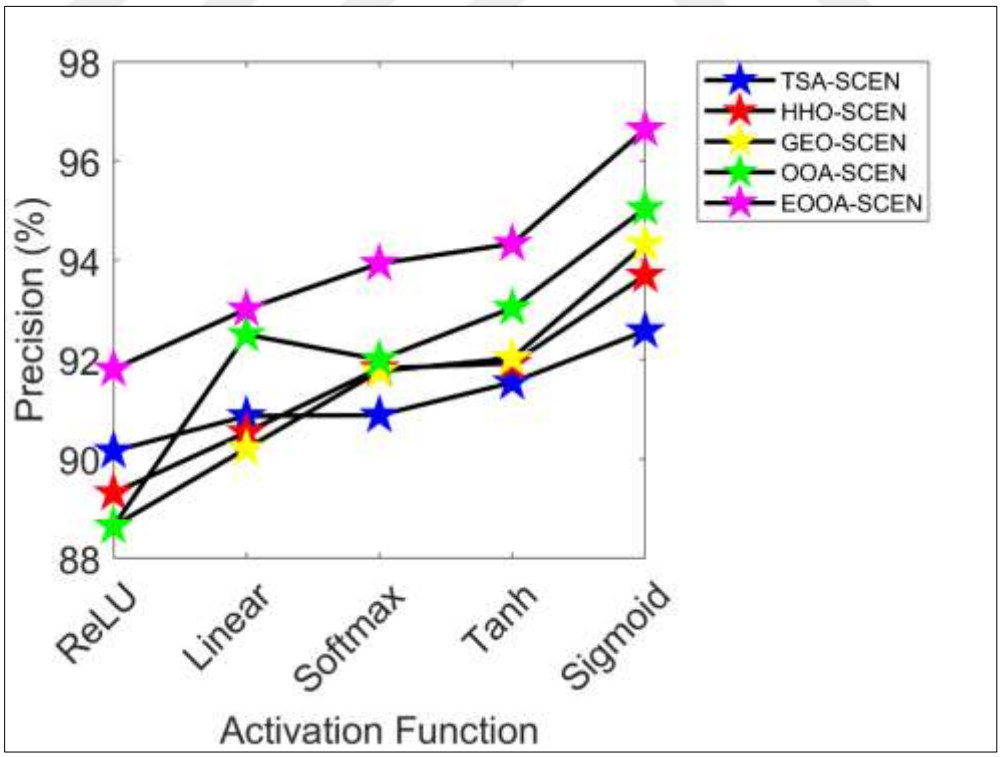

Figure 4.7: Detection Performance of the Implemented SCEN-based Cyber Attack Detection Model Regarding Percision for Dataset 1.

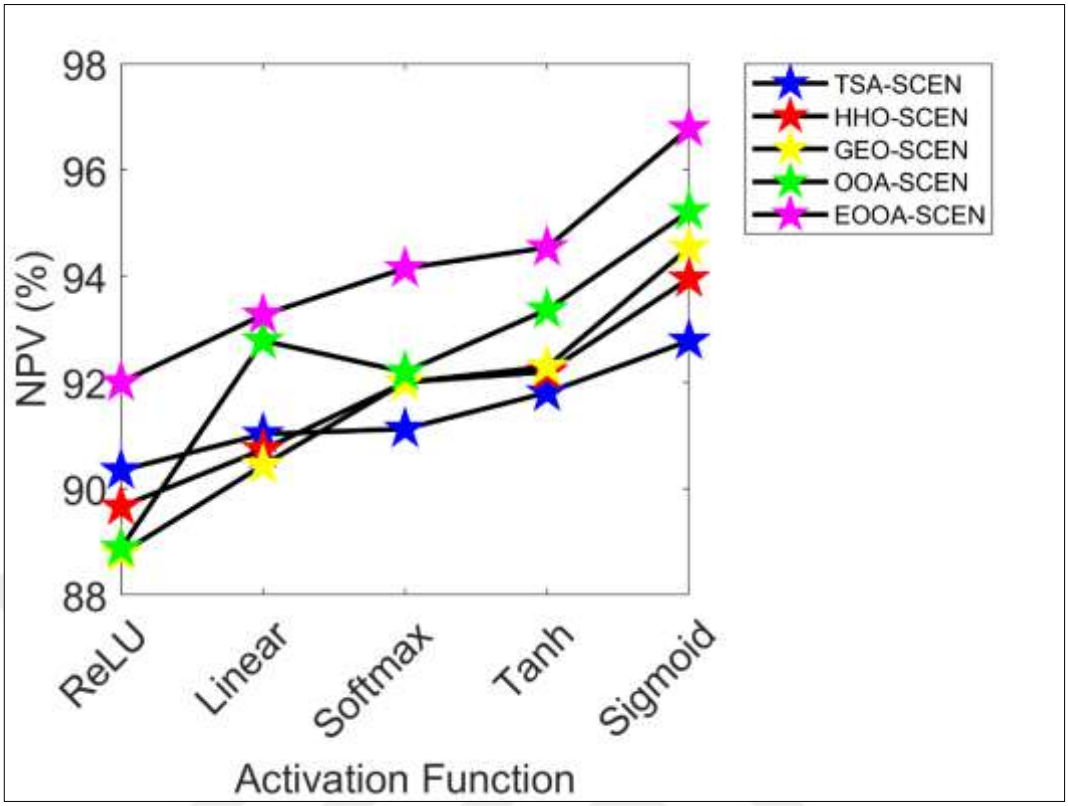

Figure 4.8: Detection Performance of the Implemented SCEN-Based Cyber Attack Detection Model Regarding NPV for Dataset 1.

All the performance measures show significant improvements over traditional algorithms for Dataset 2. The results indicate enhanced , Accuracy , FPR , Precision , NPV Comparative analysis highlights the superiority of the proposed method in datase1 and dataset 2. These findings validate the effectiveness of the approach in real-world applications.

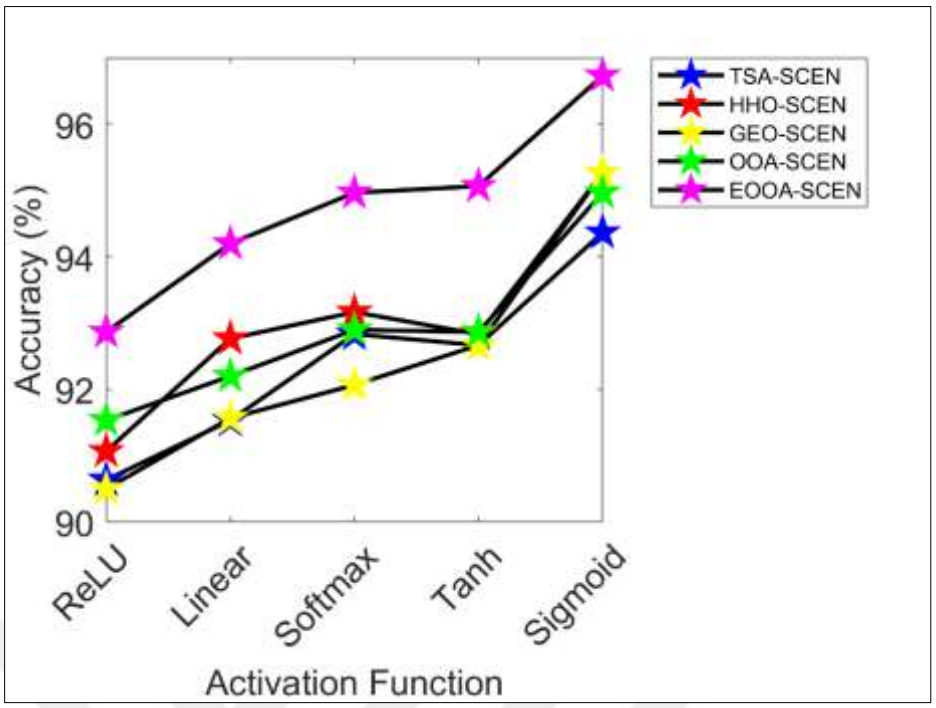

Figure 4.9: The Detection Performance of The Recommended SCEN-based Cyber Attack Detection Framework Regarding for Dataset 2.

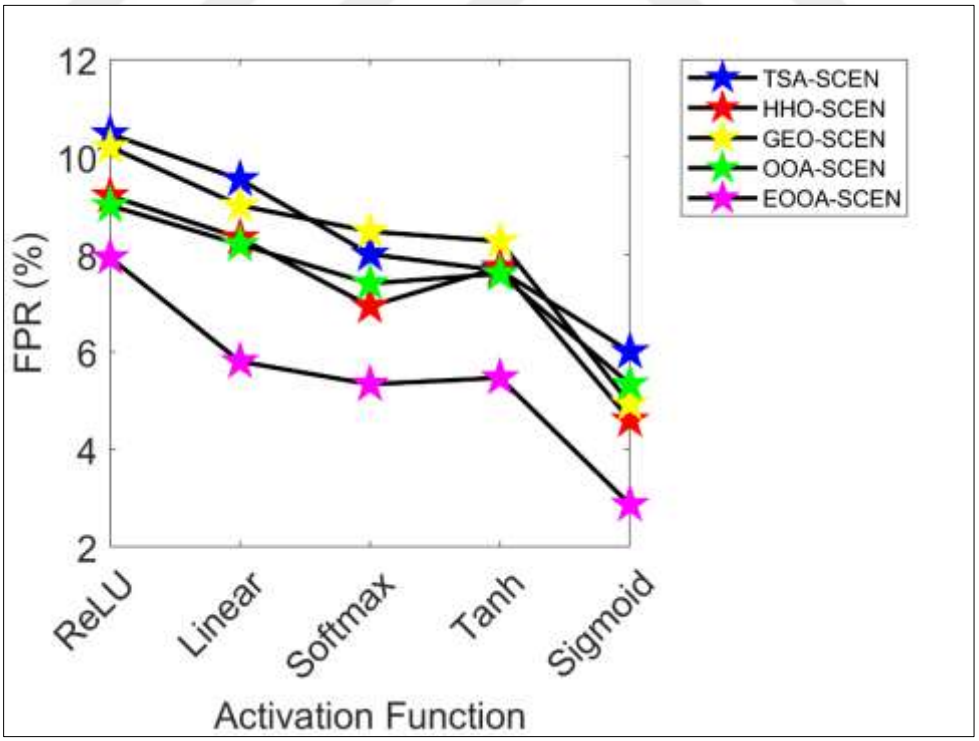

Figure 4.10: The Detection Performance of the Recommended SCEN-based Cyber Attack Detection Framework Regarding FPR for Dataset 2.

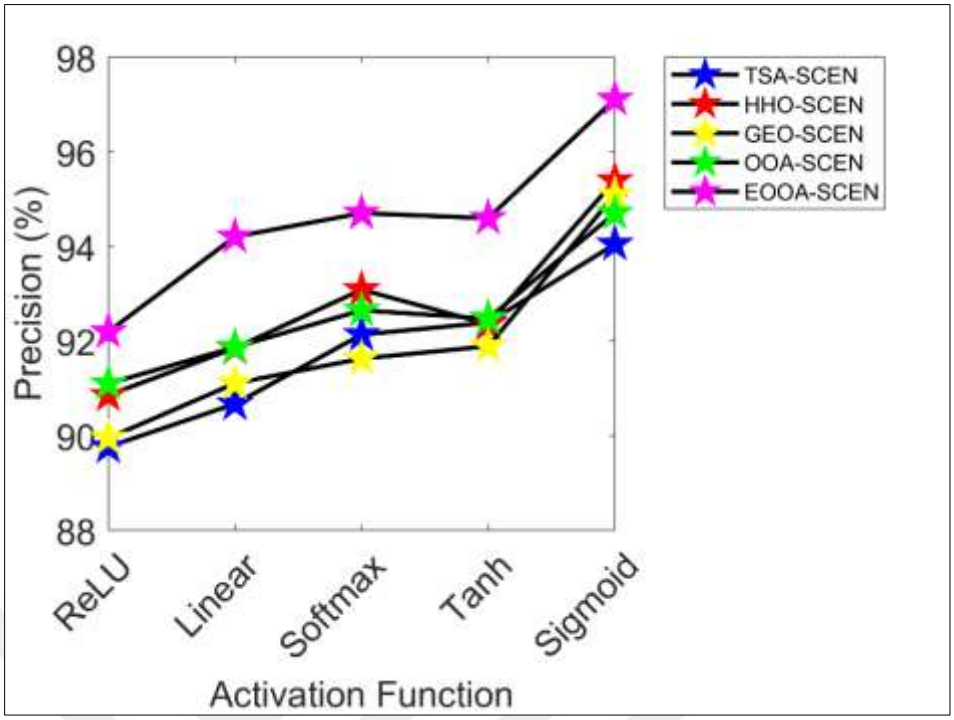

Figure 4.11: The Detection Performance of the Recommended SCEN-based Cyber Attack Detection Framework Regarding Precision for Dataset 2.

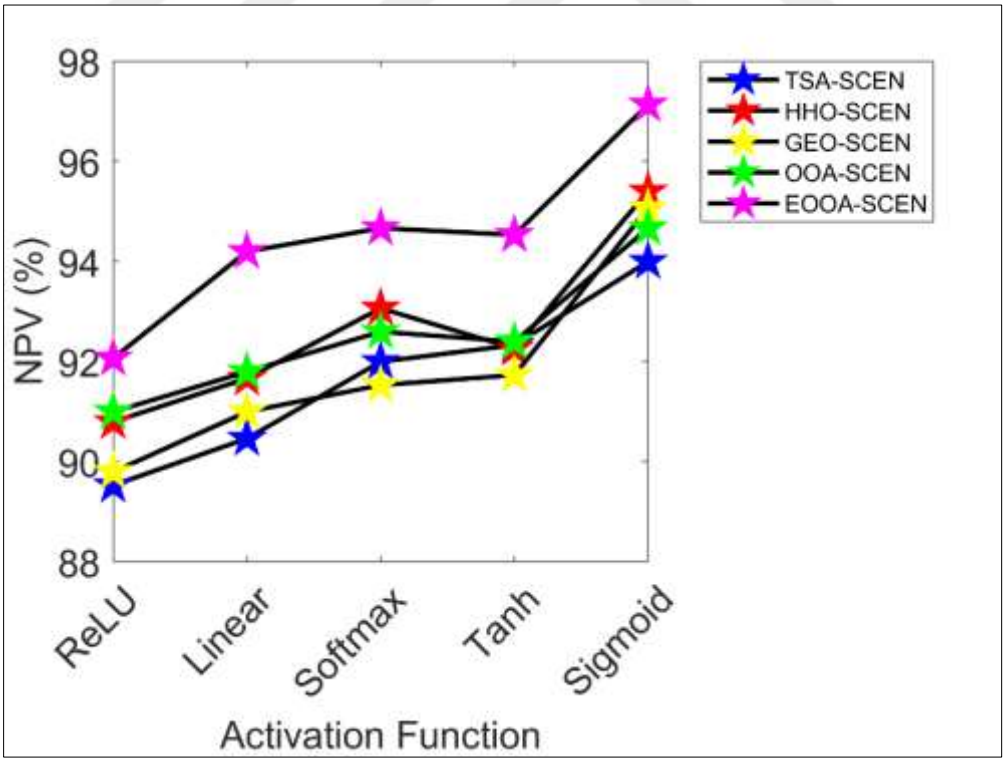

Figure 4.12: The Detection Performance of the Recommended SCEN-Based Cyber Attack Detection Framework Regarding NPV for Dataset 2.

4.5 ANALYSIS OVER BASELINE WORKS

Several baseline cyber attack detection models are taken for validating the efficiency of offered EOOA-SCEN-based cyber attack detection model among dataset 1 is given in Fig. 9 and dataset 2 is illustrated in Fig. 10. The precision of the proposed cyber attack detection scheme is highly improved with 9.41%, 10.71%, 8.13%, and 6.89% than autoencoder, Bi-LSTM, Bayesian, Ensemble and EOOA-SCEN for dataset 1 at softmax activation function. The cyber attack detection performance is higher than the previously used models in regards to accuracy, FPR, NPV and precision.

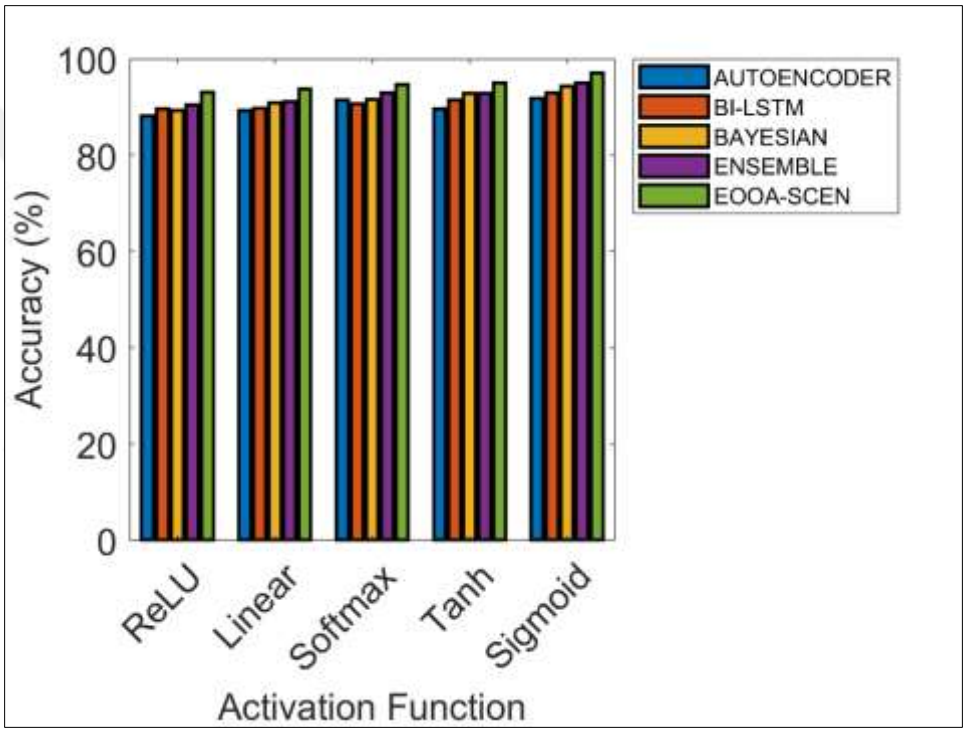

Figure 4.13: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding (a) Accuracy (b) FPR (b) Precision (b) NPV for Dataset 1.

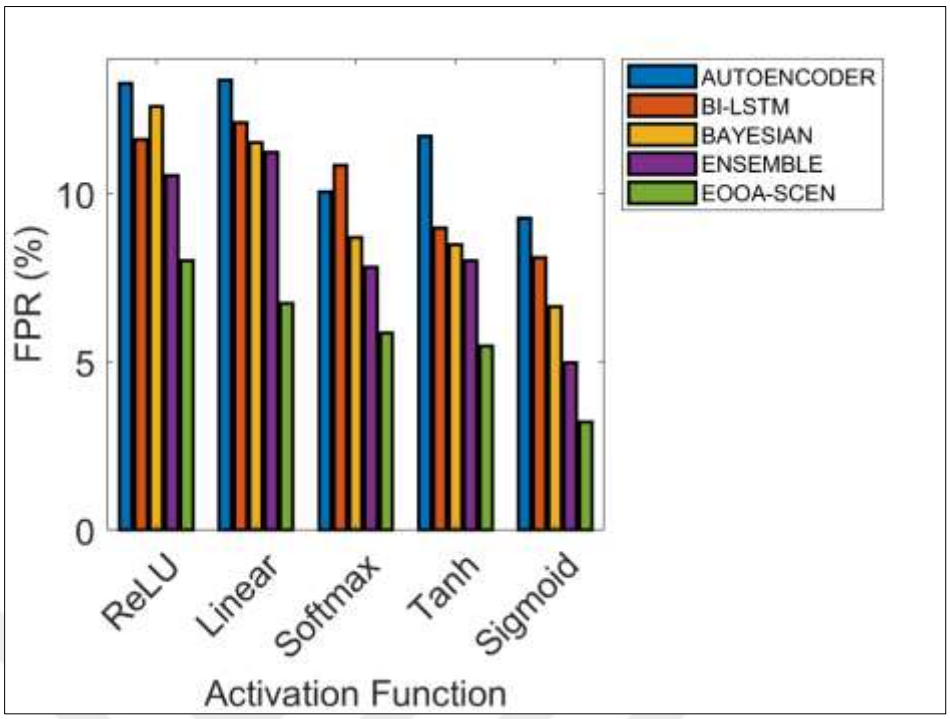

Figure 4.14: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding FPR.

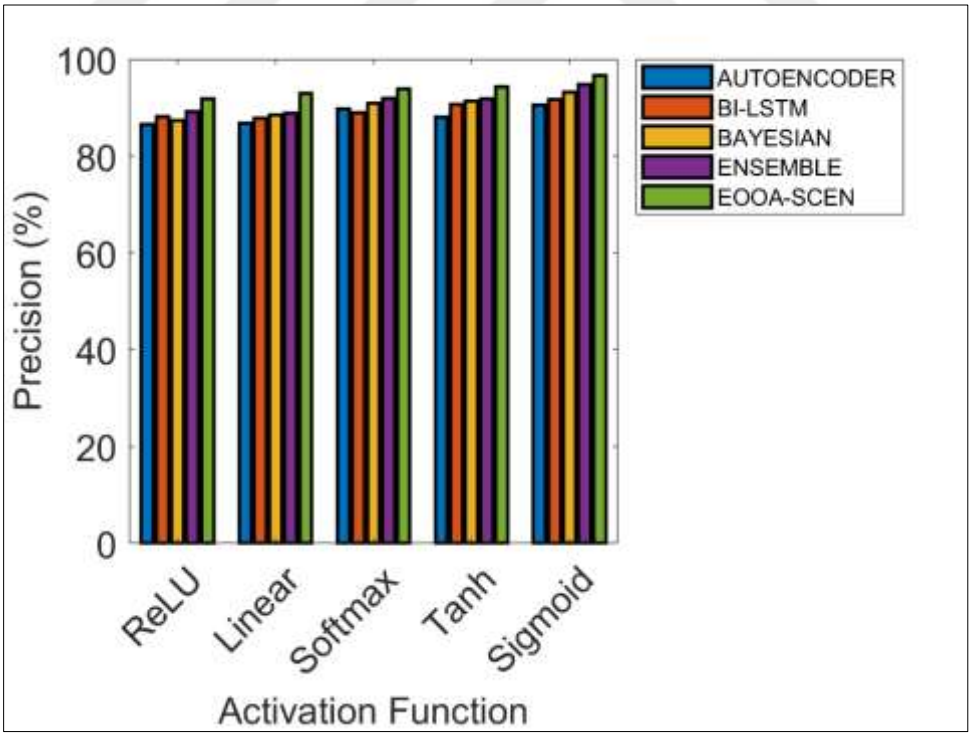

Figure 4.15: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding Precision for Dataset 1.

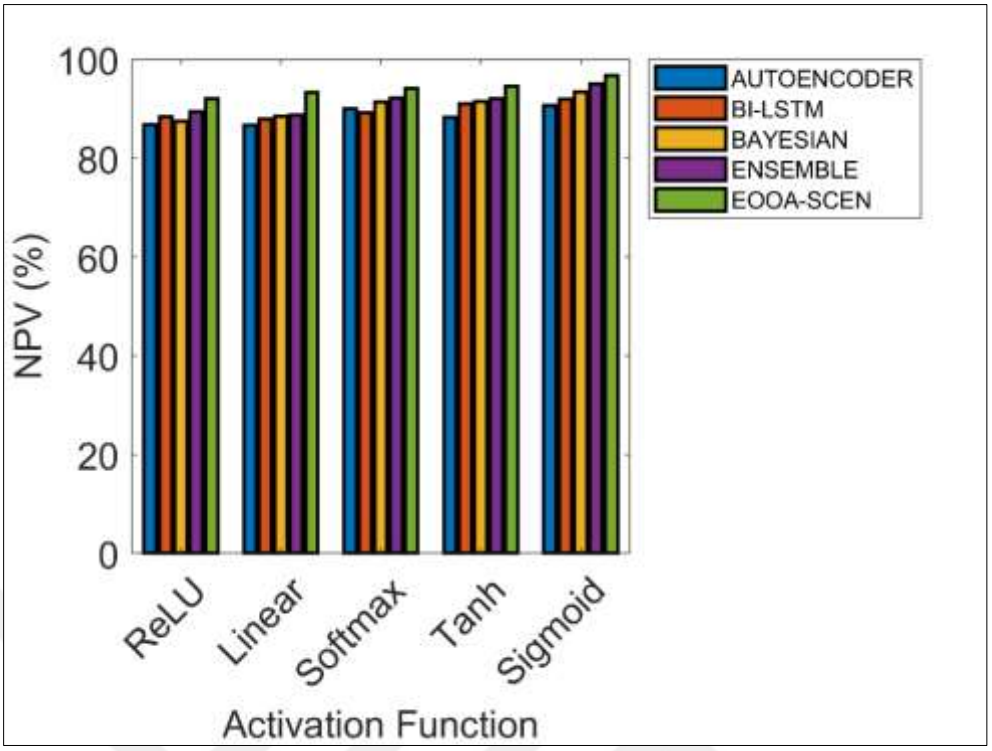

Figure 4.16: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding NPV for Dataset 1.

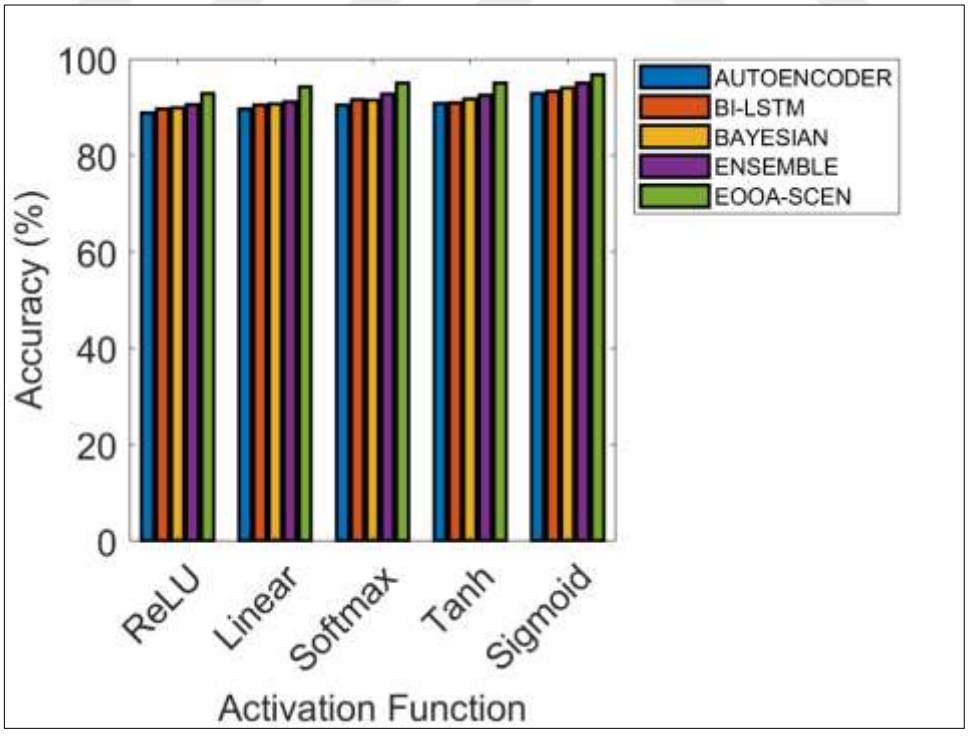

Figure 4.17: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding Accuracy for Dataset 2.

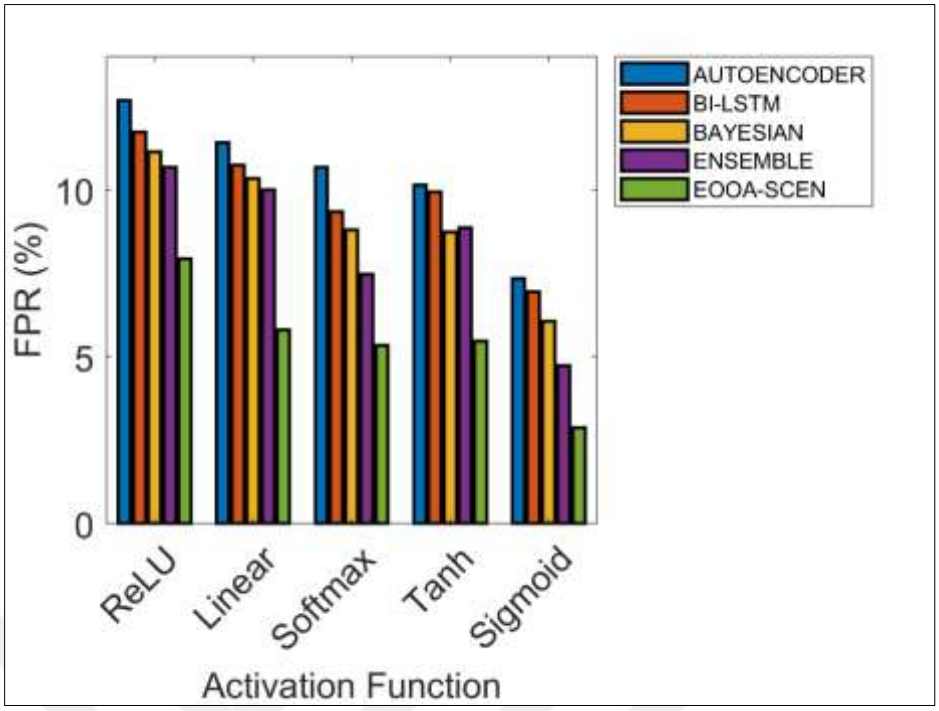

Figure 4.18: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding FPR for Dataset 2.

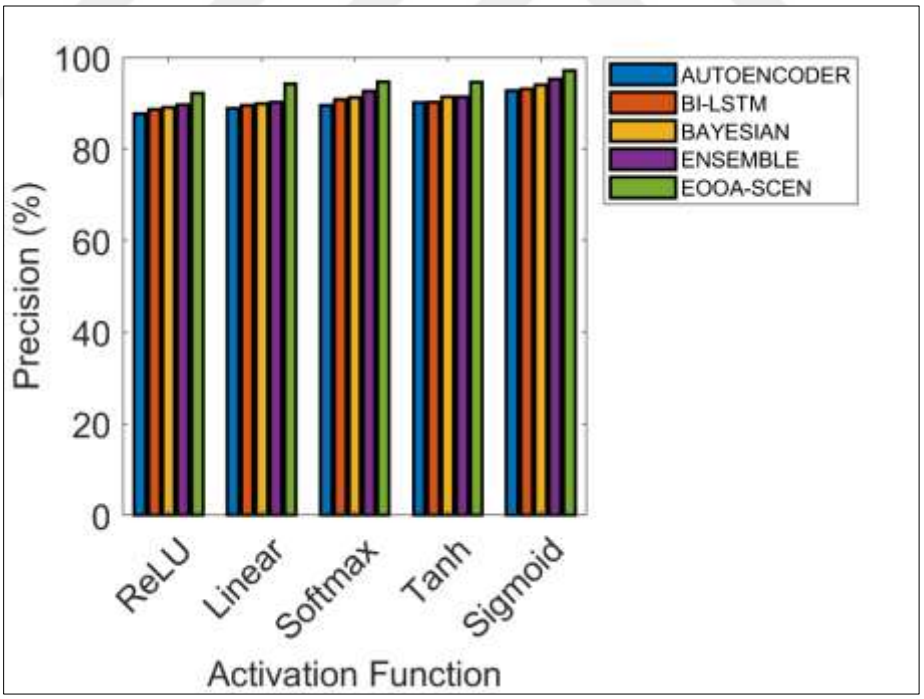

Figure 4.19: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding Percision for Dataset 2.

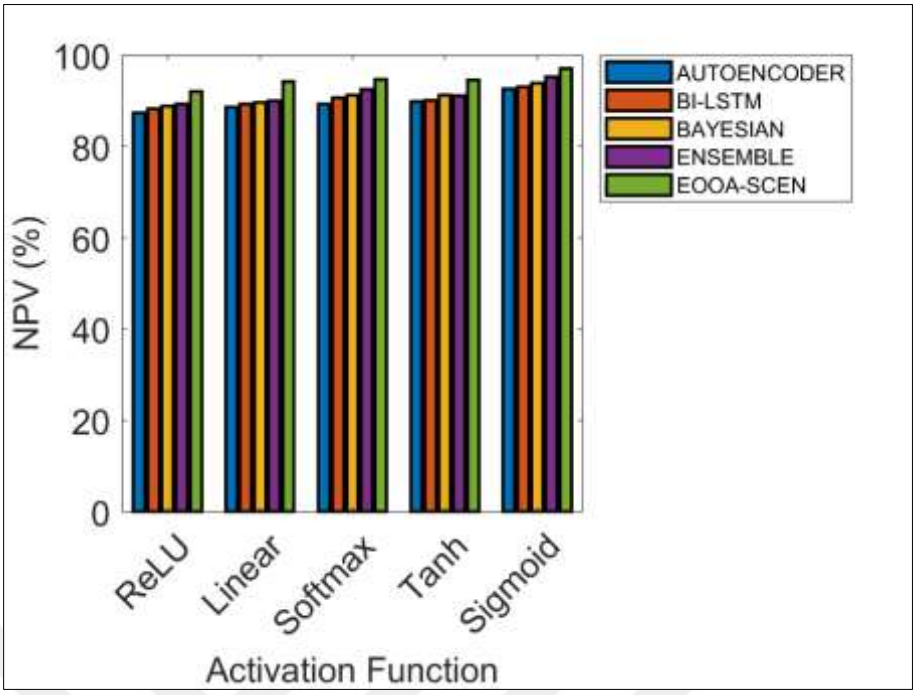

Figure 4.20: Detection Performance of the Offered SCEN-based Cyber Attack Detection Model Regarding NPV for Dataset 2.

4.6 PERFORMANCE VERIFICATION AMONG ALGORITHMS AND PREVIOUS TECHNIQUES

Below Table 4.1 and Table 4.2 describe the efficiency validation of the offered cyber attack detection scheme through divergent algorithms and classifiers. The positive and negative metrics are considered for validating the effectiveness and the results were demonstrated that the proposed scheme attained with higher MCC of 5.33%, 3.24%, 3.24%, and 3.93% with respect to the traditional algorithms like TSA-SCEN, HHO-SCEN, GEO-SCEN, and OOA-SCEN for considering dataset 2 from Table III. Dataset 1 also provides efficient outcomes for all performance metrics when compared to the state-of-the-art.

Table 4.1: Validation Of Performance On Developed Cyber Attack Detection Model Among Various Algorithms.

Metrics	TSA-SCEN [27]	HHO-SCEN [28]	GEO-SCEN [29]	OOA-SCEN [26]	EOOA-SCEN
Dataset 1					
Accuracy	93.7	94.25	95	95.8	97.05
Sensitivity	94.667	94.564	95.487	96.41	97.333
Specificity	92.78	93.951	94.537	95.22	96.78
Precision	92.578	93.699	94.326	95.046	96.64
FPR	7.2195	6.0488	5.4634	4.7805	3.2195
FNR	5.3333	5.4359	4.5128	3.5897	2.6667
NPV	92.78	93.951	94.537	95.22	96.78
FDR	7.4223	6.3008	5.6738	4.9545	3.3605
F1-Score	93.611	94.13	94.903	95.723	96.985
MCC	87.42	88.499	90.003	91.607	94.1
Dataset 2					
Accuracy	94.367	95.267	95.267	94.967	96.733
Sensitivity	94.737	95.137	95.47	95.27	96.336
Specificity	93.996	95.397	95.063	94.663	97.131
Precision	94.048	95.391	95.09	94.702	97.112
FPR	6.004	4.6031	4.9366	5.3369	2.8686
FNR	5.2632	4.8634	4.5303	4.7302	3.6642
NPV	93.996	95.397	95.063	94.663	97.131
FDR	5.9524	4.6092	4.9104	5.298	2.8878
F1-Score	94.391	95.264	95.279	94.985	96.722
MCC	88.736	90.534	90.534	89.935	93.47

Table 4.2: Validation of Performance on Developed Cyber Attack Detection Model Among Various Techniques.

Metrics	Autoencoder [30]	Bi-LSTM [31]	Bayesian [32]	Ensemble [33]	EOOA-SCEN
Dataset 1					
Accuracy	91.85	93	94.3	95.05	97.05
Sensitivity	93.026	94.154	95.282	95.077	97.333
Specificity	90.732	91.902	93.366	95.024	96.78
Precision	90.519	91.708	93.18	94.785	96.64
FPR	9.2683	8.0976	6.6341	4.9756	3.2195
FNR	6.9744	5.8462	4.7179	4.9231	2.6667
NPV	90.732	91.902	93.366	95.024	96.78
FDR	9.481	8.2917	6.8205	5.2147	3.3605
F1-Score	91.755	92.915	94.219	94.931	96.985
MCC	83.731	86.029	88.621	90.095	94.1
Dataset 2					
Accuracy	92.9	93.267	94.033	94.967	96.733
Sensitivity	93.138	93.471	94.137	94.67	96.336
Specificity	92.662	93.062	93.929	95.264	97.131
Precision	92.706	93.099	93.949	95.241	97.112
FPR	7.3382	6.938	6.0707	4.7365	2.8686
FNR	6.8621	6.529	5.8628	5.3298	3.6642
NPV	92.662	93.062	93.929	95.264	97.131
FDR	7.2944	6.9011	6.0505	4.7587	2.8878
F1-Score	92.921	93.285	94.043	94.955	96.722
MCC	85.801	86.534	88.067	89.935	93.47

4.7 STATISTICAL ANALYSIS ON HEURISTIC ALGORITHMS

The performance of the proposed cyber attack detection process among various algorithms is given in Table 4.3 The statistical analysis provides better decision-making ability rather than other analyses. The accurate analysis outcome was obtained by using statistical measures. By using this statistical analysis, best decision making ability is obtained during the detection of cyber attacks in SCADA systems. From the analysis of statistics, the efficacy of the proposed model is superior to the conventional algorithms.

Table 4.3: Statistical Evaluation on Developed Cyber Attack Detection Scheme Among Various Heuristic Algorithms.

Performance Measures	TSA-SCEN [27]	HHO-SCEN [28]	GEO-SCEN [29]	OOA-SCEN [30]	EOOA-SCEN
Dataset 1					
Best	1.5101	1.4079	1.5127	1.4072	1.2949
Worst	2.1268	1.7487	2.4979	1.9105	2.2
Mean	1.6452	1.6108	1.6837	1.4597	1.568
Median	1.577	1.6012	1.5493	1.4072	1.6785
Standard Deviation	0.1902	0.072188	0.21725	0.13809	0.2466
Dataset 2					
Best	1.44	1.5086	1.6807	1.5489	1.2781
Worst	1.9252	1.9557	2.3157	2.128	1.6041
Mean	1.6367	1.6413	1.713	1.8019	1.428
Median	1.6797	1.5827	1.6807	1.8408	1.2781
Standard Deviation	0.10521	0.13397	0.13041	0.13187	0.16412

5. RESULTS AND DISCUSSION

5.1 CONCLUSION

A new cyber attack detection model has been implemented to detect unwanted cyber attack vulnerabilities in SCADA systems. The information hacking due to the presence of malicious activities was effectively identified with the help of the developed cyber attack detection system using serial cascaded ensemble learning. The data from wind turbines has been collected from various online sources. The collected data were fed to the optimal weighted feature fusion stage, where the weight and feature tuning has carried out with the help of the proposed EOOA. Then, the weighted features have given to the SCEN for detecting the cyber attacks, where the autoencoder, Dilated BiLSTM and Bayesian classifier were serially connected to provide an efficient detection outcome. The parameters from these networks have been optimized through the developed EOOA for maximizing the accuracy, precision and MCC. The experimental outcome was validated with the traditional models, where the proposed model gained improved accuracy of 4.12%, 3.71%, 2.87%, and 1.85% than autoencoder, Bi-LSTM, Bayesian, Ensemble and EOOA-SCEN for dataset 3 in Table IV. Better detection outcomes were obtained by using the developed SCEN when compared to the conventional attack detection schemes.

5.2 FUTURE WORK

The proposed cyber attack detection model has demonstrated significant improvements in identifying vulnerabilities within SCADA systems. However, further research can enhance its efficiency and adaptability. Future work will focus on the following directions:

a. Real-Time Implementation: Deploying the developed model in real-world SCADA environments to evaluate its performance in real-time scenarios.

b. Scalability and Adaptability: Extending the model to handle large-scale and diverse cyber-physical systems beyond wind turbine data.

c. Integration with Threat Intelligence: Incorporating real-time threat intelligence feeds to enhance the model’s ability to detect emerging cyber threats.

d. Lightweight Model Optimization: Reducing computational complexity to ensure faster detection and lower resource consumption for edge and IoT devices.

e. Adversarial Attack Resistance: Strengthening the model against adversarial attacks by integrating advanced security mechanisms and robust training techniques.

f. Multi-Modal Data Fusion: Enhancing detection accuracy by integrating diverse data sources, including network traffic, system logs, and sensor data.

g. By addressing these areas, the proposed model can further improve cyber attack detection, ensuring enhanced security for critical infrastructure systems.

REFRENCES

[1] D. Li, N. Gebraeel and K. Paynabar, "Detection and Differentiation of Replay Attack and Equipment Faults in SCADA Systems," IEEE Transactions on Automation Science and Engineering, vol. 18, no. 4, pp. 1626-1639, October 2021.

[2] M. M. Hassan, A. Gumaei, S. Huda and A. Almogren, "Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154-6162, September 2020.

[3] P. Priyanga S, K. Krithivasan, P. S and S. Sriram V S, "Detection of Cyberattacks in Industrial Control Systems Using Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN)," IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4394-4404, July-August 2020.

[4] J. Appiah-Kubi and C. -C. Liu, "Decentralized Intrusion Prevention (DIP) Against Co-Ordinated Cyberattacks on Distribution Automation Systems," IEEE Open Access Journal of Power and Energy, vol. 7, pp. 389-402, 2020.

[5] S. Siamak, M. Dehghani and M. Mohammadi, "Dynamic GPS Spoofing Attack Detection, Localization, and Measurement Correction Exploiting PMU and SCADA," IEEE Systems Journal, vol. 15, no. 2, pp. 2531-2540, June 2021.

[6] F. Milano and A. Gómez-Expósito, "Detection of Cyber-Attacks of Power Systems Through Benford's Law," IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2741-2744, May 2021.

[7] S. Nath, I. Akingeneye, J. Wu and Z. Han, "Quickest Detection of False Data Injection Attacks in Smart Grid with Dynamic Models," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 1, pp. 1292-1302, February 2022.

[8] C. -W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4405-4425, September 2018.

[9] S. Chakrabarty and B. Sikdar, "Detection of Malicious Command Injection Attacks on Phase Shifter Control in Power Systems," IEEE Transactions on Power Systems, vol. 36, no. 1, pp. 271-280, January 2021.

[10] R. Zhu, C. -C. Liu, J. Hong and J. Wang, "Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations," IEEE Access, vol. 9, pp. 1240-1249, 2021.

[11] Lu, Kang-Di, Zheng-Guang Wu, and Tingwen Huang, "Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems." IEEE/ASME Transactions on Mechatronics, vol. 28, no. 2, pp. 1137-1148, 2022.

[12] Abdu Gumaei, Mohammad Mehedi Hassan, Shamsul Huda, Md. Rafiul Hassan, David Camacho, Javier Del Ser, and Giancarlo Fortino, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids," Applied Soft Computing, vol. 96, pp. 106658, November 2020.

[13] Meir Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," Computers & Security, vol. 84, pp. 225-238, July 2019.

[14] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, H. F. Wang, "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," IEEE Transactions on Power Delivery, vol. 29, no. 3, pp. 1092-1102, June 2014.

[15] J. Qian, X. Du, B. Chen, B. Qu, K. Zeng and J. Liu, "Cyber-Physical Integrated Intrusion Detection Scheme in SCADA System of Process Manufacturing Industry," IEEE Access, vol. 8, pp. 147471-147481, 2020.

[16] M. Ismail, M. F. Shaaban, M. Naidu and E. Serpedin, "Deep Learning Detection of Electricity Theft Cyber-Attacks in Renewable Distributed Generation," IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3428-3437, July 2020.

[17] Amit Shlomo, Meir Kalech, and Robert Moskovitch, "Temporal pattern-based malicious activity detection in SCADA systems," Computers & Security, vol. 102, pp. 102153, March 2021.

[18] Lu, Kang-Di, Guo-Qiang Zeng, Xizhao Luo, Jian Weng, Weiqi Luo, and Yongdong Wu. "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system." IEEE Transactions on Industrial Informatics 17, no. 11 (2021): 7618-7627.

[19] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Gradient Boosting Feature Selection With Machine Learning Classifiers for Intrusion Detection on Power Grids," IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 1104-1116, March 2021.

[20] SudhakarSengan, Subramaniyaswamy V, Indragandhi V, PriyaVelayutham, and Logesh Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," Computers & Electrical Engineering, vol. 93, pp. 107211, July 2021.

[21] M. R. Habibi, H. R. Baghaee, T. Dragičević and F. Blaabjerg, "Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural Networks," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 5, pp. 5294-5310, October 2021.

[22] S. Y. Diaba, M. Shafie-Khah and M. Elmusrati, "Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms," IEEE Access, vol. 11, pp. 18660-18672, 2023.

[23] HathalSalamahAlwageed, "Detection of cyber attacks in smart grids using SVM-boosted machine learning models," Service Oriented Computing and Applications, vol. 16, pp. 313–326, 2022.

[24] P. Nader, P. Honeine and P. Beauseroy, " lp -norms in One-Class Classification for Intrusion Detection in SCADA Systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2308-2317, Novomber 2014.

[25] F. Khan, R. Alturki, M. A. Rahman, S. Mastorakis, I. Razzak and S. T. Shah, "Trustworthy and Reliable Deep-Learning-Based Cyberattack Detection in Industrial IoT," IEEE

[26] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.

[27] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, 2010.

[28] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[29] S. Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," *IEEE Industrial Electronics Magazine*, vol. 6, no. 4, pp. 18–21, 2011.

[30] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

[31] S. K. Lakshmanan and K. Sankaranarayanan, "Machine learning approaches for SCADA intrusion detection systems: A survey," *Computers & Security*, vol. 111, 102490, 2021.

[32] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.

[33] S. Mirjalili, "Genetic algorithm," in *Evolutionary Algorithms and Neural Networks*, Springer, 2019, pp. 43–55.

[34] M. A. Ewees, M. Abd Elaziz, and A. H. Elsheikh, "Osprey Optimization Algorithm: A novel nature-inspired metaheuristic approach for engineering optimization problems," *Expert Systems with Applications*, vol. 183, 115352, 2021.

[35] H. He and E. A. Garcia, "Learning from imbalanced data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263–1284, 2009.

[36] Z.-H. Zhou, *Ensemble Methods: Foundations and Algorithms*, CRC Press, 2012.

[37] M. Abdar et al., “A review of ensemble learning for network intrusion detection systems,” *Applied Soft Computing*, vol. 99, 106744, 2021.

[38] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber–physical systems security—A survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[39] E. Byres, J. Lowe, "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems," *Proc. of the VDE Kongress*, 2004.

[40] R. Heady et al., “The Architecture of a Network Level Intrusion Detection System,” *Technical Report*, University of New Mexico, 1990.

[41] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Elsevier, 2014.

[42] M. Cheminod, L. Durante, and A. Valenzano, “Review of Security Issues in Industrial Networks,” *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

[43] S. M. Amin, “Challenges in Reliability, Security, Efficiency, and Resilience of Energy Infrastructure: Toward Smart Self-Healing Electric Power Grid,” *IEEE Power and Energy Society General Meeting*, 2011.

[44] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–Physical System Security for the Electric Power Grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[45] A. Nicholson et al., “SCADA Security in the Light of Cyber–Warfare,” *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.

[46] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, 2010.

[47] A. Cárdenas, S. Amin, and S. Sastry, “Secure Control: Towards Survivable Cyber–Physical Systems,” *Proc. of the 28th International Conference on Distributed Computing Systems,* 2008.

[48] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber–Physical Systems Security—A Survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[49] ICS-CERT, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” *Department of Homeland Security*, 2016.

[50] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[51] M. Krotofil and D. Gollmann, “Industrial Control Systems Security: What Is Happening?” *IEEE Security & Privacy*, vol. 12, no. 6, pp. 75–79, 2014.

[52] Y. Cherdantseva et al., “A Review of Cyber Security Risk Assessment Methods for SCADA Systems,” *Computers & Security*, vol. 56, pp. 1–27, 2016.