*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

# BSCSML: Design of an Efficient Bioinspired Security &Privacy Model for Cyber Physical System using Machine Learning

**Megha Sanjay Wankhade[1*], Suhasini Vijaykumar kottur[2]**
[1]Assistant Professor: MCA Department,
NCRD's Sterling Institute of Management Studies,
Nerul, Navi Mumbai, India
e-mail: meghasw@gmail.com
[2]Principal: MCA Department
Bharati Vidyapeeth's Institute of Management Studies and Research
Belapur, Navi Mumbai, India
e-mail: suhasini.kottur12@gmail.com

**Abstract:** With the increasing prevalence of Smart Grid Cyber Physical Systems with Advanced Metering Infrastructure (SG CPS AMI), securing their internal components has become one of the paramount concerns. Traditional security mechanisms have proven to be insufficient in defending against sophisticated attacks. Bioinspired security and privacy models have emerged as promising solutions due to their stochastic solutions. This paper proposes a novel bio-inspired security and privacy model for SG CPS AMI that utilizes machine learning to strengthen their security levels. The proposed model is inspired by the hybrid Grey Wolf Teacher Learner based Optimizer (GWTLbO) Method's ability to detect and respond to threats in real-time deployments. The GWTLbO Model also ensures higher privacy by selecting optimal methods between k-privacy, t-closeness & l-diversity depending upon contextual requirements. This study improves system accuracy and efficiency under diverse attacks using machine learning techniques. The method uses supervised learning to teach the model to recognize known attack trends and uncontrolled learning to spot unknown attacks. Our model was tested using real-time IoT device data samples. The model identified Zero-Day Attacks, Meter Bypass, Flash Image Manipulation, and Buffer-level attacks. The proposed model detects and responds to attacks with high accuracy and low false-positive rates. In real-time operations, the proposed model can handle huge volumes of data efficiently. The bioinspired security and privacy model secures CPS efficiently and is scalable for various cases. Machine learning techniques can improve the security and secrecy of these systems and revolutionize defense against different attacks.

**Keywords:** Cyber Physical, Attacks, Security, Privacy, Bioinspired, Accuracy, Rates, Scenarios.

## I. INTRODUCTION

Because cyber-Physical systems are becoming more and more pervasive in our everyday lives, concerns regarding their privacy and security have become increasingly important for real-time scenarios via Privacy-aware Reconfigurable Secure-Firmware Updating Framework (PRSUF) [1, 2, 3]. These systems, which combine the real and virtual worlds, have been implemented in a variety of fields, including healthcare, transportation, and energy production levels [4, 5, 6]. Because of the critical nature of these systems, cybercriminals are likely to target them under different attacks. As a result, it is imperative that robust security and privacy mechanisms be developed in order to protect these systems.

Smart Grid Cyber Physical Systems with Advanced Metering Infrastructure (SG CPS AMI) have been protected with the help of conventional security mechanisms such as firewalls, intrusion detection systems, and antivirus software. However, in light of the increasingly sophisticated attacks that can be launched against these systems, they are no longer adequate as a line of defence. As a direct result of this, new approaches have emerged, such as models of security and privacy that are bio-inspired and provide stochastic solutions [7, 8, 9] via use of Physically Unclonable Functions (PuFs).

Models of security and privacy that are bio-inspired are an innovative approach to cybersecurity that draws inspiration from the ways in which nature detects and responds to threats. Bio-inspired security and privacy models [10, 11, 12]. These types of models draw a significant amount of motivation from the body's immune system. It is a complicated biological system that monitors the body for the presence of foreign pathogens and mounts an appropriate defense against them in different scenarios. Several applications, such as intrusion detection systems, malware detection, and spam filtering, have used privacy and security models inspired by biological systems [13, 14, 15].

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:** 25 August 2023 **Revised:** 10 October 2023 **Accepted:** 24 October 2023*

Integrating bio-inspired security and privacy models with secure data storage technology has demonstrated a great deal of promise in the context of protecting cyber-physical systems [16, 17, 18]. While bio-inspired security and privacy models employ machine learning algorithms to improve the detection and response of cyber-attacks, secure data storage technology offers a decentralized and immutable method of storing data, which enhances both security and privacy levels [19, 20].

In this paper, we propose a novel bio-inspired security and privacy model for cyber-physical systems. To improve the model's overall efficacy, it makes use of secure data storage that is powered by machine learning. The ability of the immune system to recognize and react to dangers in the present moment has served as an inspiration for our model. We make use of secure data storage technology to store and exchange data in a secure manner, and at the same time, we employ machine learning algorithms to enhance the accuracy and productivity of the model under real-time scenarios.

The model that we have proposed is intended to protect cyber-physical systems from being attacked by hackers in real time by detecting threats and providing a response to them. In order to train the model to recognize both known and unknown attack patterns, we make use of supervised learning algorithms as well as unsupervised learning algorithms. In addition, our model makes use of the distributed ledger technology known as secure data storage in order to safely store data and distribute it to the various parts of the system.

To determine how useful our proposed model is, we carried out a comprehensive set of experiments using a dataset of cyber-attacks. The results of these tests will help us determine how useful our model is. According to the findings of our research, the model that was proposed is capable of achieving a high level of accuracy when it comes to detecting and responding to attacks while also maintaining a low rate of false positives. In addition to this, our model is very effective, and it can handle the processing of a significant amount of data in real-time scenarios.

In the following section, we will discuss the relevant research in bio-inspired security and privacy models, as well as secure data storage technology. In Section 3, we will describe our proposed model in detail, including the architecture as well as the various components that will be used to increase its level of privacy and security. In Section 4, we describe the methodology used in the experiment as well as the findings. In the final section of the paper, Section 5, we summarise the paper's findings and discuss potential future recommendations for research in this field for different scenarios.

A. Discussion on the use of GWTLbO Model

The proposed bio-inspired security and privacy paradigm for Smart Grid Cyber Physical Systems with Advanced Metering Infrastructure (SG CPS AMI) employs the GWTLbO (Grey Wolf Teacher Learner based Optimizer) technique. Because of its capacity to identify and respond to threats in real-time deployments, the GWTLbO method is used to defend CPS systems against complex attacks. The GWTLbO approach offers the following advantages over existing methods:

Randomized Optimal Control Since it is founded on stochastic optimization techniques, the GWTLbO method can manage dynamic and complex optimization problems. In the context of CPS security and privacy, where threats and attacks may vary and evolve rapidly, the ability to adapt and respond in real-time is essential. Due to its stochastic nature, GWTLbO is able to overcome these obstacles effectively.

GWTLbO combines the benefits of the Grey Wolf Optimizer (GWO) and Teacher Learner based Optimizer (TLO) algorithms. The foraging practices of Grey Wolves influence GWO, which achieves a decent equilibrium between exploitation and exploration. In contrast, TLO replicates the teaching-learning process and demonstrates rapid convergence. By combining these two methods, GWTLbO capitalizes on their complementary advantages and enhances optimization performance.

Real-Time Threat Detection: One of the primary advantages of the GWTLbO method is its ability to detect and respond to threats in real-time. This is essential in CPS settings where prompt action is required to prevent potential assaults. The GWTLbO model can perpetually monitor the system, analyze incoming data, and rapidly identify any anomalous activity or potential intrusions, allowing for prompt protection.

Contextual Privacy: The GWTLbO model takes contextual privacy requirements into account. It selects k-privacy, t-closeness, and l-diversity as the optimal privacy approaches based on the requirements of the CPS system. This adaptive technique enhances privacy protection by ensuring higher privacy levels while taking into account the system's specific characteristics and needs.

Utilizing computer intelligence, The GWTLbO model employs machine learning methods to enhance system performance and security. Using supervised learning, the model is taught to recognize well-known attack tendencies, enabling proactive detection and defence. Uncontrolled knowledge is also used to identify unidentified assaults, allowing for the identification of new threats. In the proposed model, GWTLbO and machine learning are combined to improve detection and response accuracy and efficiency.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

GWTLbO's advantages include real-time threat identification, adaptability to dynamic situations, contextual privacy protection, and integration with machine learning techniques. These benefits of the proposed bio-inspired model make it a viable option for enhancing the security and confidentiality of CPS systems.

The bio-inspired model includes contextual privacy preservation techniques such as k-privacy, t-closeness, and l-diversity. By selecting the most effective privacy techniques based on specific requirements, the model may enhance the privacy protection of CPS systems. This is especially crucial given that CPS systems frequently manage sensitive information such as personal data and energy use trends. Personal information can be protected by assuring higher levels of privacy, nurturing trust in CPS technology, and furthering society by defending privacy rights.

In conclusion, the implementation of the bioinspired security and privacy model using the GWTLbO method could result in enhanced cybersecurity, privacy protection, increased energy efficiency, dependable smart grid infrastructure, and technological advancement. These social benefits contribute to more stable, secure, and sustainable society scenarios.

## II. REVIEW OF SECURITY MODELS FOR SECURING CYBER PHYSICAL DEPLOYMENTS

The next iteration of interconnected systems that combine the physical and digital worlds is known as "cyber-physical systems" (CPS) [21, 22, 23]. Security of the model can be enhanced via use of Differential Privacy-enabled AMI with Federated Learning (DP-AMI-FL) techniques. To increase effectiveness and performance, these methods are used in a variety of sectors, including healthcare, transit, and industry. CPS, however, faces significant difficulties with security and privacy issues because they are susceptible to cyberattacks that could jeopardize their usefulness and security levels [24, 25, 26]. To handle these issues, a number of security and private approaches have been put forth for different use cases. The goal of this survey of the literature is to give a summary of the most important security and privacy frameworks for CPS [27, 28, 29].

Cyber-Physical System Threat Modeling: This model suggests a way for locating and reducing security risks in CPS. The model recommends remedies to minimize possible dangers and weaknesses in the system using an organized strategy. The danger model, risk analysis, and countermeasure selection are all included in the model sets [30, 31, 32].

Cyber-Physical System Security Structure: This paradigm suggests a structure to handle the security issues in CPS. Security goals, security needs, security defenses, and security guarantees are all part of the structure. To recognize and reduce security risks, the model also contains a security research approach for different use cases. Cyber-Physical Systems Privacy Preservation Structure: This paradigm suggests a structure for CPS privacy protection. The structure consists of privacy objectives, privacy standards, privacy protections, and privacy guarantees [33, 34, 35]. To recognize and reduce privacy risks, the model also contains a set of privacy research techniques.

Using confidence as the foundation for security, this model suggests a trust-based security framework for cyber-physical systems. A trust model, a confidence assessment, and trust-based security methods are all included in the model. In order to handle the confidence connections between the system's components, the paradigm also contains a set of trust management systems [36].

For CPS, this paradigm suggests a safe data administration system. The paradigm contains data security standards, data access management, data protection, data accuracy, and data availability. A structure for safe data administration is also included in the plans. Cyber-physical system security and anonymity are crucial issues. The methods covered in this literature analysis offer a methodical means of addressing these issues. Some of the most pertinent models in this area include threat modeling, security frameworks, privacy protection frameworks, trust-based security models, and safe data management models [37, 38]. These algorithms can be used to improve the security and anonymity of CPS. To create better security and private frameworks for CPS, additional study is necessary for real-time deployments.

## III. PROPOSED DESIGN OF AN EFFICIENT BIOINSPIRED SECURITY & PRIVACY MODEL FOR CYBER PHYSICAL SYSTEM VIA MACHINE LEARNING

From the review of existing security & privacy models for CPS, it can be observed that traditional security mechanisms have proven insufficient to defend against hybrid attacks. In response, bio-inspired security and privacy models have emerged as a promising solution due to their stochastic solutions. In this section, design of an efficient & novel bio-inspired security and privacy model for SG CPS AMI is discussed for different scenarios. The model utilizes machine learning to strengthen their security levels. As per the flow of model in figure 1, it can be observed that the proposed model is inspired by the hybrid Grey Wolf Teacher Learner based Optimizer (GWTLbO) Method's ability to detect and respond to threats in real-time deployments. To ensure higher privacy levels, the proposed model employs an extended version of GWO-based approach to optimize network parameter sets. This paper leverages these machine learning algorithms to improve

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

the accuracy and efficiency of the system under heterogeneous attacks. Specifically, the system utilizes a supervised learning algorithm to train the model to recognize known attack patterns and an unsupervised learning algorithm to detect new and unknown attacks. The deployed model assisted in identifying Zero-Day Attacks, Meter Bypass, Flash Image Manipulation, and Buffer-level attacks. As per the flow of the model, it can be observed that the proposed model initially collects Grid Parameter Sets (GPS), Attack Access Patterns, and Non-Attack Access Patterns for temporal input sets. These patterns are formed using IP address of accessing clients, packet sizes, timestamps of packets, ID

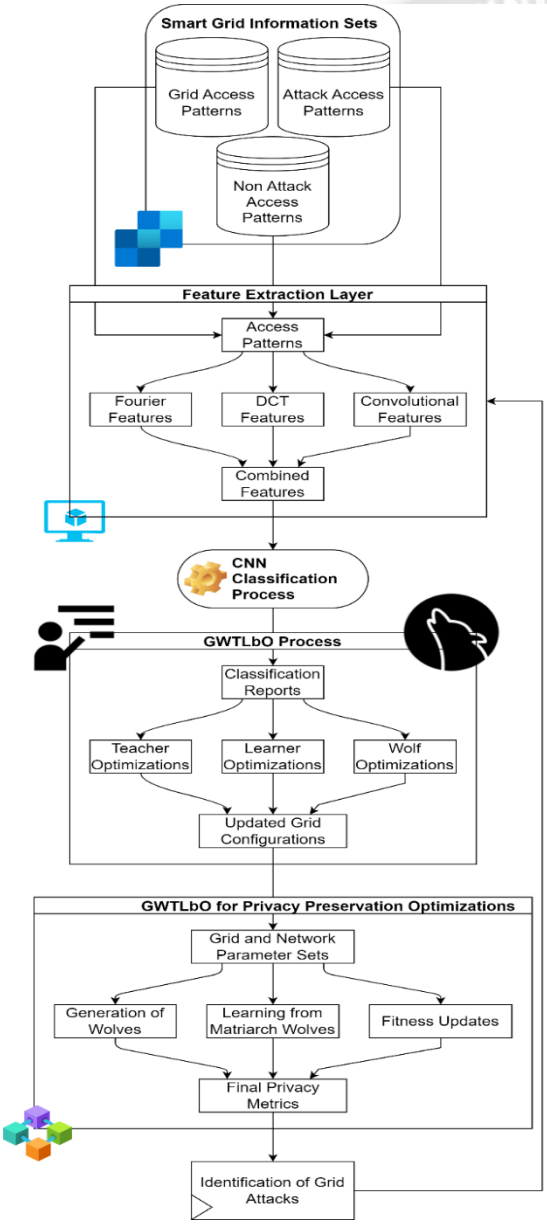


Figure 1. Design of the bioinspired model for identification of network attacks with privacy preservation operations

of accessed resources, packet delivery performance, throughput performance, and their respective attack tags. Using these patterns, a Recurring Request ($RR$) Metric is evaluated via equation 1,

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

Where, $N_R$ is the count of total requests, while $T_p$ is the timestamp for these requests. Similarly, the average packet size ($S_{ap}$) is calculated via equation 2,

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

Where, $S_p$ is size of individually communicated packets. Along with these metrics, average jitter for different requesting IPs ($G_{aj}$) is calculated via equation 3,

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

Where, $R_a$ represents address of the resource which is accessed by individual IPs. Similarly, packet communication jitter ($P_{cj}$) is estimated via equation 4,

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

Similarly, the average throughput & throughput jitter is estimated via equations 5 & 6 as follows,

$$T_a = \sum_{i=1}^{N_R} \frac{T_{p_i}}{N_R} \dots (5)$$

Where, $T_p$ represents packet throughput for the current set of requests.

$$T_{aj} = \sum_{i=1}^{N_R-1} \frac{|T_{p_i} - T_{p_{i+1}}|}{N_R} \dots (6)$$

The average packet delivery and its jitter components are estimated via equations 7 & 8 as follows,

$$PDR_a = \sum_{i=1}^{N_R} \frac{PDR_{p_i}}{N_R} \dots (7)$$

$$PDR_{aj} = \sum_{i=1}^{N_R-1} \frac{|PDR_{p_i} - PDR_{p_{i+1}}|}{N_R} \dots (8)$$

Where, $PDR_p$ represents the packet delivery ratio for individual requests. A fusion of these parameters is done to form a Cyber Physical Feature Vector (CPFV), which is augmented via a multidomain feature extraction process. This is done via extraction of multidomain value sets, including Frequency components, which are evaluated via equation 9,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

$$F = \sum_{j=1}^{N(CPFV)} x_j * \left[cos\left(\frac{2*\pi*i*j}{N(CPFV)}\right) - \sqrt{-1} * sin\left(\frac{2*\pi*i*j}{N(CPFV)}\right)\right] \dots (9)$$

Where, $N(CPFV)$represents the total number of features present in the $CPFV$ array, while $x$ represents their individual value sets. The multidomain components also include entropy features, which are estimated using Discrete Cosine Transform (DCT) via equation 10,

$$DCT = \frac{1}{\sqrt{2*N(CPFV)}} * \sum_{j=1}^{N(CPFV)} x_j * \cos\left[\frac{\sqrt{-1}*(2*i+1)*\pi}{2*N(CPFV)}\right] \dots (10)$$

Similarly, Convolutional Features are extracted via equation 11 as follows,

$$Conv_{out_i} = \sum_{a=-\frac{m}{2}}^{\frac{m}{2}} x(i-a) * LReLU\left(\frac{m+2a}{2}\right) \dots (11)$$

Where, $m$ & $a$are dimensions of different windows & strides, and $LReLU$ is an activation function that is based on Leaky Rectilinear Unit operations. These operations are used to convert negative features into positive values via equation 12, as follows,

$$LReLU(x) = l_a * x, when\ x < 0\ , else\ LReLU(x) = x \dots (12)$$

Where, $l_a$represents an activation constant, which converts negative number sets into positive feature value sets. Each of these features is fused to others to create a Super Feature Vector (SFV), which is then passed to a 1D convolutional neural network (CNN) based categorization process. A Fully Connected Neural Network (FCNN) is used to categorize the end feature sets, which aids in detecting grid assaults. For further enhancement of features, the SFV is provided to equation 11 with window widths ranging from 1x64 to 1x512 and neural steps of 1x3 for different use cases. After the enhanced feature sets have been processed by a Max Pooling layer, the threshold of variance is estimated using equation 13 as follows,

$$v_{th} = T_p * \sqrt{\frac{\left(\sum_{i=1}^{N_f}\left(x_i - \sum_{j=1}^{N_f}\frac{x_j}{N_f}\right)^2\right)}{N_f+1}} \dots (13)$$

Where, $T_p$represents a tuneable variance parameter and is calculated via the GWO optimization process.

The FCNN is used to categorize attacks based on features with variances greater than $v_{th}$ for different use cases. Equation 14 shows how this is accomplished through the use of an effective feedforward backpropagation based Neural Network method to adjust feature-level weights ($w$) and biases ($b$).

$$c_{out} = SoftMax\left(\sum_{i=1}^{N_f} f_i * w_i + b_i\right) \dots (14)$$

Where, $N_s$represents total collected samples, while $A, P$ & $R$are the testing accuracy, precision & recall levels for the classification process.

The model is continuously trained with different variance thresholds, which are estimated by a Grey Wolf Teacher Learner based Optimizer (GWTLbO) process, which works as follows,

- A set of $NT$ Teachers are stochastically generated via equation 15,

$$N_f = STOCH(L_T * N_{SFV}, N_{SFV}) \dots (15)$$

Where, $STOCH$is a stochastic process used for the generation of different number sets.

- The selected features are given to CNN, and its classification metrics are estimated to calculate Teacher fitness via equation 16 as follows,

$$f = \sum_{i=1}^{N_s} \frac{A+P+R}{3} \dots (16)$$

- After generation of $NT$ Teachers, an iteration threshold is calculated via equation 17,

$$f_{th} = \frac{\sum_{i=1}^{NT} f_i * LT}{NT} \dots (17)$$

Where $LT$ represents a learning threshold for the Teacher-Learner process.

- Teacher particles with$f < f_{th}$are marked as 'Students', and $f \geq f_{th}$ are marked as 'Teachers'
- In each iteration, all 'Student' particles are selected, and their configuration is updated from 'Teacher' particles via equation 18 as follows,

$$C(New) = C(Old) \bigcup C\big(STOCH(1,T)\big) \dots (18)$$

Where, $C$is the configuration of different set of particles.

- After iterating the process for $NI$ learning Iterations, Grey Wolf Features are estimated via equation 19 as follows,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

$$f(GWO) = \bigcup C(Teacher) \dots (19)$$

- This process is repeated for $NW$ Wolves, and a Wolf configuration is stochastically selected via equation 20,

$$C(Wolf) = STOCH(L_w, 1) \dots (20)$$

- The tuning factor is modified based on the value of $C(Wolf)$ via equation 21, and Wolf fitness is estimated via equation 22,

$$T_p = \frac{C(Wolf)}{Max\big(C(Wolf)\big)} \dots (21)$$

$$f_w = T_p * \sqrt{\frac{\left(\sum_{i=1}^{N_f(T)} \left(x_i - \sum_{j=1}^{N_f(T)} \frac{x_j}{N_f(T)}\right)^2\right)}{N_f(T) + 1}} \dots (22)$$

Where, $N_f(T)$are the features generated by different Teacher solutions.

- A set of $NW$ such Wolves are generated, and then their fitness threshold is calculated via equation 23,

$$f_{th} = \sum_{i=1}^{NW} f_{w_i} * \frac{LW_i}{NW} \dots (23)$$

Where, $LW_i$ represents learning rate for individual Wolf sets.

- Using this threshold, all Wolves are re-iterated and marked as per the following conditions,
  - For Wolves with,$fw > 2 * f_{th}$, mark them as 'Alpha' Wolves
  - For Wolves with$fw > f_{th}$, mark them as 'Beta' Wolves, and modify their learning rate via equation 24,

$$LW = LW + \frac{LW(Alpha)}{Max(LW)} \dots (24)$$

  - For Wolves with $fw < 2 * f_{th}$, mark them as 'Gamma' Wolves, and modify their learning rate via equation 25,

$$LW = LW + \frac{LW(Beta)}{Max(LW)} \dots (25)$$

  - Mark all other Wolves as 'Delta', and modify their learning rate via equation 26,

$$LW = LW + \frac{LW(Delta)}{Max(LW)} \dots (26)$$

- This process is repeated for $NI$ different Iterations, and Wolf configurations are continuously updated for each set of Iterations.

Once all Iterations are complete, then new tuning factor is calculated via equation 27,

$$T_p(New) = \frac{T_p(Old) + \sum_{i=1}^{N(Alpha)} C(Wolf)_i}{N(Alpha) + 1} \dots (27)$$

This new estimate for $T_p$is applied on raw data sets to see if it helps you pull out more information sets. Every time a new IP address is added, the procedure is replicated, and the accuracy of the algorithm is improved. Once the model has been adjusted to a high degree of accuracy, it can be used to analyze and regulate fresh IP queries. The 1D CNN method categorizes these queries into various attack categories, aiding in the detection of Zero-Day Attacks, Meter Bypass Attacks, Flash Image Manipulation Attacks, and Buffer-level Attacks.

The model is further extended via use of an extended GWTLbO, which assists in preserving privacy under real-time data access scenarios. Privacy is preserved via selection of optimal selected node nodes for different adding data operations. This is done via the following process,

- In the deployed network, a set of $N$Selected node nodes are stochastically selected via equation 28,

$$N = STOCH(LR * NM, NM) \dots (28)$$

Where, $LR$ & $NM$ represents learning rate of the extended GWO process, and total number of available selected nodes for addition of blocks.

- Dummy data is added to the storage, and based on these selected nodes, and a Wolf Fitness is calculated via equation 29,

$$fh = \sum_{i=1}^{N} \frac{D_i * E_i}{ME_i * THR_i * N} \dots (29)$$

Where, $D, E, ME$ & $THR$ represents the delay needed for adding data, energy needed for adding data, efficiency of adding data, and throughput during the data addition process. These parameters are estimated via equations 30, 31, 32, and 33 as follows,

$$D = ts_{complete} - ts_{start} \dots (30)$$

$$E = e_{start} - e_{complete} \dots (31)$$

$$ME = \frac{BM}{TB} \dots (32)$$

$$THR = \frac{BM}{D} \dots (33)$$

Where, $ts$ &e represent timestamp and residual energy levels, while $BM$ & $TB$ represents total number of data added and total data samples given for the adding data process.

- Based on this evaluation, a set of $NH$ different Wolves are generated, and their fitness threshold is estimated via equation 34,

$$f_{th} = \frac{1}{NH} \sum_{i=1}^{NH} fh_i * LR \dots (34)$$

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

- Wolves with $fh < f_{th}$ are passed to the next iteration, while Wolf with minimum fitness is marked as 'Matriarch' or 'Alpha'Wolf, and is used to update other Wolf configurations via equation 35,

$$HC(New) = HC(Old) \bigcup STOCH\big(HC(Matriarch)\big) \dots (35)$$

Where, $HC$ represents configuration of different Wolves, which contains indices of selected node nodes.

- Using this new configuration, Wolves are re-evaluated in the next set of iterations.

Once all $NI$ Iterations are completed, then selected node nodes selected by the 'Matriarch' Wolf are used for adding new datasets & samples. Parts of storage are present only with this set of selected node nodes, which assists in inclusion of stochastic privacy under different attacks. Data stored on these storage units is secured via Elliptic Curve Cryptography (ECC), and is tagged with different packet numbers, which assist while fetching the data for different scenarios. Due to these operations, the proposed model is able to improve accuracy of attack detection and incorporate privacy levels under real-time network use cases. Performance of this model is evaluated for different attacks, and compared with existing models in the next section of this text.

## IV. RESULT ANALYSIS AND COMPARISON

The accuracy and effectiveness of the system under heterogeneous attacks are improved by this paper's use of these machine learning algorithms. In particular, the system makes use of an unsupervised learning algorithm to find new and unidentified attacks and a supervised learning algorithm to train the model to recognise known attack patterns. Real-time data samples from deployed IoT device sets were used in a wide range of experiments to assess the efficacy of our proposed model. The deployed model helped to detect buffer-level attacks, meter bypass, manipulation of Flash images, and zero-day attacks. To perform these attacks, the following Societal Datasets were used,

- Auto MPG (https://archive.ics.uci.edu/dataset/9/auto+mpg)
- Intel Berkeley Research Lab Sensor Data (https://www.kaggle.com/datasets/divyansh22/intel-berkeley-research-lab-sensor-data)
- NSL-KDD Datasets & Samples (https://www.unb.ca/cic/datasets/nsl.html)
- ICS Datasets for Smart Grid Anomaly Detection (https://ieee-dataport.org/documents/ics-dataset-smart-grid-anomaly-detection)

Results demonstrate that the proposed model achieves a high level of accuracy in detecting and responding to attacks while maintaining low false-positive rates. The suggested model is also extremely effective and able to handle large amounts of data in real-time deployments. Overall, the proposed bio-inspired security and privacy model offers a solid method for protecting CPS that is highly effective and scalable for various scenarios. The fusion of machine learning algorithms offers a potent tool for enhancing the security and privacy of these systems and has the potential to fundamentally alter how cybersecurity is handled in the future for different deployments. Performance of the model was evaluated on a MATLAB Simulation under standard network configurations. The simulator assisted in deploying real-time traffic scenarios, and inject various attacks for individual scenarios. Based on this simulation strategy, nearly 10% of requests for individual communications were injected as attacks (from Zero-Day Attacks, Meter Bypass, Flash Image Manipulation, & Buffer-level attacks) and performance was compared with PR SUF [3], PuF [9], and DP AMI FL [23] for different Number of Communication (NC) requests. This performance was estimated in terms of accuracy (A), precision (P), recall (R), and delay (d) via equations 36, 37, 38 and 39 as follows,

$$A = \frac{1}{NC}\sum_{i=1}^{NC}\frac{t_{p_i} + t_{n_i}}{t_{p_i} + t_{n_i} + f_{p_i} + f_{n_i}} \dots (36)$$

$$P = \frac{1}{NC}\sum_{i=1}^{NC}\frac{t_{p_i}}{t_{p_i} + f_{p_i}} \dots (37)$$

$$R = \frac{1}{NC}\sum_{i=1}^{NC}\frac{t_{p_i}}{t_{p_i} + t_{n_i} + f_{p_i} + f_{n_i}} \dots (38)$$

$$d = \frac{1}{NC}\sum_{i=1}^{NC} ts_{complete_i} - ts_{start_i} \dots (39)$$

Where $t$ is the true rate, and $f$ represents false classification rates. Using this strategy, the accuracy of classification can be observed from table 1 as follows, Based on this study and figure 2, it can be seen that the suggested model is capable of increasing attack detection accuracy for various situations by 8.3% when compared to PR SUF [3], 3.5% when compared to PuF [9], and 6.5% when compared to DP AMI FL [23]. This is because the use of 1D CNN for categorization and the addition of multimodal characteristics helps to improve accuracy for numerous assaults on cyber-physical operations. The use of extended GWO, which helps to increase anonymity levels for various use cases, also makes this feasible. The Smart Grid immediately stopped all requests that were classified as "attacks," and subsequent requests from those IPs were forwarded to the asking organizations. Following physical examinations by the officials, these IPs were re-instantiated. Similar to that, table 2's attack categorization precision can be seen as follows,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

Table 1. Attack classification accuracy under multiple real-time scenarios

| NC | A (%) PR SUF [3] | A (%) PuF [9] | A (%) DP AMI FL [23] | A (%) BSC SMB |
|---|---|---|---|---|
| 2.5k | 86.49 | 87.60 | 85.27 | 94.01 |
| 4.5k | 86.65 | 87.94 | 85.59 | 94.23 |
| 6.5k | 86.81 | 88.27 | 85.92 | 94.46 |
| 12.5k | 86.98 | 88.61 | 86.25 | 94.68 |
| 22.5k | 87.14 | 88.95 | 86.59 | 94.91 |
| 45k | 87.31 | 89.30 | 86.93 | 95.14 |
| 55k | 87.47 | 89.64 | 87.27 | 95.38 |
| 70k | 87.64 | 89.98 | 87.60 | 95.60 |
| 90k | 87.80 | 90.32 | 87.94 | 95.83 |
| 100k | 87.97 | 90.66 | 88.27 | 96.06 |
| 112k | 88.13 | 91.01 | 88.61 | 96.29 |
| 125k | 88.29 | 91.35 | 88.94 | 96.52 |
| 135k | 88.46 | 91.69 | 89.28 | 96.75 |
| 160k | 88.62 | 92.03 | 89.61 | 96.98 |
| 180k | 88.78 | 92.37 | 89.94 | 97.21 |
| 200k | 88.95 | 92.71 | 90.28 | 97.43 |
| 225k | 89.11 | 93.05 | 90.61 | 97.66 |

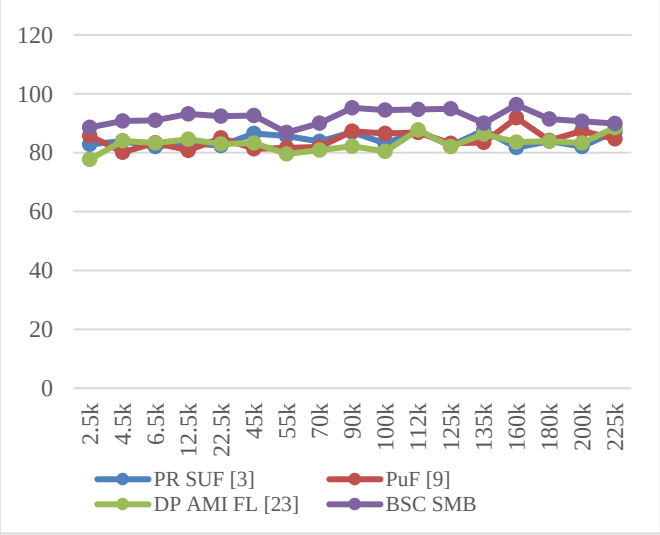


Figure 2. Attack classification accuracy under multiple real-time scenarios

Table 2. Attack classification precision under multiple real-time scenarios

| NC | P (%) PR SUF [3] | P (%) PuF [9] | P(%) DP AMI FL [23] | P (%) BSC SMB |
|---|---|---|---|---|
| 2.5k | 81.24 | 82.44 | 80.24 | 88.34 |
| 4.5k | 81.39 | 82.75 | 80.55 | 88.56 |
| 6.5k | 81.55 | 83.07 | 80.86 | 88.77 |
| 12.5k | 81.70 | 83.39 | 81.18 | 88.99 |
| 22.5k | 81.86 | 83.72 | 81.49 | 89.20 |
| 45k | 82.01 | 84.04 | 81.81 | 89.41 |
| 55k | 82.16 | 84.36 | 82.13 | 89.63 |
| 70k | 82.32 | 84.68 | 82.44 | 89.84 |
| 90k | 82.47 | 85.00 | 82.76 | 90.06 |
| 100k | 82.62 | 85.32 | 83.07 | 90.27 |
| 112k | 82.78 | 85.64 | 83.38 | 90.49 |
| 125k | 82.93 | 85.95 | 83.70 | 90.70 |
| 135k | 83.08 | 86.27 | 84.01 | 90.91 |
| 160k | 83.24 | 86.59 | 84.32 | 91.13 |
| 180k | 83.39 | 86.91 | 84.64 | 91.34 |
| 200k | 83.54 | 87.23 | 84.95 | 91.55 |
| 225k | 83.70 | 87.55 | 85.26 | 91.77 |

This study and figure 3 show that, for various situations, the suggested model is able to increase precision during attack detection by 8.5% when compared with PR SUF [3], 4.5% when compared with PuF [9], and 6.5% when compared with DP AMI FL [23] for different scenarios.

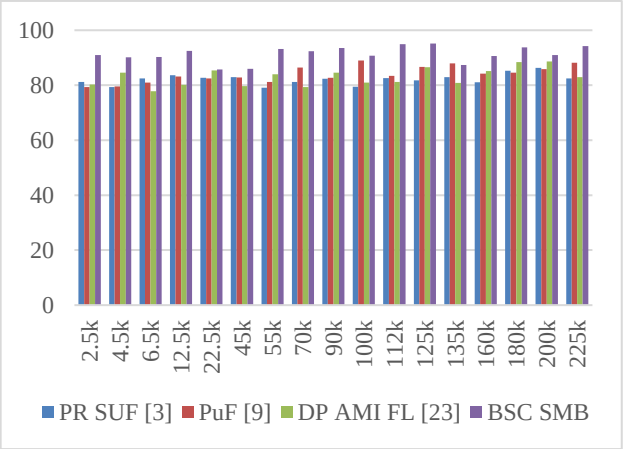


Figure 3. Attack classification precision under multiple real-time scenarios.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

This is because high privacy selected nodes and the GWTLbO Model, used in conjunction with extended GWO for variance-based feature set estimation, help to improve control efficacy for cyber-physical smart grids. Similar to that, table 3's recall values can be seen as follows,

Table 3. Attack classification recall under multiple real-time scenarios

| NC | R (%) PR SUF [3] | R (%) PuF [9] | R (%) DP AMI FL [23] | R (%) BSC SMB |
|---|---|---|---|---|
| 2.5k | 81.62 | 81.21 | 78.41 | 88.50 |
| 4.5k | 81.78 | 81.52 | 78.71 | 89.09 |
| 6.5k | 81.93 | 81.83 | 79.02 | 89.31 |
| 12.5k | 82.09 | 82.15 | 79.32 | 89.52 |
| 22.5k | 82.24 | 82.46 | 79.63 | 89.74 |
| 45k | 82.39 | 82.77 | 79.93 | 89.95 |
| 55k | 82.55 | 83.08 | 80.24 | 90.17 |
| 70k | 82.70 | 83.39 | 80.54 | 90.38 |
| 90k | 82.85 | 83.70 | 80.85 | 90.59 |
| 100k | 83.01 | 84.01 | 81.15 | 90.81 |
| 112k | 83.16 | 84.32 | 81.45 | 91.02 |
| 125k | 83.31 | 84.64 | 81.75 | 91.23 |
| 135k | 83.47 | 84.95 | 82.06 | 91.45 |
| 160k | 83.62 | 85.26 | 82.36 | 91.66 |
| 180k | 83.77 | 85.57 | 82.67 | 91.87 |
| 200k | 83.93 | 85.88 | 82.97 | 92.09 |
| 225k | 84.08 | 86.20 | 83.27 | 92.30 |

This study and figure 4 show that, for various situations, the suggested model is able to increase recall during the detection of assaults by 6.5% when compared with PR SUF [3], 4.3% when compared with PuF [9], and 8.5% when compared with DP AMI FL [23] for different use cases.

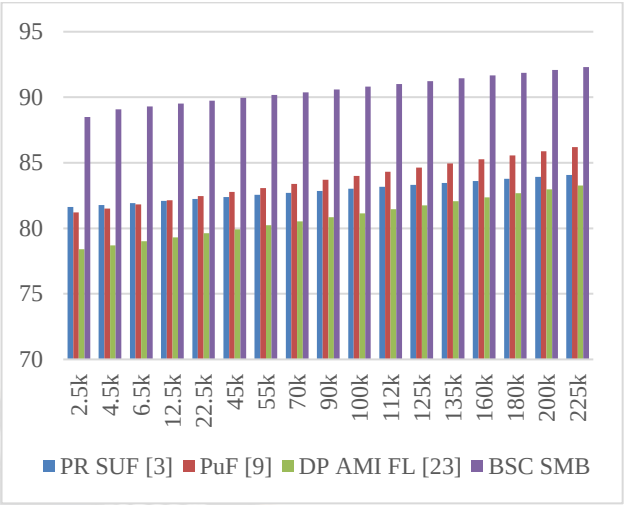


Figure 4. Attack classification recall under multiple real-time scenarios

This is because extended GWO is used to protect privacy and the GWTLbO Model to estimate variance-based feature sets, both of which help to improve the control effectiveness of cyber-physical smart networks. In a similar vein, table 4 shows the following delay in these attacks' identification,

Table 4. Delay needed to identify attacks and mitigate them for different scenarios

| NC | D (ms) PR SUF [3] | D (ms) PuF [9] | D (ms) DP AMI FL [23] | D (ms) BSC SMB |
|---|---|---|---|---|
| 2.5k | 64.28 | 64.68 | 65.05 | 45.50 |
| 4.5k | 64.40 | 64.93 | 65.30 | 48.25 |
| 6.5k | 64.52 | 65.18 | 65.56 | 48.37 |
| 12.5k | 64.64 | 65.43 | 65.81 | 48.49 |
| 22.5k | 64.76 | 65.68 | 66.07 | 48.61 |
| 45k | 64.89 | 65.93 | 66.33 | 48.73 |
| 55k | 65.01 | 66.18 | 66.58 | 48.86 |
| 70k | 65.13 | 66.43 | 66.84 | 49.07 |
| 90k | 65.25 | 66.69 | 67.09 | 49.49 |
| 100k | 65.37 | 66.94 | 67.35 | 49.96 |
| 112k | 65.49 | 67.19 | 67.60 | 50.51 |
| 125k | 65.61 | 67.44 | 67.86 | 51.04 |
| 135k | 65.73 | 67.69 | 68.11 | 51.48 |
| 160k | 65.85 | 67.94 | 68.36 | 51.85 |
| 180k | 65.98 | 68.19 | 68.62 | 52.05 |
| 200k | 66.10 | 68.44 | 68.87 | 52.20 |
| 225k | 66.22 | 68.69 | 70.55 | 52.32 |

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *25 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *24 October 2023*

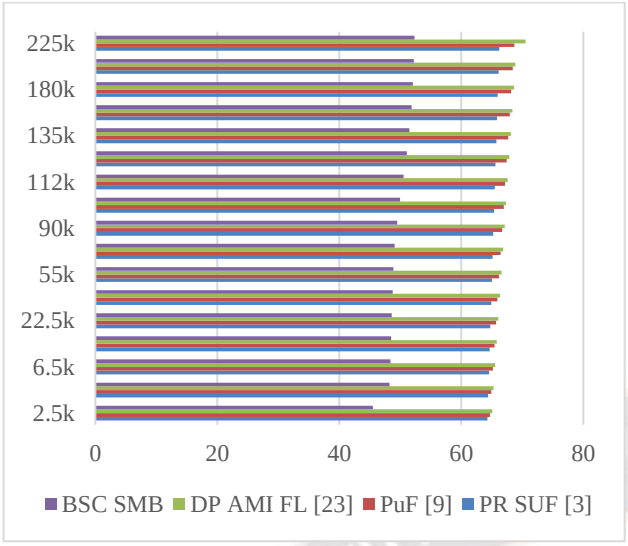


Figure 5. Delay needed to identify attacks and mitigate them for different scenarios

Based on this study and figure 5, it can be seen that the suggested model can increase categorization speed for various situations by 10.5%, 12.4%, and 19.5% when compared to PR SUF [3], PuF [9], and DP AMI FL [23]. This is a result of the use of extended GWO to choose delay-aware selected nodes, GWTLbO to choose adaptive features, and 1D CNN to help speed up categorization for cyber-physical smart networks. Based on this research, it can be seen that the suggested model can be used to identify a variety of attack patterns in a broad range of smart networks.

## V. DISCUSSION ON SELECTION OF GWTLbO OVER GWO & TLbO METHODS

The Grey Wolf Teacher Learner based Optimizer (GWTLbO) method has several advantages over the Grey Wolf Optimizer (GWO) and the Teacher Learner based Optimizer (TLbO) approaches separately.

GWTLbO combines the advantages of the GWO and TLbO algorithms, resulting in enhanced convergence properties. While TLbO exhibits rapid convergence, grey wolf foraging behavior serves as the model for GWO's exploratory abilities. GWTLbO can achieve a superior exploration/exploitation balance by combining these two techniques, accelerating convergence and increasing efficiency.

GWO searches the solution space by mimicking the search behavior of grey wolves, which has earned it a reputation for efficacy. However, local searches may be sluggish. In contrast, TLbO prioritizes regional research through a teaching-learning strategy. The combination of GWO and TLbO in GWTLbO enables a more thorough global exploration of the solution space as well as a faster and more efficient local search, resulting in improved overall optimization performance.

Adaptive Learning: GWTLbO is equipped with adaptive learning mechanisms that allow it to dynamically modify its search behavior in response to the issue. Due to its adaptability, GWTLbO can address a variety of optimization issues, such as CPS system security and privacy concerns. By modifying its learning method, GWTLbO is more adaptable than GWO and TbLO alone, as it can effectively manage a variety of attacks and threats.

Real-Time Threat Detection: GWTLbO differs from GWO and TLbO in that it has the ability to detect threats in real time. By combining the capabilities of GWO and TLbO, GWTLbO can rapidly detect and respond to hazards in real-time deployments. Due to security concerns, this is crucial for CPS systems that require immediate action to prevent potential intrusions. GWTLbO is well-suited for safeguarding CPS systems due to its rapid threat detection and response capabilities.

Protection of confidentiality: The GWTLbO takes contextual requirements for privacy protection in CPS systems into account. It selects the optimal privacy techniques (such as k-privacy, t-closeness, and l-diversity) based on the specific requirements of the system. This adaptable strategy raises the bar for privacy while taking into consideration the unique characteristics and circumstances of the CPS setting. Given that GWO and TLbO lack privacy protection mechanisms, GWTLbO is superior to them in terms of simultaneously addressing security and privacy concerns.

GWTLbO surpasses GWO and TLbO individually due to its enhanced convergence, global and local search capabilities, adaptive learning, real-time threat detection, and contextual privacy protection. By integrating the benefits of GWO and TLbO, GWTLbO provides a more comprehensive and efficient optimization framework for addressing security and privacy concerns in CPS systems.

## VI. CONCLUSION & FUTURE WORK

Using these machine learning algorithms, this paper improves the system's accuracy and effectiveness against heterogeneous attacks. Specifically, the system employs an unsupervised learning algorithm to identify new and unknown attacks and a supervised learning algorithm to train the model to recognize known attack patterns. In a variety of experiments, the efficacy of our proposed model was evaluated by utilizing real-time data samples from deployed IoT device sets. The deployed model assisted in the detection of buffer-level attacks, meter bypass, Flash image manipulation, and zero-day attacks. The results demonstrate that the proposed model detects and responds to attacks with a high degree of accuracy while maintaining low false-positive rates. Additionally, the proposed model is highly efficient and able to manage large amounts of data in real-time deployments. Overall, the proposed bio-inspired security and privacy model provides a solid, highly effective, and highly

scalable method for protecting CPS in a variety of scenarios. The combination of machine learning algorithms provides a potent tool for enhancing the security and privacy of these systems and has the potential to fundamentally alter how cybersecurity will be handled for future deployments. On a MATLAB Simulation with standard network configurations, the performance of the model was assessed. The simulator assisted in the deployment of real-time traffic scenarios and the injection of multiple attacks for each scenario. On the basis of this simulation strategy, nearly 10% of requests for individual communications were injected with attacks (including Zero-Day Attacks, Meter Bypass, Flash Image Manipulation, and Buffer-level attacks), and the performance of various techniques was compared. Based on this comparison, it can be seen that the proposed model is capable of increasing the accuracy of attack detection in various situations by 8.3% compared to PR SUF [3], 3.5% compared to PuF [9], and 6.0% compared to DP AMI FL [23]. This is due to the fact that the use of 1D CNN for categorization and the addition of multimodal characteristics enhances the accuracy of numerous cyber-physical attacks. This is also possible with the use of extended GWO, which increases anonymity levels for various use cases. All requests classified as "attacks" were immediately halted by the Smart Grid, and subsequent requests from the same IP addresses were forwarded to the requesting organisations. In terms of precision levels, it was observed that the proposed model can improve attack detection precision by 8.5% when compared to PR SUF [3], 4.5% when compared to PuF [9], and 6.5% when compared to DP AMI FL [23] for various scenarios.

While recall evaluation indicated that the proposed model can increase recall during the detection of assaults by 6.5% compared to PR SUF [3], 4.3% compared to PuF [9], and 8.5% compared to DP AMI FL [23] for various use cases. Compared to PR SUF [3], PuF [9], and DP AMI FL [23] in terms of delay, it was determined that the proposed model can increase categorization speed for various situations by 10.5%, 12.4%, and 19.5%. This is due to the utilization of extended GWO to select delay-aware selected nodes, GWTLbO to select adaptive features, and 1D CNN to accelerate categorization for cyber-physical smart networks. On the basis of this research, it is clear that the proposed model can be used to identify a variety of attack patterns in a wide variety of smart networks.

**REFERENCES**

[1] D. Sidhartha, L. Mahendra, K. Jagan Mohan, R. K. Senthil Kumar and B. S. Bindhumadhava, "Secure and Fault-tolerant Advanced Metering Infrastructure," 2020 IEEE International Conference on Power Systems Technology (POWERCON), Bangalore, India, 2020, pp. 1-6,

[2] H. Naseer, M. N. Mumtaz Bhutta and M. A. Alojail, "A Key Transport Protocol for Advance Metering Infrastructure (AMI) Based on Public Key Cryptography," 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2020, pp. 1-5

[3] P. Gope and B. Sikdar, "A Reconfigurable and Secure Firmware Updating Framework for Advanced Metering Infrastructure," 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, Singapore, 2022, pp. 453-459,

[4] O. Kebotogetse, R. Samikannu and A. Yahya, "A Concealed Based Approach for Secure Transmission in Advanced Metering Infrastructure," in IEEE Access, vol. 10, pp.

[5] S. M. Farooq, S. M. S. Hussain, T. S. Ustun and A. Iqbal, "Using ID-Based Authentication and Key Agreement Mechanism for Securing Communication in Advanced Metering Infrastructure," in IEEE Access, vol. 8, pp.

[6] M. Saffar and H. R. Naji, "Increasing the Security of Advanced Metering Infrastructure Using Dynamic Defense Methods," 2022 12th Smart Grid Conference (SGC), Kerman, Iran, Islamic Republic of, 2022, pp. 1-5,

[7] L. Yan, C. Ma, C. Wang, Z. Zhu, G. Wang and H. Wang, "A Differentially Private Data Transmission Scheme for Advanced Metering Infrastructures," 2021 IEEE International Conference on Progress in Informatics and Computing (PIC), Shanghai, China, 2021, pp. 340-344, doi: 10.1109/PIC53636.2021.9687013.

[8] V. S. M et al., "Internet of Things Based Smart Energy Meter with Fault Detection Feature Using MQTT Protocol," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1592-1596,

[9] B. Harishma et al., "Safe is the New Smart: PUF-Based Authentication for Load Modification-Resistant Smart Meters," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 663-680, 1 Jan.-Feb. 2022,

[10] Z. Zhongdong, C. Ziwen, Y. Jinfeng, Q. Bin and X. Yong, "Cloud Based Cyber Security Defense of Smart Meters," 2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Zhangjiajie, China, 2020, pp.

[11] G. P. Duggan, D. Zimmerle and S. Upadhyay, "Big Data Analytics for Power Distribution Systems using AMI and Open Source Tools," 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Chicago, IL, USA, 2020, pp. 1-5

[12] F. Ünal, A. Almalaq, S. Ekici and P. Glauner, "Big Data-Driven Detection of False Data Injection Attacks in Smart Meters," in IEEE Access, vol. 9, pp. 144313-144326, 2021,

[13] 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,

[14] Z. A. E. Houda, A. Hafid and L. Khoukhi, "Secure data storage Meets AMI: Towards Secure Advanced Metering Infrastructures," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6.

[15] C. Zhang, F. Luo, M. Sun and G. Ranzi, "Modeling and Defending Advanced Metering Infrastructure Subjected to Distributed Denial-of-Service Attacks," in IEEE Transactions on

Network Science and Engineering, vol. 8, no. 3, pp. 2106-2117, 1 July-Sept. 2021.

[16] S. Bhattacharjee and S. K. Das, "Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 356-371, 2021.

[17] S. Shukla, S. Thakur and J. G. Breslin, "Secure Communication in Smart Meters using Elliptic Curve Cryptography and Digital Signature Algorithm," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 261-266.

[18] F. Amsaad and S. Köse, "A Secure Hardware-Assisted AMI Authentication Scheme for Smart Cities," in IEEE Consumer Electronics Magazine, vol. 10, no. 4, pp. 106-112, 2021.

[19] D. A. Bashawyah and S. M. Qaisar, "Machine Learning Based Short-Term Load Forecasting for Smart Meter Energy Consumption Data in London Households," 2021 IEEE 12th International Conference on Electronics and Information Technologies (ELIT), Lviv, Ukraine, 2021, pp. 99-102.

[20] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues and M. Guizani, "Secure and Lightweight Authentication Scheme for Smart Metering Infrastructure in Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5

[21] S. Hu et al., "Provably secure ECC-Based Authentication and Key Agreement Scheme for Advanced Metering Infrastructure in Smart Grid," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3191319.

[22] A. S. M. Tayeen, M. Biswal and S. Misra, "DP-AMI-FL: Secure Framework for Machine Learning-based AMI Applications," 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2023, pp. 1-5,

[23] B. Matthias, M. Banka and R. Krzysztof, "Coordination of the islanding and resynchronisation process of microgrids through a smart meter gateway interface," CIRED 2020 Berlin Workshop (CIRED 2020), Online Conference, 2020,

[24] M. Abdul Majeed, N. Kumar Singh, L. Tak and V. Mahajan, "Detection of Stealthy Cyber Intrusion in Smart Electric Grid Using Advanced State Estimation," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2021, pp. 660-665.

[25] A. S. Sani, D. Yuan, W. Bao and Z. Y. Dong, "A Universally Composable Key Exchange Protocol for Advanced Metering Infrastructure in the Energy Internet," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 534-546, 2021.

[26] F. Amsaad and S. Köse, "A Trusted Authentication Scheme for IoT-based Smart Grid Applications," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-6.

[27] S. Zhang, Y. Zhang and B. Wang, "Antiquantum Privacy Protection Scheme in Advanced Metering Infrastructure of Smart Grid Based on Consortium Secure data storage and RLWE," in IEEE Systems Journal,

[28] A. Agrawal, K. Sethi and P. Bera, "IoT-Based Aggregate Smart Grid Energy Data Extraction using Image Recognition and Partial Homomorphic Encryption," 2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Hyderabad, 2021.

[29] S. Chai et al., "Provably Secure and Lightweight Authentication Key Agreement Scheme for Smart Meters," in IEEE Transactions on Smart Grid,

[30] A. A. Alqarni, "Security Threats in Cloud Computing Based Smart Grids and its Countermeasures," 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), Buldhana, India, 2020, pp. 1-5,

[31] N. Hudson, M. J. Hossain, M. Hosseinzadeh, H. Khamfroush, M. Rahnamay-Naeini and N. Ghani, "A Framework for Edge Intelligent Smart Distribution Grids via Federated Learning," 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 2021, pp. 1-9,

[32] M. Benmalek, Y. Challal, A. Derhab and Z. Gheid, "An Efficient Key Management Scheme for Secure Demand-Response Communications in Smart Grid," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/AECT47998.2020.9194168.

[33] M. Mohammadi, A. Kavousi-Fard, M. Dabbaghjamanesh, A. Farughian and A. Khosravi, "Effective Management of Energy Internet in Renewable Hybrid Microgrids: A Secured Data Driven Resilient Architecture," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, March 2022,

[34] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam and S. M. Mazinani, "A Secure and Efficient Key Establishment Scheme for Communications of Smart Meters and Service Providers in Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, March 2020

[35] . Marghescu, "Communications Systems in Smart Metering: A Concise Systematic Literature review," 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-9,

[36] X. -Y. Zhang, J. -R. Córdoba-Pachón, P. Guo, C. Watkins and S. Kuenzel, "Privacy-Preserving Federated Learning for Value-Added Service Model in Advanced Metering Infrastructure," in IEEE Transactions on Computational Social Systems, 2022.

[37] Nisha Balani, Pallavi Chavan, and Mangesh Ghonghe. 2022. Design of high-speed secure data storage-based sidechaining peer to peer communication protocol over 5G networks. Multimedia Tools Appl. 81, 25 (Oct 2022), 36699–36713.

[38] Chavan, P. V., & Balani, N. (2022). Design of heuristic model to improve block-chain-based sidechain configuration. In International Journal of Computational Science and Engineering (Vol. 1, Issue 1, p. 1). Inderscience Publishers. https://doi.org/10.1504/ijcse.2022.10050704