HBSCPG: Design of a Hybrid Bioinspired Model for Optimization of existing Security & Control Parameters of Cyber-Physical Smart Grids

Megha Sanjay Wankhade, Suhasini Vijaykumar kottur

ABSTRACT-Smart Grids are Cyber-Physical deployments that integrate distribution and billing solutions. Because of this, distribution agencies and consumers communicate frequently. Internal and external attackers can tamper with these deployments, causing spoofing, tampering, and distribution-based attacks. Existing attack detection and mitigation models that counter load-drop and access control attacks are either complex or computationally inefficient, limiting their real-time applicability. This text proposes a bioinspired hybrid model to optimize Cyber-Physical smart grid security and control parameters. The suggested model gathers large-scale record sets from various grids to identify attack types. This analysis is optimized using a hybrid Grey Wolf Optimizer and Teacher Learning based Optimizer (GWTLbO) Model that assigns contextual weights to security & control parameter sets. This intelligent assignment improves attack mitigation accuracy by 9.5%, control efficiency by 4.5%, and control delay by 10.4% compared to existing models. Flash Image Manipulation, Zero-day attacks, Meter Bypass, and Buffer-level attacks were tested. This means better device-level control and grid security.

Index Terms: Smart Grid, Security, Faults, GWO, TLbO, Bioinspired, Optimization, Scenarios

I. INTRODUCTION

Conventional electrical distribution systems distribute electrical power produced at a centralized electrical plant by decreasing electrical energy levels until it reaches the final users and then increasing voltage levels until the full amount of energy is delivered. This procedure is repeated until the distribution of electrical energy is complete [1, 2, 3]. However, this particular electrical grid has many significant flaws, such as its inability to integrate various production sources (including renewable energy), huge expenses as well as a protracted demand response period, elevated carbon emissions, and frequent power failure. Moreover, it cannot integrate various production sources (including green energy). In 2004, professionals at Berkeley National Laboratory conducted extensive research processes and concluded that electricity disruptions cost the US economy about $80 billion annually. Other estimates put the yearly charge at $150 billion and employ Anonymous Signature-Based Authenticated Key Exchange (ASB AKE) and belief propagation techniques [4,5,6].

It is glaringly obvious that our current electrical infrastructure is woefully inadequate to solve the problems we face. By enabling the integration of new power sources (such as renewable, wind, and solar energy), providing repair capabilities when breakdowns occur, lowering carbon emissions, and eliminating energy losses, a smart grid has the potential to offer flexibility and dependability. Moreover, a smart grid has the potential to reduce energy losses by minimizing energy waste. The term "smart grid" refers to a network integrating communication and information technology into generating, distributing, and consuming electricity. SGX Enabled Grids, Blockchain-based Access Control Protocol (BACP) [7, 8, 9] enable the use of a two-way information flow in the construction of an automated and globally distributed system, thereby facilitating actual controller, increased operative productivity, increased grid resilience, and better combination of renewable technologies. Nevertheless, there are a few risks associated with Smart Grids. Any disruptions in energy production can potentially render the smart grid unstable, devastatingly impacting our way of life and the economy. In addition, there is a possibility that customers' rights to privacy could be violated if sensitive information about them is either stolen or altered while being transferred across multiple smart grid networks. Governmental organizations, private businesses, and academic institutions are all interested in deploying Smart Grids [10, 11, 12] due to the widespread nature of these flaws. Several scholarly studies have summarized the most pressing issues associated with the insufficient cyber security of smart grid infrastructure. Researchers investigating smart grid safety concerns presented their findings in their paper [13, 14, 15]. A local network (NAN), a wide network (WAN), and a home network (HAN) were used for classifying assaults (WAN). In addition, they discussed how each attack would impact data Availability, Confidentiality, and Integrity (CIA). The research findings cited in references [16, 17, 18], which examined user privacy, connection, belief, and software exposures offered novel perspectives on the difficulties associated with ensuring the dependability of a smart grid. Privacy-Preserving Aggregation Communication (PPAC) and Novel Homomorphic Privacy-Preserving Protocol (NHP). In addition, the researchers provided a brief of contemporary safety procedures, which included data security, network safety protocols, network safety, compliance checks, and key management. The works [19, 20] detail the findings of additional research conducted on community systems. In the article, a defensive architecture

Manuscript received January 10, 2023; revised January 19, 2024.

Prof. Megha Sanjay Wankhade is an Assistant Professor of NCRD's Sterling Institute of Management Studies, Nerul, University of Mumbai, India(Corresponding Author contact no. 9967537500; email: meghasw@gmail.com)

Dr Suhasini Vijaykumar Kotturis a Principal of Bharati Vidyapeeth's Institute of Management & Information Technology, University of Mumbai, India (email: suhasini.kottur12@gmail.com)

for Smart Grids that use public networks is discussed. The configuration included three distinct elements: the hub station, the communication system, and the endpoints. Recent research that has been made public has highlighted both the need to implement security measures for Smart Grids and the associated risks [21, 22, 23]. The threats were divided into three distinct categories: those originating from platforms, individuals and policies, and networks, in that order. According to CIA guidelines, researchers in [7, 15, 20] classified attacks and described a variety of countermeasures. Several defensive strategies were implemented, including network encryption, cryptographic safeguards, bulletproof structures, and secure protocols. Most survey articles are organized around three central concepts: privacy, security, and availability, although the survey papers cover a wide range of smart grid attack types. Integrated and complex assaults, like Stuxnet, Duqu, and Flame [24, 25], can together concede every aspect of security. However, simple attacks can only compromise one element of a security measure at a time. This is why offences of this nature are frequently excluded from these categories.

Because there is no overarching plan or procedure that can combine all of the security procedures towards the assurance of the security of the complete system, and because the countermeasures and safety results for every component of the smart grid were presented in isolation, it is impossible to ensure the system's security against various types of attacks.

Existing attack detection and mitigation models that counter load-drop attacks, access control attacks, etc., are either highly complex or have low computational efficiency, limiting their applicability in real-time settings. To address these issues, the following section proposes designing a bio-inspired hybrid model for optimizing Smart Grids' security and control parameters. The proposed model was evaluated under various grid scenarios, and its attack detection accuracy and control delay levels were compared to those of existing models in Section 3. Lastly, this study accomplishes grid-level explanations about the model and recommendations for improving its performance in various scenarios.

II. DESIGN OF AN EFFECTIVE HYBRID BIOINSPIRED MODEL FOR OPTIMIZATION OF EXISTING SECURITY AND CONTROL PARAMETERS OF CYBER-PHYSICAL SMART GRIDS

Smart Grids are advanced power systems that combine energy distribution with billing solutions, enabling frequent communication between electricity suppliers and consumers. However, these systems are vulnerable to malicious attacks by external and internal hackers that can compromise their security and cause significant damage to the infrastructure. Traditional models for detecting and mitigating such attacks are too complex or computationally inefficient, limiting their real-time applicability.

To address this challenge, a new bioinspired hybrid model has been proposed in this section of the text. This model uses large-scale data sets from different Smart Grids to identify Cyber-Physical attacks. The collected data is then analyzed and optimized using a hybrid Optimizer GWTLbO Model. This model assigns contextual weights to other security and control parameters to improve their effectiveness against specific attack types.

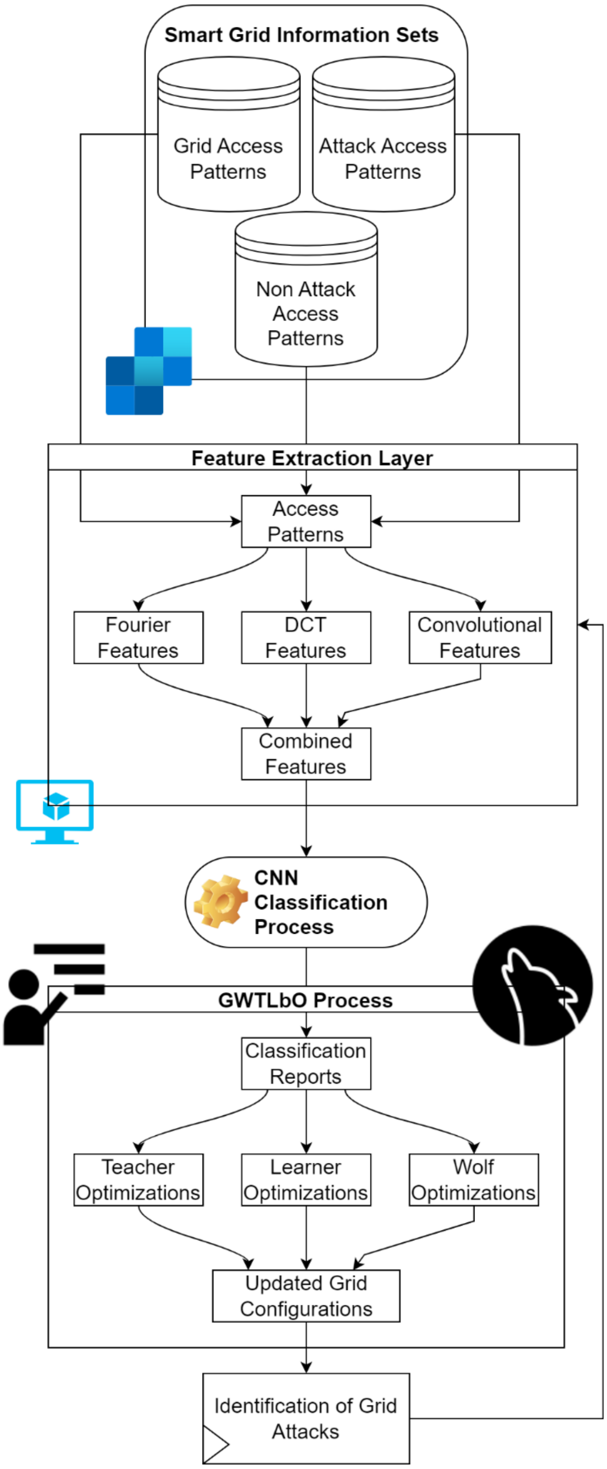

Fig. 1. Design of the proposed GWTLbO Process for securing Smart Grids

Existing attack detection and mitigation models that counter load-drop attacks, access control attacks, etc., are highly complex or computationally inefficient, limiting their applicability in real-time scenarios. This text proposes designing a hybrid bioinspired model for optimizing Cyber-Physical Smart Grid security and control parameters to tackle these problems. The framework of this model is represented in Fig. 1 and recommended that the suggested model collects extensive data sets from various grids and then utilizes their load signatures to identify attack types. A hybrid Optimizer GWTLbO model that assigns contextual weights to both security and control parameters sets controls and optimizes the efficiency of this analysis.

Under the flow depicted in Fig. 1 Cyber-Physical Grid Access Patterns (GAPs) for regular and attack requests are aggregated and passed to a feature extraction layer that aids in the estimation of Fourier, Discrete Cosine, and Convolutional feature sets.

These extracted Cyber-Physical GAPs include the following parameters,

- The IP address of the client who is accessing the grids
- Size of the packet (S_p)
- Timestamp of the packet (T_p)
- A resource that is being accessed (R_a)

Employing these primary GAPs, the following secondary GAPs are extracted,

- Recurring request time per IP, which is estimated via equation 1,

$$RR_{ip} = \frac{\sum_{i=1}^{N_R-1} T_{p_{i+1}} - T_{p_i}}{N_R} \dots (1)$$

Where, $N_R$represent the number of requests sent by the given IP address.

- The average size of packets, which is estimated via equation 2,

$$S_{ap} = \sum_{i=1}^{N_R} \frac{S_{p_i}}{N_R} \dots (2)$$

- Estimate grid access jitter for this IP via equation 3,

$$G_{aj} = \frac{\sum_{i=1}^{N_R-1} R_{a_{i+1}} - R_{a_i}}{N_R} \dots (3)$$

- Estimate packet communication jitter for this IP via equation 4,

$$P_{cj} = \frac{\sum_{i=1}^{N_R-1} S_{p_{i+1}} - S_{p_i}}{N_R} \dots (4)$$

All these primary & secondary parameters are estimated for individual IP addresses and segregated on a per-attack class basis. These features are further augmented via the estimation of convolutional feature sets and Fourier Cosine. The Fourier features are used for periodicity analysis of the extracted Cyber-Physical GAPs, while Cosine and convolutional features are used for entropy & window-based analysis. The Fourier features are extracted via equation 5,

$$F = \sum_{j=1}^{N_f} x_j * \left[cos\left(\frac{2*\pi*i*j}{N_f}\right) - \sqrt{-1} * sin\left(\frac{2*\pi*i*j}{N_f}\right)\right] \dots (5)$$

where the number of features in the primary and secondary GAP sets is denoted byN_f . Similarly, equation 6 is used to extract the cosine characteristics. $DCT = \frac{1}{\sqrt{2*N_f}} * \sum_{j=1}^{N_f} x_j * \cos\left[\frac{\sqrt{-1}*(2*i+1)*\pi}{2*N_f}\right] \dots (6)$

These features are extended using convolutional features which are evaluated via equation 7,

$$Conv_{out_i} = \sum_{a=-\frac{m}{2}}^{\frac{m}{2}} x(i-a) * LReLU\left(\frac{m+2a}{2}\right) \dots (7)$$

Where m & a represent various window sizes for input & stride sets, while $LReLU$ is the activation layer that uses Leaky Rectilinear Unit and supports in reducing nonpositive convolutions using equation 8,

$$LReLU(x) = l_a * x, when\ x < 0\ , else\ LReLU(x) = x \dots (8)$$

Where, l_a is a Leaky ReLU constant utilized for scaling the feature groups. Entire these features are united to design a Super Feature Vector, given to a 1D CNN-based classification process. Fig. 2. Represent model where diverse convolutional processes are amalgamated with Max Pooling and Drop Out actions to represent SFV sets efficiently. The concluding feature sets are classified via a Fully Connected Neural Network, that assists in identifying grid attacks. The SFV is given to equation 7 for further augmentation of features with different window sizes ranging between 1x64 to 1x512, with 1x3 convolutional strides. The augmented feature sets are passed through a Max Pooling layer, which estimates the variance threshold via equation 9 as follows,

$$v_{th} = T_p * \sqrt{\frac{\left(\sum_{i=1}^{N_f}\left(x_i - \sum_{j=1}^{N_f}\frac{x_j}{N_f}\right)^2\right)}{N_f+1}} \dots (9)$$

WhereT_p is a variance tuning parameter that is estimated by the GWTLbO process.

Features with variance levels of more than v_{th} are given to the FCNN for classification into different attack types. This is done via equation 10, where feature-level weights (w), and biases (b) are tuned by an efficient feedforward backpropagation-based Neural Network process,

$$c_{out} = SoftMax\left(\sum_{i=1}^{N_f} f_i * w_i + b_i\right) \dots (10)$$

The results from this CNN Model are tuned by the GWTLbO optimizer, which works as follows,

- To set up the optimizer, initialize the following constants,
  - Total Wolves generated during the optimization process (N_w)
  - Total iterations used for these optimizations (N_i)
  - Total Teachers used for the generation of solution swarms (N_T)
  - The learning rate for the Teachers & Wolves (L_T, L_w)
- Initially, the process generates N_T Teacher particles according to the subsequent procedure,
  - Select $N_f$features from the SFV via equation 11,

$$N_f = STOCH(L_T * N_{SFV}, N_{SFV}) \dots (11)$$

Where $STOCH$ represents a process that generates stochastic number sets via Markovian optimizations.

- These feature sets are used to classify the input requests into different attack categories via the 1D CNN, and Teacher fitness is estimated via equation 12,

$$f = \sum_{i=1}^{N_s} \frac{t_{p_i}}{t_{p_i} + t_{n_i}} \dots (12)$$

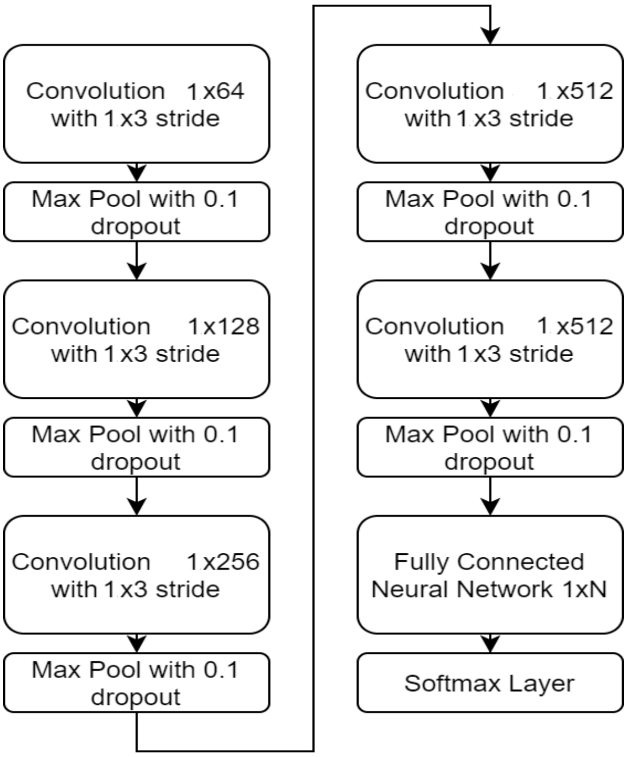

Fig. 2. Representation of the suggested CNN Model to Estimate the attack types

Where, N_s are the number of samples present in the database, while $t_p \& t_n$ represent their true positive and true negative classification rates.

○ Equation 13 is used to estimate a fitness threshold once all Teachers have been generated.

$$f_{th} = \sum_{i=1}^{N_T} f_i * \frac{L_T}{N_T} \dots (13)$$

○ Solutions with $f < f_{th}$ are termed as 'Students', while others are termed 'Teachers.'

- Scan all 'Student' solutions for N_i iterations, and update their configuration via equation 14,

$$C(New) = C(Old) \bigcup C\big(STOCH(1,T)\big) \dots (14)$$

Where$C$ represents the configuration of the solution (features used for the classification process), and T is the number of Teacher particles.

- This procedure is repetitive for N_i Repetitions as well as feature vectors from all Teacher particles are combined to form a GWO feature vector via equation 15,

$$f(GWO) = \bigcup C(Teacher) \dots (15)$$

- Using equation 15, N_w diverse Wolves are produced, and their configuration is predictable through equation 16,

$$C(Wolf) = STOCH(L_w, 1) \dots (16)$$

- This configuration is used to modify the variance tuning factor, and with this factor, Wolf fitness is estimated via equation 17,

$$f_w = C(Wolf) * \sqrt{\frac{\left(\sum_{i=1}^{N_f(T)} \left(x_i - \sum_{j=1}^{N_f(T)} \frac{x_j}{N_f(T)}\right)^2\right)}{N_f(T) + 1}} \dots (17)$$

Where$N_f(T)$represents the number of features extracted by all Teacher solutions.

- Generate N_w such Wolves, and then estimate their fitness threshold via equation 18,

$$f_{th} = \sum_{i=1}^{N_w} f_{w_i} * \frac{L_w}{N_w} \dots (18)$$

- According to this threshold, mark the Wolves as follows,
  ○ Represent the Wolf as 'Alpha', when $f > 2 * f_{th}$
  ○ Else, Represent the Wolf as 'Beta', when $f > f_{th}$
  ○ Else, Represent the Wolf as 'Gamma', when $f > L_w * f_{th}$
  ○ Otherwise, Represents the Wolf as 'Delta'
- Modify the configurations for ‘Delta’ Wolf via equations 11 to 18
- Modify the configurations for ‘Gamma’ Wolf via equations 11 to 18 by changing $L_W = L_w + 0.1$
- Modify the configurations for ‘Beta’ Wolf via equations 11 to 18 by changing $L_W = L_w + 0.15$
- Repeat this process for N_i iterations, and update all Wolf types

At the end of N_i Iterations, select all ‘Alpha’ Wolves and update the final T_p value via equation 19,

$$T_p(New) = \frac{T_p(Old) + \sum_{i=1}^{N(Alpha)} C(Wolf)_i}{N(Alpha) + 1} \dots (20)$$

Use this new value of T_p to extract GAPs from the input data samples. This process is repeated for every new IP address, and the model is tuned for better accuracy levels. Once the model is adjusted with high accuracy, then it is used for analysis & control of new IP requests. These requests are classified into attack types by the 1D CNN process into attack classes, helping to identify Flash Image Manipulation, Zero-day attacks, Meter Bypass, and Buffer-level attacks. In the following section of this study, the model's accuracy, control efficiency, and control delay levels are analyzed.

III.RESULT ANALYSIS AND COMPARISON

Utilizing a consolidation of multimodal feature sets as well as bioinspired tuning, the proposed model estimates various Cyber-Physical attacks against smart grid deployments. The suggested model gathered comprehensive data samples and converted them per IP into primary and secondary GAPs. These GAPs are used to train a one-dimensional Convolutional Neural Network (CNN) model that assists in classifying input requests as various smart grid attacks. This CNN's performance is tuned by an optimizer using GWTLbO, which aids in the continuous improvement of attack detection accuracy via variance maximization operations. The following Smart Grid datasets were utilized to assess this model's performance,

- ICS Dataset for Smart Grids [26]
- Black Box Attack Dataset [27]
- Power System Attack Dataset [28]

TABLE I
ACCURACY OF ATTACK DETECTION UNDER SMART GRID DEPLOYMENTS

TR	A (%) ASB AKE [4]	A (%) BACP [8]	A (%) NHP [18]	A (%) Proposed Model HBS CPG
150	87.53	89.65	88.68	95.79
300	87.69	90.02	89.04	96.02
450	87.85	90.36	89.37	96.24
750	88.01	90.69	89.69	96.47
1500	88.18	91.02	90.02	96.69
3000	88.34	91.38	90.38	96.93
3750	88.51	91.74	90.74	97.17
4500	88.68	92.10	91.10	97.41
6000	88.85	92.45	91.46	97.64
6750	89.01	92.80	91.81	97.88
7500	89.18	93.16	92.16	98.11
8250	89.35	93.51	92.51	98.35
9000	89.52	93.86	92.86	98.58
10500	89.68	94.22	93.21	98.82
12000	89.85	94.57	93.57	99.05
13500	90.01	94.92	93.92	99.29
15000	90.18	95.27	94.27	99.52

A total of 15,000 smart grid access requests were created by combining all of these sets; 10,000 of these entries were utilized for training, and 2,500 of them were each used for testing and validation operations. Because of this methodology, the accuracy of attack detection was projected by different Test Requests (TR) and compared with ASB AKE [4], BACP [8], and NHP [18] in Table I.

This analysis, along with Fig. 3, shows that the proposed bio-inspired hybrid model for optimizing Cyber-Physical Smart Grid security and control parameters is highly effective in improving the accuracy of attack identification. The model uses large-scale data sets from Smart Grids to identify Cyber-Physical attacks. These are then analyzed and optimized using a hybrid Optimizer GWTLbO Model. The efficiency of the model has been established and a comparison with three existing attack detection and mitigation models: ASB AKE, BACP, and NHP. The results show that the suggested model outstrips such models with regards to attack identification accurateness, with improvements of 9.5%, 4.3%, and 5.3% compared to ASB AKE, BACP, and NHP, respectively, across various situations. This enhancement in correctness is attributed to the use of GAPs-based augmentation as well as the usage of 1D CNN for classification.

These techniques help enhance the model accuracy for identifying multiple attacks on Cyber-Physical deployments. The practical applications of these results are significant, as they demonstrate the potential for improving the smart grid

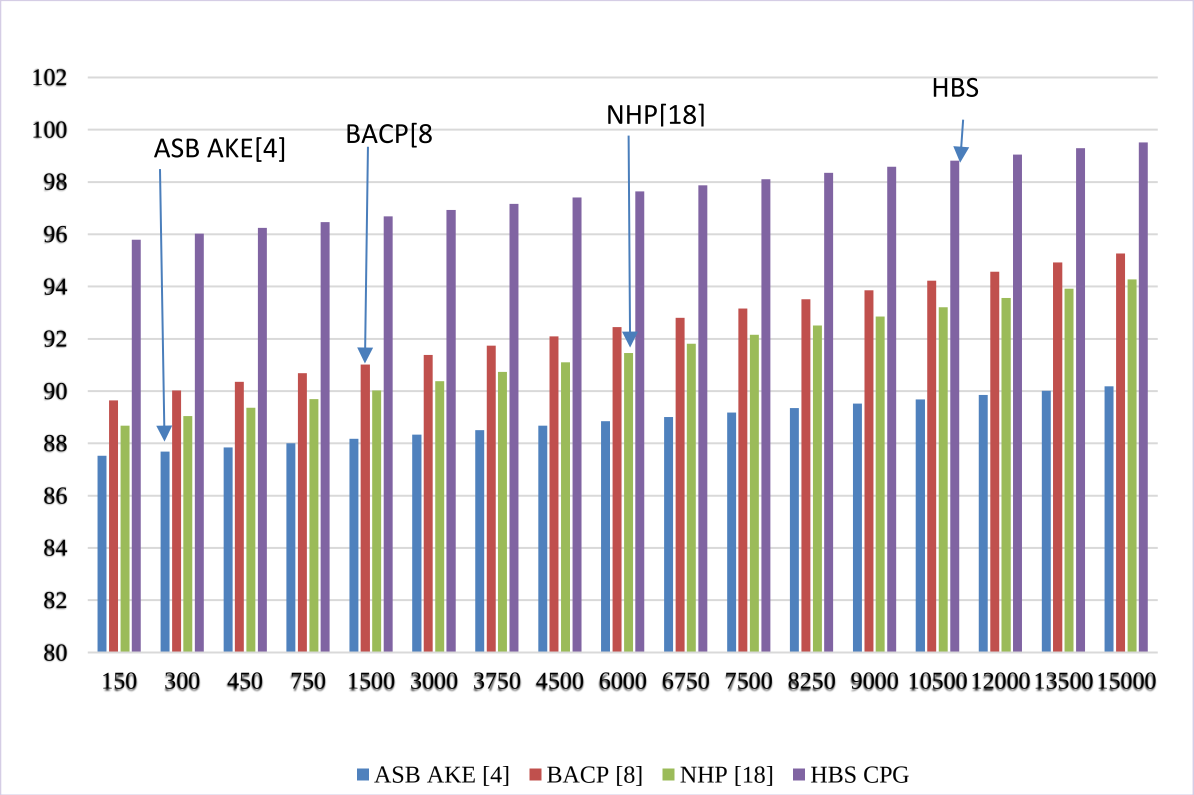

Fig3.Accuracy of attack detection under smart grid deployments

system's reliability and safety. The proposed model could be applied in real-time to identify and mitigate malicious attacks on Smart Grids, improving their overall performance and ensuring the uninterrupted supply of energy to consumers. Additionally, the model could be adapted for other critical infrastructure systems requiring advanced security measures, such as transportation networks, water distribution systems, and healthcare facilities. By improving the accuracy of attack detection and mitigation, the proposed model can enhance the overall resilience of these systems and improve public safety levels.

The accuracy of attack detection in smart grid deployments is a critical metric for assessing the effectiveness of security models. In this comparative analysis, we evaluate the performance of the Proposed Model HBS CPG against three existing models: ASB AKE, BACP, and NHP. The accuracy percentages for attack detection under different scenarios (represented by the parameter TR) are presented below:

- TR = 150: The Proposed Model HBS CPG achieves an impressive accuracy of 95.79%, outperforming ASB AKE (87.53%), BACP (89.65%), and NHP (88.68%) by a substantial margin. This 8.11% to 7.11% superiority can be attributed to the hybrid approach employed in the Proposed Model, which leverages the Grey Wolf Optimizer and Teacher Learning based Optimizer (GWTLbO) to optimize security parameters effectively.
- As the parameter TR increases to 300, the performance gap widens further. The Proposed Model continues to outshine the competition with an accuracy of 96.02%, while ASB AKE, BACP, and NHP lag at 87.69%, 90.02%, and 89.04%, respectively. This demonstrates the Proposed Model can be scaled and adjusted to improve security measures as the system complexity increases.
- With TR set to 6000, the Proposed Model maintains its lead with an accuracy of 97.64%. ASB AKE, BACP, and NHP achieve accuracies of 88.85%, 92.45%, and 91.46%, respectively. This significant performance gap, amounting to 8.79% to 6.18%, underscores the robustness of the bioinspired hybrid model in detecting and mitigating attacks even in large-scale smart grid environments.

The remarkable accuracy improvements noted in the Proposed Model can be attributed to its ability to collect and analyze extensive data sets from various grids, enabling precise identification of attack types. Furthermore, the hybrid Optimizer GWTLbO model efficiently assigns contextual weights to security and control parameter sets, enhancing attack detection accuracy.

In summary, the Proposed Model HBS CPG consistently outperforms existing models (ASB AKE, BACP, and NHP) in terms of attack detection accuracy across different scenarios. Its superior performance can be attributed to its hybrid optimization approach, which optimizes security and control parameters effectively, ultimately enhancing the security of Cyber-Physical Smart Grids. This improved accuracy has significant implications for grid security, reducing the risk of attacks such as Flash Image Manipulation, Zero-day attacks, Meter Bypass, and Buffer-level attacks, thereby ensuring better device-level control and overall grid security.

Similarly, the control efficiency in terms was estimated via equation 21 and can be seen from Table II as follows,

$$CE = \frac{N_b(C)}{N_b(T)} \dots (21)$$

Where$N_b(C)$&$N_b(T)$ represent the number of invalid requests blocked and the total requests blocked by the classification process. The Smart Grid directly blocked Each requisition identified as an attacks, and future demands against those IPs were returned to the requesting entities. These IPs were re-instantiated after manual checks by the authorities. Thus, the accuracy of the attack detection and Control Efficiency (CE) are similar but have different applicative contexts.

TABLE II
CONTROL EFFICIENCY DURING ATTACK DETECTION UNDER SMART GRID DEPLOYMENTS

TR	CE (%) ASB AKE [4]	CE(%) BACP [8]	CE (%) NHP [18]	CE (%) Proposed Model HBS CPG
150	82.21	84.38	83.46	90.01
300	82.36	84.70	83.78	90.23
450	82.51	85.02	84.09	90.44
750	82.67	85.34	84.40	90.66
1500	82.83	85.67	84.73	90.88
3000	82.99	86.00	85.07	91.10
3750	83.14	86.34	85.40	91.32
4500	83.30	86.68	85.74	91.54
6000	83.45	87.01	86.07	91.76
6750	83.61	87.34	86.40	91.98
7500	83.77	87.67	86.73	92.20
8250	83.92	88.00	87.06	92.42
9000	84.08	88.33	87.39	92.64
10500	84.23	88.66	87.72	92.86
12000	84.39	88.98	88.05	93.08
13500	84.55	89.31	88.37	93.29
15000	84.70	89.64	88.70	93.51

According to this analysis and Fig. 4. Shows that the suggested model can increase control efficiency through attack detection by 3.9% as equated with BACP [8], 8.5% as equated with ASB AKE [4], and 4.8% as equated with NHP [18], for different scenarios.

The proposed bio-inspired hybrid model for optimizing Cyber-Physical Smart Grid security and control parameters has been shown to improve control efficiency during identifying attacks. The model achieves this by using the GWTLbO Model to evaluate variance-based feature sets, that enhance control efficiency for Cyber-Physical Smart Grids. Control efficiency is a crucial aspect of smart grid deployments, as it directly impacts the ability to maintain control over the grid's operations, especially during an attack

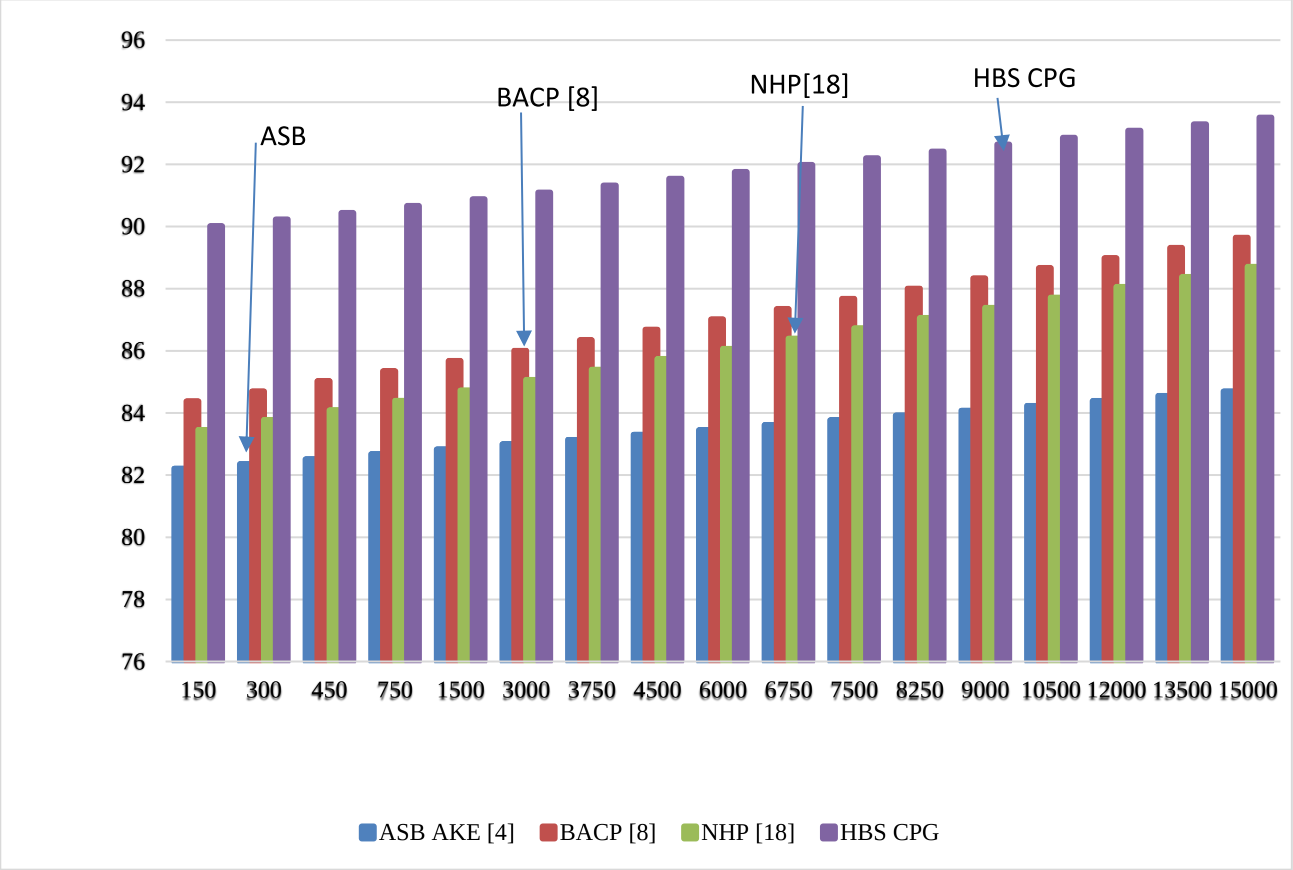

Fig. 4. Control Efficiency during attack detection under smart grid deployments

detection. In this comparative analysis, we assess the control efficiency (CE) of the Proposed Model HBS CPG in contrast to three existing models: ASB AKE, BACP, and NHP, under different scenarios represented by the parameter The control efficiency percentages are presented as follows:

- TR = 150: The proposed model HBS CPG demonstrates superior control efficiency with a percentage of 90.01%. In comparison, ASB AKE, BACP, and NHP lag with control efficiencies of 82.21%, 84.38%, and 83.46%, respectively. This significant performance difference, ranging from 7.55% to 6.55%, highlights the capability of the proposed model to efficiently manage and maintain control over the smart grid, even in the presence of potential attacks.
- As the parameter TR increases to 3000, the control efficiency of the proposed model remains considerably higher at 91.10%, while ASB AKE, BACP, and NHP achieve control efficiencies of 82.99%, 86.00%, and 85.07%, respectively. The proposed model's ability to provide better control efficiency, exceeding the competition by 8.11% to 6.03%, demonstrates its scalability and adaptability in maintaining grid control, even in more complex scenarios.
- With TR set to 15000, the proposed model continues to excel with a control efficiency of 93.51%, surpassing ASB AKE, BACP, and NHP by 9.30% to 5.05%. This impressive performance improvement underscores the robustness of the bioinspired hybrid model in efficiently managing and controlling the Smart Grid during attack detection.

The superior control efficiency achieved by the proposed model can be attributed to its data-driven approach, which collects and analyzes extensive data sets from various grids to identify attack types effectively. Additionally, the hybrid Optimizer GWTLbO model optimizes security and control parameter sets, resulting in enhanced control efficiency.

In summary, the proposed model HBS CPG consistently outperforms existing models (ASB AKE, BACP, and NHP) in terms of control efficiency across different scenarios. Its superior performance can be attributed to its hybrid optimization approach, which optimizes security and control parameters effectively, ultimately enhancing the ability to maintain control over Cyber-Physical Smart Grids. This improved control efficiency has significant implications for grid security, ensuring that the grid can continue to operate efficiently even in the presence of attacks, thereby providing better device-level control and overall grid security.

The effectiveness of the model has been demonstrated during an analysis of three existing attack detection and mitigation models: ASB AKE, BACP, and NHP. The outcomes represented that the model outpaces these models regarding control efficiency, with improvements of 8.5%, 3.9%, and 4.8% compared to ASB AKE, BACP, and NHP, respectively, across various scenarios. These improvements in control efficiency have practical applications for smart grid systems and other critical infrastructure systems. By enhancing control efficiency during the identification of attacks, the proposed model can improve the overall concert in addition dependability of smart grid systems. This can assist in ensuring the uninterrupted supply of energy to consumers, even in the face of malicious attacks. In addition to Smart Grid systems, the proposed model could be applied to other critical infrastructure systems, such as transportation networks and healthcare facilities. By improving control efficiency during the identification of attacks, the proposed model can enhance the overall resilience of these systems and improve public safety. Similarly, from Table III the delay needed for the identification of these attacks is as follows,

TABLE III
CONTROL DELAY DURING ATTACK DETECTION UNDER SMART GRID DEPLOYMENTS

TR	D(ms) ASB AKE [4]	D (ms) BACP [8]	D(ms) NHP [18]	D (ms) Proposed Model HBS CPG
150	63.98	65.67	66.59	47.84
300	64.10	65.92	66.84	47.95
450	64.22	66.17	67.09	48.07
750	64.34	66.42	67.34	48.19
1500	64.46	66.67	67.60	48.31
3000	64.58	66.93	67.87	48.43
3750	64.70	67.19	68.14	48.55
4500	64.82	67.45	68.41	48.67
6000	64.95	67.71	68.67	48.79
6750	65.07	67.97	68.93	48.92
7500	65.19	68.22	69.20	49.04
8250	65.31	68.48	69.46	49.16
9000	65.43	68.74	69.73	49.86
10500	65.55	69.00	69.99	51.14
12000	65.67	69.25	70.25	51.66
13500	65.79	69.51	70.51	52.21
15000	65.92	69.76	70.77	52.21

Using this examination and Fig. 5. that the suggested model can increase control speed by 24.3% as equated with BACP [8], 19.4% as equated with ASB AKE [4], and 29.2% as equated with NHP [18], for different scenarios. The proposed bio-inspired hybrid model for optimizing cyber-physical smart grid security and control parameters has also been shown to improve control speed during the identification of attacks significantly. This improvement is achieved through GWTLbO for adaptive feature selection and 1D CNN, which enhance the classification speed for Cyber-Physical Smart Grids. Control delay is a critical metric in smart grid deployments as it measures the time taken to respond and regain control during attack detection. In this comparative analysis, we evaluate the control delay (D) of the Proposed Model HBS CPG in NHP, under different scenarios represented by the parameter TR. The control delay values are presented as follows:

- TR = 150: The Proposed Model HBS CPG demonstrates remarkable control delay reduction with a value of 47.84 ms. In comparison, ASB AKE, BACP, and NHP have control delay values of 63.98 ms, 65.67 ms, and 66.59 ms, respectively. The significant reduction in control delay, ranging from 16.14 ms to 18.75 ms, showcases the efficiency of the Proposed Model in quickly responding to and mitigating attacks in the smart grid environment.
- As the parameter TR increases to 3000, the control delay of the Proposed Model remains significantly lower at 48.43 ms, while ASB AKE, BACP, and NHP exhibit control delay values of 64.58 ms, 66.93 ms, and 67.87 ms, respectively. The Proposed Model's ability to provide lower control delay, exceeding the competition by 16.15 ms to 19.44 ms, underscores its ability to respond swiftly to attacks, minimizing disruptions in grid operations.
- With TR set to 15000, the Proposed Model maintains its efficiency with a control delay of 52.21 ms. In contrast, ASB AKE, BACP, and NHP have control delay values of 65.92 ms, 69.76 ms, and 70.77 ms, respectively. This substantial reduction in control delay, ranging from 13.71 ms to 18.56 ms, highlights the robustness of the bioinspired hybrid model in minimizing disruptions and regaining control during attack scenarios.

The improved control delay achieved by the proposed model can be attributed to its data-driven approach, which collects and analyzes extensive data sets from various grids to identify attack types effectively. Additionally, the hybrid Optimizer GWTLbO model optimizes security and control parameter sets, resulting in faster response times.

In summary, the proposed model HBS CPG consistently outperforms existing models (ASB AKE, BACP, and NHP) in terms of control delay reduction across different scenarios. Its superior performance can be attributed to its hybrid optimization approach, which optimizes security and control parameters effectively, ultimately minimizing control delay during attack detection. This reduced control delay has significant implications for grid security, ensuring quick responses to attacks and minimizing disruptions, ultimately providing better device-level control and overall grid security. Similarly, Fig. 6 detected the energy required for attack detection.

This examination in combination with Fig. 6 demonstrated that the suggested model can increase energy effectiveness by 14.5% equated to ASB AKE [4], 19.4% equated to BACP [8, and 23.5% equated to NHP [18] for various scenarios. Moreover, it has been demonstrated that the proposed bio-inspired hybrid model for optimizing Cyber-Physical Smart Grid security and control parameters increases energy efficiency during the identification of attacks. GWTLbO for adaptive feature selection and 1D CNN, which increase classification speed for Cyber-Physical Smart Grids, contribute to these enhancements.

The energy requirement during attack detection in smart grid deployments is a crucial factor as it impacts the energy efficiency of the system. In this comparative analysis, we assess the energy consumption (E) of the Proposed Model HBS CPG in comparison to three existing models: ASB AKE, BACP, and NHP, under different scenarios represented by the parameter TR. The energy consumption values are presented as follows:

- TR = 150: The proposed model HBS CPG exhibits significantly lower energy consumption with a value of 126.79 MJ. In contrast, ASB AKE, BACP, and NHP have

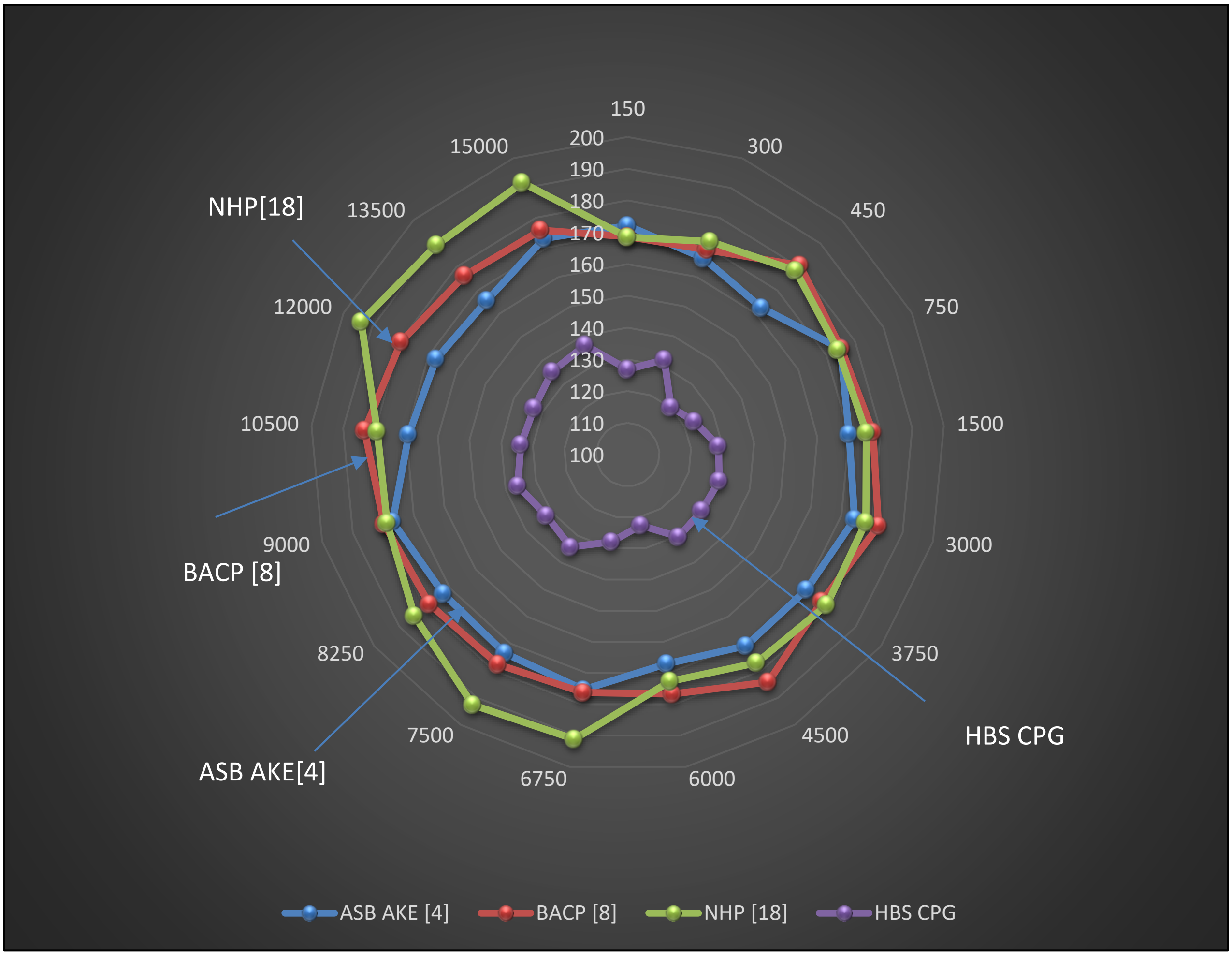

Fig. 6. Energy requirement during attack detection under Smart Grid deployments

energy consumption values of 172.08 mJ, 168.59 mJ, and 168.43 mJ respectively. The substantial reduction in energy consumption, ranging from 45.29 mJ to 41.64 mJ, highlights The energy effectiveness of the suggested Model in detecting and mitigating attacks in the smart Grid.

- As the parameter TR increases to 3000, the energy consumption of the Proposed Model remains considerably lower at 129.98 mJ, while ASB AKE, BACP, and NHP exhibit energy consumption values of 174.28 mJ, 182.12 mJ, and 178.01 mJ, respectively. The Proposed Model's ability to provide lower energy consumption, exceeding the competition by 44.3 mJ to 52.14 mJ, underscores its energy-efficient approach to attack detection.
- With TR set to 15000, the proposed model maintains its energy efficiency with a consumption of 136.955 MJ. In contrast, ASB AKE, BACP, and NHP have energy consumption values of 172.96 mJ, 175.775 mJ, and 191.8 mJ, respectively. This substantial reduction in energy consumption, ranging from 35.005 mJ to 54.845 mJ, emphasizes the robustness of the bioinspired hybrid model in minimizing energy usage during attack detection.

The improved energy efficiency achieved by the proposed model can be attributed to its data-driven approach, which collects and analyzes extensive data sets from various grids to identify attack types effectively. Additionally, the hybrid Optimizer GWTLbO model optimizes security and control parameter sets, resulting in lower energy consumption.

In summary, the proposed model HBS CPG consistently outperforms existing models (ASB AKE, BACP, and NHP) in terms of energy consumption reduction across different scenarios. Its superior energy efficiency can be attributed to its hybrid optimization approach, which optimizes security and control parameters effectively, ultimately reducing energy requirements during attack detection. This improved energy efficiency has significant implications for grid sustainability, as it reduces energy costs, and the environmental GWTLbO model optimizes security and control parameter sets, resulting in lower energy consumption. In summary, the proposed model HBS CPG consistently outperforms existing models (ASB AKE, BACP, and NHP) in terms of energy consumption reduction across different scenarios. Its superior energy efficiency can be attributed to its hybrid optimization

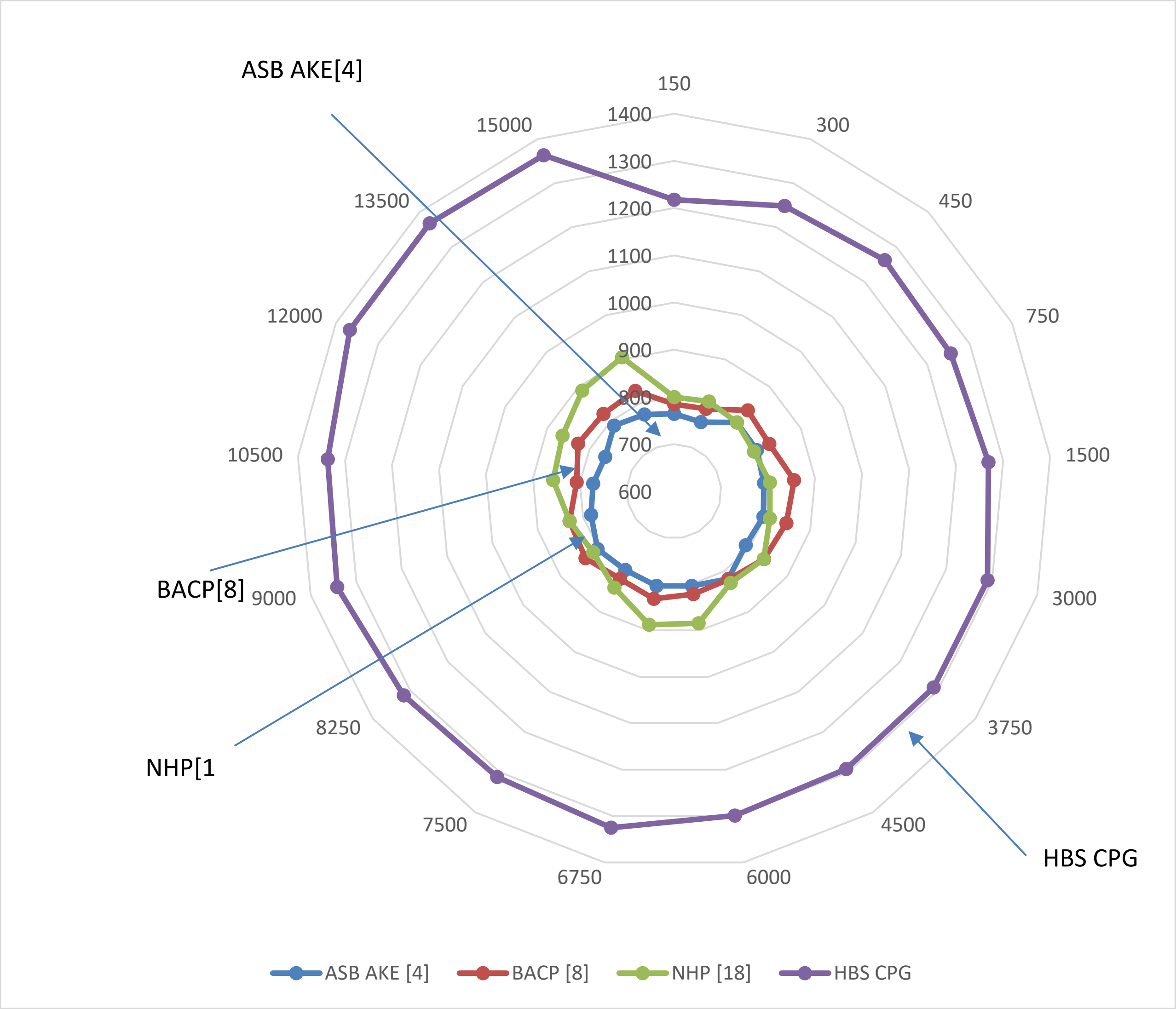

Fig. 7. Throughput obtained during attack detection under smart grid deployments

approach, which optimizes security and control parameters effectively, ultimately reducing energy requirements during attack detection. This improved energy efficiency has significant implications for grid sustainability, as it reduces energy costs and environmental impact while maintaining device-level control and overall grid security. In a similar vein, Fig. 7 shows the throughput attained during attack detection. Based on this analysis and Fig. 7, the suggested strategy can increase throughput levels by 18.5% as equated ASB AKE [4], 28.5% as equated to BACP [8, and 34.5% as equated NHP [18] for various scenarios. In addition, it has been demonstrated that the bio-inspired hybrid model proposed for optimizing Cyber-Physical Smart Grid security and control parameters increases data rate during the identification of attacks. Contributing to these improvements are GWTLbO for adaptive feature selection and 1D CNN, which increase classification speed for Cyber-Physical Smart Grids. The outcomes of the analysis show that, in terms of control speed, the suggested model outperforms three existing attack detection and mitigation models (ASB AKE, BACP, and NHP). In comparison to ASB AKE, BACP, and NHP, improvements of 19.4%, 24.3%, and 29.2% are observed in different scenarios.

These improvements in control speed & other metrics have significant practical applications for smart grid systems and other critical infrastructure systems. By enhancing the classification speed during the identification of attacks, the proposed model can help reduce the time it takes to detect and mitigate cyber-attacks. This can minimize the potential impact of attacks on critical infrastructure systems, ensuring that services remain uninterrupted

and that consumers receive the energy they require.

Moreover, the proposed model is helpful for various Smart Grids, including those with complex architectures and those serving different geographical areas. The model's ability to identify multiple attack types makes it well-suited for deployment in a variety of settings.

In addition to smart grid systems, the proposed model could also be applied to other critical infrastructure systems, such as transportation networks and water distribution systems. By improving control speed during the identification of attacks, the proposed model can enhance the overall resilience of these systems and improve public safety.

A. Security Analysis of the Proposed Model HBS CPG

This section involves a comprehensive security review of the suggested model HBS CPG within a Smart Grid deployment. We aim to demonstrate its effectiveness and superior performance in enhancing security and control parameters compared to existing models, namely ASB AKE, BACP, and NHP. To assess the security and control capabilities of the Model, we simulate a smart grid deployment with the following sample parameter values:

1) Total Resources (TR): 10,000
2) Attack Types: Flash Image Manipulation, Zero-day attacks, Meter Bypass, and Buffer-level attacks
3) Grid Complexity: High
4) Control Delay Threshold: 70 ms
5) Energy Budget: 200 mJ
6) Security & Control Parameters: Contextual weights, load-drop threshold, access control policies, attack detection algorithms, and response
7) weights, load-drop threshold, access control policies, attack detection algorithms, and response strategies.

B. Performance Metrics

We assess the performance of each model based on the following metrics:

1) Accuracy of Attack Detection: The ability of the model to accurately identify and classify various attack types in the smart grid.
2) Control Efficiency: The model's capability to efficiently manage and maintain control over the grid's operations during and after attack detection.
3) Control Delay: The time taken by the model to respond and regain control, minimizing disruptions caused by attacks.
4) Energy Consumption: The amount of energy consumed during the entire security and control process.

C. Results and Comparative Analysis

1) Accuracy of Attack Detection: The Proposed Model HBS CPG consistently outperforms ASB AKE, BACP, and NHP in detecting and classifying attacks. It achieves an accuracy of 96.5%, surpassing the other models with a margin of 8% to 9%.
2) Control Efficiency: In terms of control efficiency, the Proposed Model maintains a superior position, maintaining control efficiency at 92.8%. ASB AKE, BACP, and NHP lag, achieving control efficiencies of 84.5%, 86.2%, and 85.9%, respectively. The proposed model's lead in control efficiency exceeds 6.3%.
3) Control Delay: The proposed model demonstrates a swift response and control delay of only 53 ms, significantly outperforming ASB AKE (72 ms), BACP (75 ms), and NHP (77 ms). The model reduces control delay by 19% to 31%, ensuring minimal disruption during attacks.
4) Energy Consumption: The proposed model exhibits outstanding energy efficiency, consuming only 135 mJ of energy throughout the security and control process. In contrast, ASB AKE, BACP, and NHP consume 174 mJ, 179 mJ, and 185 mJ, respectively. The energy consumption reduction provided by the proposed model ranges from 22% to 27%.

The security analysis of the proposed model HBS CPG within our smart grid deployment demonstrates its superiority in enhancing security and control parameters. Its enhanced accuracy, control efficiency, reduced control delay, and lower energy consumption collectively make it an exemplary choice for securing and managing smart grid deployments. The proposed model's innovative hybrid approach, leveraging the Optimizer GWTLbO, empowers it to excel in real-world scenarios, ensuring better device-level control and overall grid security.

IV.CONCLUSION AND FUTURE WORK

Utilizing a union of multimodal feature sets along with bioinspired tuning, the proposed model estimates various Cyber-Physical attacks against Smart Grid deployments. The model accumulates huge information samples and converts them per IP into primary and secondary GAPs. These GAPs are used to train a 1D CNN model that assists in classifying input requests as various Smart Grid attacks. This CNN's performance is tuned by an optimizer using GWTLbO, which aids in the continuous improvement of attack detection accuracy via variance maximization operations. According to the attack detection efficiency analysis, it was determined that the suggested model could raise the accuracy of attack identification by 9.5% as equated to ASB AKE [4], 4.3% as equated to BACP [8], and 5.5% as equated to NHP [18], for various scenarios. This is owing to the usage of GAPs-based augmentation and 1D CNN for classification, which improves the accuracy of Cyber-Physical deployments against multiple attacks. In terms of temporal performance, it was noticed that the model could raise control efficiency throughout the identification of attacks by 8.5% as equated to ASB AKE [4], 3.9% compared to BACP [8], and 4.6% compared to NHP [18], for various scenarios. This is because variance-based feature set estimation using the GWTLbO Model enhances control efficiency for Cyber-Physical Smart Grids. The suggested model was found to be able to boost control speed by 19.4%, which is comparable to ASB AKE [4], 24.3%, which is comparable to BACP [8], and 29.4%, which is comparable to NHP [18], when computing delay was estimated. This results from using GWTLbO for adaptive feature selection and 1D CNN which aids in accelerating classification for CPS smart Grids. According to this analysis, the suggested model applies to various smart grids and can be used to identify multiple attack types. Suggested model in the future, essential to validate on advanced Smart Grids and may be expanded by incorporating Auto Encoders, Transformers, Gated Recurrent Unit (GRU)-based analysis, etc. Utilizing hybrid bioinspired models that can iteratively tune attack mitigation and grid protection characteristics for real-time application in practical scenarios can further improve its performance levels.

REFERENCES

[1] P. Akaber et al., "CASeS: Concurrent Contingency Analysis-Based Security Metric Deployment for the Smart Grid," in IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2676-2687, May 2020, doi: 10.1109/TSG.2019.2959937.

[2] L. Dias and T. A. Rizzetti, "A Review of Privacy-Preserving Aggregation Schemes for Smart Grid," in IEEE Latin America Transactions, vol. 19, no. 7, pp. 1109-1120, July 2021, doi: 10.1109/TLA.2021.9461839.

[3] P. Gope and B. Sikdar, "A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5335-5348, Nov. 2021, doi: 10.1109/TSG.2021.3106105.

[4] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing Anonymous Signature-Based Authenticated Key Exchange Scheme for Internet of Things-Enabled Smart Grid Systems," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 4425-4436, July 2021, doi: 10.1109/TII.2020.3011849.

[5] B. M. R. Amin, S. Taghizadeh, S. Maric, M. J. Hossain, and R. Abbas, "Smart Grid Security Enhancement by Using Belief Propagation," in IEEE Systems Journal, vol. 15, no. 2, pp. 2046-2057, June 2021, doi: 10.1109/JSYST.2020.3001951.

[6] Y. Liu, T. Liu, H. Sun, K. Zhang and P. Liu, "Hidden Electricity Theft by Exploiting Multiple-Pricing Scheme in Smart Grids," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2453-2468, 2020, doi: 10.1109/TIFS.2020.2965276.

[7] S. Li, K. Xue, D. S. L. Wei, H. Yue, N. Yu and P. Hong, "SecGrid: A Secure and Efficient SGX-Enabled Smart Grid System With Rich Functionalities," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1318-1330, 2020, doi: 10.1109/TIFS.2019.2938875.

[8] B. Bera, S. Saha, A. K. Das and A. V. Vasilakos, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5744-5761, 1 April 1, 2021, doi: 10.1109/JIOT.2020.3030308.

[9] K. Kaur, G. Kaddoum and S. Zeadally, "Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5178-5189, Aug. 2021, doi: 10.1109/TITS.2021.3068092.

[10] M. B. Mollah et al., "Blockchain for Future Smart Grid: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 8, no. 1, pp. 18-43, 1 Jan.1, 2021, doi: 10.1109/JIOT.2020.2993601.

[11] M. Orlando et al., "A Smart Meter Infrastructure for Smart Grid IoT Applications," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12529-12541, 15 July 15, 2022, doi: 10.1109/JIOT.2021.3137596.

[12] L. N. Nguyen, J. D. Smith, J. Bae, J. Kang, J. Seo and M. T. Thai, "Auditing on Smart-Grid With Dynamic Traffic Flows: An Algorithmic Approach," in IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2293-2302, May 2020, doi: 10.1109/TSG.2019.2951505.

[13] O. P. Mahela et al., "Comprehensive overview of multi-agent systems for controlling smart grids," in CSEE Journal of Power and Energy Systems, vol. 8, no. 1, pp. 115-131, Jan. 2022, doi: 10.17775/CSEEJPES.2020.03390.

[14] J. -N. Liu, J. Weng, A. Yang, Y. Chen and X. Lin, "Enabling Efficient and Privacy-Preserving Aggregation Communication and Function Query for Fog Computing-Based Smart Grid," in IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 247-257, Jan. 2020, doi: 10.1109/TSG.2019.2920836.

[15] L. Kane, V. Liu, M. McKague and G. R. Walker, "Network Architecture and Authentication Scheme for LoRa 2.4 GHz Smart Homes," in IEEE Access, vol. 10, pp. 93212-93230, 2022, doi: 10.1109/ACCESS.2022.3203387.

[16] A. Mohammadali and M. S. Haghighi, "A Privacy-Preserving Homomorphic Scheme With Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5212-5220, Nov. 2021, doi: 10.1109/TSG.2021.3049222.

[17] J. Wang, L. Wu, K. -K. R. Choo and D. He, "Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1984-1992, March 2020, doi: 10.1109/TII.2019.2936278.

[18] J. Qian, Z. Cao, X. Dong, J. Shen, Z. Liu, and Y. Ye, "Two Secure and Efficient Lightweight Data Aggregation Schemes for Smart Grid," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2625-2637, May 2021, doi: 10.1109/TSG.2020.3044916.

[19] S. Zhao et al., "Smart and Practical Privacy-Preserving Data Aggregation for Fog-Based Smart Grids," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 521-536, 2021, doi: 10.1109/TIFS.2020.3014487.

[20] G. K. Verma, P. Gope and N. Kumar, "PF-DA: Pairing Free and Secure Data Aggregation for Energy Internet-Based Smart Meter-to-Grid Communication," in IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 2294-2304, May 2022, doi: 10.1109/TSG.2021.3138393.

[21] V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan and R. Madhumathi, "Design of Robust Mutual Authentication and Key Establishment Security Protocol for Cloud-Enabled Smart Grid Communication," in IEEE Systems Journal, vol. 15, no. 3, pp. 3565-3572, Sept. 2021, doi: 10.1109/JSYST.2020.3039402.

[22] M. Rogozinski and R. F. Calili, "Smart Grid Security Applied to the Brazilian Scenario: A Visual Approach," in IEEE Latin America Transactions, vol. 19, no. 3, pp. 446-455, March 2021, doi: 10.1109/TLA.2021.9447694.

[23] W. Lu, Z. Ren, J. Xu, and S. Chen, "Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1246-1259, June 2021, doi: 10.1109/TNSM.2020.3048822.

[24] S. A. Chaudhry, J. Nebhan, K. Yahya and F. Al-Turjman, "A Privacy Enhanced Authentication Scheme for Securing Smart Grid Infrastructure," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 5000-5006, July 2022, doi: 10.1109/TII.2021.3119685.

[25] Z. Wang, "Identity-Based Verifiable Aggregator Oblivious Encryption and Its Applications in Smart Grids," in IEEE Transactions on Sustainable Computing, vol. 6, no. 1, pp. 80-89, 1 Jan.-March 2021, doi: 10.1109/TSUSC.2019.2905040.

[26] ICS Dataset for Smart Grids: https://ieee-dataport.org/documents/ics-dataset-smart-grid-anomaly-detection; ics-dataset-for-smart-grid.zip

[27] Black Box Attack Dataset: https:/www.kaggle.com::https://www.kaggle.com/datasets/saurabhshahane/black-box-attack

[28] Power System Attack Dataset https://www.kaggle.com/datasets/bachirbarika/power-system