[1]Hailin Wang
[2]Jian Hu*
[3]Ying Yan
[4]Yuting Liu
[5]Yinglu Liao

Dual Attention Graph Convolutional Network optimized with the Sun Flower Optimization for Differential Privacy Protection Mechanism for Smart Grid against Security Attacks

Journal of Electrical Systems

Abstract: - A smart grid combines information and communication technology with the conventional power system to provide efficient and dependable electricity generation, transmission, distribution, and control. Utilities and users share information and electricity in a smart grid. This manuscript presents a Dual Attention Graph Convolutional Network (DAGCN) optimized with the Sun Flower Optimization Algorithm (SFO) predicting the differential privacy protection mechanism for smart grid (DPSG-DAGCN-SFO). Initially, the data is collected from NSL-KDD datasets. Afterward, the data is fed to an Adaptive Robust Cubature Kalman Filter (ARCKF) based preprocessing process. Then the preprocessed data's are fed to Adaptive and Concise Empirical Wavelet Transform (ACEWT)for extracting features such as authentication, integrity and trusted authority. The extracted features are fed to Dual Attention Graph Convolutional Network (DAGCN)to classify the privacy protection in smart grid such as stealthy attack and no attack. The weight parameters of DAGCN are optimized using SFO. The proposed DPSG-DAGCN-SFO is implemented in python, effectiveness assessed by several performance metrics such as accuracy, error rate, precision, sensitivity, F1-score and recall. The proposed method error rate attains 2% stealthy attack and4% no attack of the of the privacy protection in smart grid. The proposed method shows better results in all existing systems like Bayesian Clustering Algorithm (BCA), Self-Adaptive Grid-Partitioning Algorithm (SGNA) and Elliptic Curve Digital Signature Algorithm (ECDSA).From the result it is concludes that the proposed DPSG-DAGCN-SFO method based error rate lower than the existing methods.

Keywords: Application, Privacy protection, Sun Flower Optimization, Computation Time, Location Information, Energy Consumption Data.

I. INTRODUCTION

Cities' already overcrowded infrastructure and services face new challenges as a result of the population's rapid development, including waste management, resource overconsumption, traffic congestion, and rising energy costs [1,2]. The notion of "smart city" originated with technology, specifically the use of ICT to connect individuals, organizations, and governmental institutions. Smart buildings, smart infrastructure, smart transportation, smart infrastructure management, smart power and water distribution, smart healthcare, and smart services are all common features of smart cities [3, 4]. A smart city's smart grid (SG) is a crucial element [5]. Electricity generation, transmission, distribution, and control are made easier by an electrical system known as the "grid" [6]. SG is cognizant of all user actions, permits increased asset utilization, and offers a long-term sustainable power system [7]. With these qualities, it can effectively provide a low-loss, sustainable supply of electricity while upholding high standards of quality and security for a reliable power source. Reduction of carbon emissions has also been demonstrated by SG technology [8].

Security and privacy are the two biggest issues facing the future smart grid. Customers may experience power disruptions if the SG infrastructure does not have a sufficient security mechanism in place in case security concerns force the power system to shut down [9].In contemporary smart cities, a lack of energy can cause the collapse of routine daily activities such as the inability of online payment systems, the failure of heating systems, and many other things [10]. In terms of privacy, sharing client private data with criminal individuals might have a severe influence on their lives [11]. A significant amount of research has been conducted to improve the security of smart grid infrastructure. This paper looked at fault tolerance and secure data aggregation in SG [12]. One of Smart Grid technology's most notable features is its ability to support bidirectional connectivity, which, unlike the previous grid, enables the movement of energy-related data to and from hardware, software, and entities [13]. The SG collects and evaluates real-time data on electricity generation, transmission, and consumption through two-way communication. To collect and transmit data on electricity usage and other consumer information, SMs are installed at customer locations [14, 15].

[1,2,3,4,5]*Research Scholar, Information Center, Yunnan Power Grid Company Limited, Kunming, Yunnan, 650217, China*
*Corresponding author e-mail: csghujian@126.com

By enabling users to track their consumption and output, observe their periodic energy usage trends, and select from a variety of easily available power producing options, SG, as opposed to standard grid systems, fosters energy awareness [16]. The acquisition and administration of client private data creates security challenges connected to customer privacy. Private information about a consumer, such as lifestyle habits, the types of appliances they use, and daily activities, is thought to be revealed to attackers who may exploit it if their fine-grained data is not sufficiently secured by security and privacy measures [17, 18]. An insurance company may raise a customer's premium costs if their lifestyle is unhealthy. A marketing business can identify potential buyers for its products based on appliance usage habits [19]. Thieves might plan robberies based on their presence or absence. Privacy is extremely important to the average home user. Malicious users can discover routine behaviors, everyday activities, and other privacy-related information if metering data is submitted in plaintext [20].

The existing techniques of differential privacy protection mechanism for smart grid based methods affected from various issues of security attacks. By providing a novel method for differential privacy protection mechanism for smart grid using DAGCN optimized using the Sun Flower Optimization Algorithm (SFO), this research attempts to address the shortcomings of previous models.

A. Contribution Statement

- Predicting differential privacy protection mechanism for smart grid using DAGCN optimized with the Sun Flower Optimization Algorithm (SFO)
- The data's are gathered from the NSL-KDD datasets. Then the data's are fed to pre-processing.
- Using adaptive robust cubature Kalman filter eliminates the noise of input data in the pre-processing segment.
- The pre-processing output is fed into Adaptive and Concise Empirical Wavelet Transform for extracting texture features such as authentication, integrity and trusted authority.
- The extracted features are fed to Dual Attention Graph Convolutional Network, it classify the smart grid against the security attacks such as stealthy attack and no attack.
- The performance of the proposed approach is validated through python platform and compared with other existing techniques.
- Using the proposed DPSG-DAGCN-SFO approach, performance metrics such as recall, accuracy, precision, sensitivity, error rate, and F1-score are examined.

The following sections comprise the remainder of this manuscript: sector 2 looks at a survey of the works; sector 3 defines the suggested method; sector 4 demonstrations the findings and discussion; and sector 5 wraps up.

II. LITERATURE SURVEY

Numerous studies have previously been published in books related toprivacy protection in smart grid against security attacks, a certain recent works are divulged here,

Guan et al. [21] have suggested Optimizing asset utilization, enhancing customer satisfaction, and enhancing system stability and reliability are all possible with the smart grid. To further support the data-driven smart grid, using cluster analysis, other machine learning systems may be able to handle the enormous volumes of data produced by the smart grid. Private information, however, can be revealed as a consequence of cluster analysis. In this paper, a Differentially Private Clustering technique called IDPC which is based on the IGMM is proposed for performing privacy-preserving cluster analysis. The hybrid approach used by IDPC combines differential privacy with nonparametric Bayesian approaches. Nonparametric Bayesian approach, which permits some parameters to vary with the data, was often the foundation for clustering techniques without a fixed number of groups. To make IDPC differentially private, the data-release mechanism employed the Laplace approach. It demonstrates how create selectively private nonparametric Bayesian clustering using Laplace noise.

Liu et al. [22] have suggested data sharing among users, which offers a wealth of helpful information, was becoming increasingly important. Specifically, a significant quantity of location-based data has been produced with the increasing use of smart devices. Users must submit precise location information to guarantee that service providers can give the highest quality service possible. However, in that circumstance, the possibilities for privacy disclosure were limitless. People were interested in ways to protect private data using location information. The differential privacy theory solves this difficulty by providing clear definitions and quantitatively analyzed strategies for privacy protection; it was commonly employed in location-based

applications. A self-adjusting grid-partitioning method for noise augmentation that is based on differential privacy and offers more robust security for location data. The algorithm first divides the geographic two-dimensional data into uniform grids and Laplace noise with every grid having the same scale parameter. Next, the grid set that needs to be optimized is selected, and each grid has sound added to it in a recursive and adaptive way to lower its relative inaccuracy. Lastly, for every optimized grid, it partitions at a second level. First, this technique can inject noise adaptively based on the grid's determined count values.

Khan et al. [23] have developed the SG was a compute-intensive application that requires rigorous latency-aware capabilities and minimal delays. Meters collect data on electricity use, which may include private information about a person. Security and privacy were the two main issues facing the next generation of smart grids. However, in current years, research has focused on fog-enabled aggregation for SG communications that protects privacy. There was, however, a dearth of research on the need for fault tolerance, which permits data aggregation operations for operational SMs to go successfully and efficiently even in the face of malfunctioning meters. A secure, fail-tolerant, fog-enabled data aggregation method that protects privacy. The BGN cryptosystem was used to achieve metering data privacy, and the ECDSA was used for source authentication. Because of its reduced key size, the ECDSA generates signatures quickly and was appropriate for devices with limited resources, such as Advanced Metering Infrastructure (AMI).

Gough et al. [24] have introduced to delivers considerable benefits to both electricity merchants and distribution system operators, but raises serious concerns about consumer privacy. Data from customers' smart meters was safeguarded using a brand-new method that complies with Differential Privacy (DP). The consequences of this unique algorithm on distribution grid operation were thoroughly explored, not only in terms of customer electricity bills, but also in terms of power systems. With this method, the losses, power quality issues, and extra expenses that a privacy-preserving mechanism might bring to the system can be empirically investigated. To ensure that additional expenses were distributed among participants in a way that was effective, equitable, and fair, a number of cooperative game theory-based cost distribution procedures were employed.

Zuo et al. [25] have introduced In order to safeguard users' privacy in smart grids, Data aggregation applications are being used more frequently in order to satisfy the requirements of a multidimensional, fine-grained data investigation, privacy-preserving multidimensional data aggregation was an essential component. Contrarily, conventional multidimensional data aggregation methods depend on reliable sources and were exposed to coalition attacks from the control center (CC) and gateway (GW), which alarmed users about potential privacy violations. A distributed decryption method based on the ElGamal holomorphic cryptosystem that protects privacy smart grids' multidimensional data aggregation without the need for trusted authority and is resistant to a coalition attack by the GW and CC. The proposed plan lacked foundation in a reliable source, which in practice was not totally dependable. The thorough security analysis demonstrates that our plan satisfies the security specifications for a smart grid.

Guan et al. [26] have presented the data on power use was collected in order to maximize energy utilization. On the other hand, practical issues about communications security remain. A cost-effective smart grid aggregation solution and adaptive while maintaining privacy and authentication is needed to tackle these problems. Specifically, the suggested technique achieves great efficiency for data aggregation as well as data source authentication. In addition, the aggregation threshold was modified to accommodate the dynamic smart grid system by taking into account the time period and the energy consumption statistics of individual residential areas. This allows for fault tolerance to be maintained while ensuring the privacy of individual data during aggregation. Our solution can meet the required security requirements of the smart grid, as shown by a detailed security analysis.

Li et al. [27] have presented the smart grid's privacy-preserving data aggregation has been the subject of extensive research. But almost all systems in use today compile information on the overall amount of electricity used by all users, which occasionally falls short of the exact specifications established by a smart grid's control center. PPMA is a multi subset data aggregating technique for smart grids that protects privacy. Preserving the confidentiality of individual users, PPMA is able to compile statistics on clients' electricity use across a variety of ranges. Based on a comprehensive security analysis, PPMA can defend against a powerful attacker the privacy of individual customers' electricity usage.

III. PROPOSED METHODOLOGY

In this section, the privacy protection in smart grid against security attacks using DAGCN optimized with the sun flower optimization algorithm is discussed. The NSL-KDD datasets are the source of the input data at first. The data are then fed into preprocessing. Preprocessing involves removing noise using adaptive robust cubature Kalman filtering. After that, the preprocessing output is given into the compact and adaptable empirical wavelet transform for feature extraction, including authentication, integrity and trusted authority. The smart grid is then categorized using DAGCN in order to protect it from security threats including stealthy attacks and non-attacks. Using SFO, the weight parameters of DAGCN are tuned. The block diagram of DPSG-DAGCN-SFO technique is presented in Fig 1.The detail description of proposed methodology are given below,

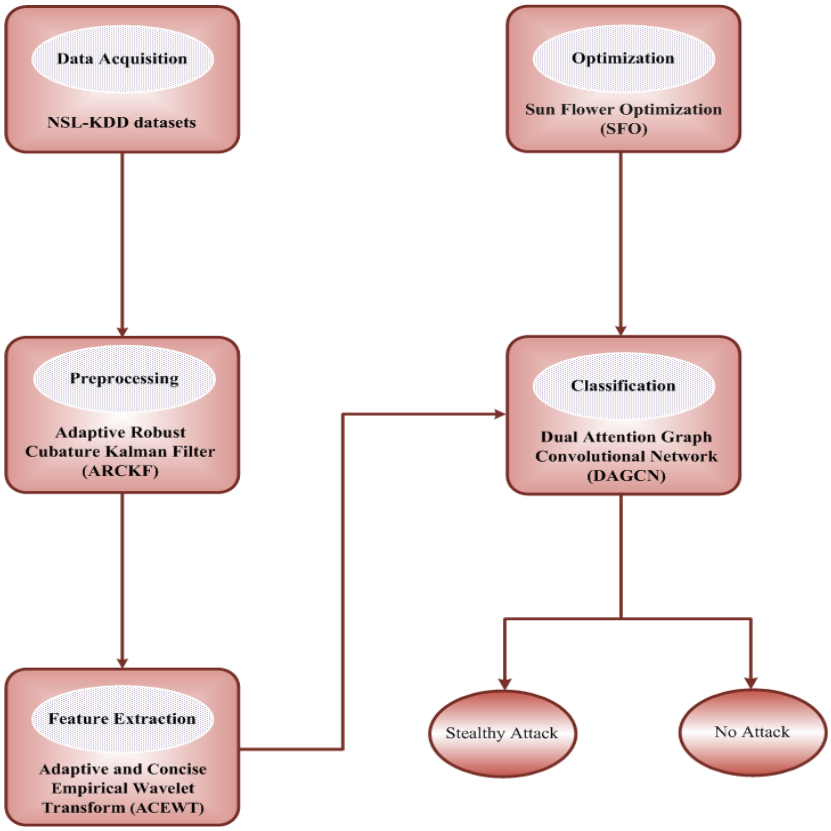

Fig 1: Block diagram of DPSG-DAGCN-SFO method

A. Data Acquisition

The NSL-KDD datasets are the source of the smart grid security attack-based data, which included 21 projected label records with 41 attributes for assaults and normal [28]. For every feature, there exist three distinct sorts of attribute values: normal, binary, and numeric. The four categories of attack types were DoS, Probing, U2R, and R2L. The popular KDD'99 test set has roughly 75% fewer redundant records than NSL-KDD, and it has a large enough training set with attack-type labels and difficulty levels. There are 125,973 records in the training set totaling attacks and normal, and 22,544 records in the testing set totaling both types of data. There were a total of 24 different types of assaults, despite not coming from the training data's same probability distribution, 14 of them were present in the testing data. Because new assaults are assumed to be variations of old attacks, this increases the task's realism because it only takes the signature of known attacks to recognize novel variants.

B. Pre-processing using Adaptive Robust Cubature Kalman Filtering

In this phase, adaptive robust cubature kalman filter (ARCKF)pre-processes the input data, it is employed to reduce noise in the input data and enhance the data's purity [29]. A measurement and system noise-free ARCKF that can lessen the negative consequences of observation outliers and innovation. To modify the state estimation error covariance matrix according to various conditions, a versatile approach is created.

The corresponding error covariance matrix for state estimation is given, which enables the cubature point generation to produce cubature points that represent the statistical features. Formally, get

$$Y_{i,k-1} = \hat{y}_{k-1} + \xi_i \sqrt{\hat{Q}_{k-1}}, \qquad i = 1,\ldots\ldots,2n \tag{1}$$

In this case, ξ_i represents the basic data point set's ith column, $\sqrt{(.)}$ stands for the cholesky decomposition operation, n stands for the dimension of state variables, and $Y_{i,k-1}$ is indicated as the ith cubature point of $\hat{y}_{k-1}$.

To instantiate the cubature points, one uses the state transition function. Next, the corresponding state error covariance and the anticipated state can be computed as

$$Y_{i,k}^{*} = f\left(Y_{i,k-1}, u_{k-1}\right), \; i = 1, \ldots\ldots, \; 2n \tag{2}$$

$$\tilde{y}_k = \frac{1}{2n}\sum_{i=1}^{2n} Y_{i,k}^{*} \tag{3}$$

$$\tilde{Q}_k = \frac{1}{2n}\sum_{i=1}^{2n} Y_{i,k}^{*}\left(Y_{i,k}^{*}\right)^{T} - \tilde{y}_k \tilde{y}_k^{T} + P_{k-1} \tag{4}$$

Where, $Y_{i,k}^{*}$ is denoted as the modified points of cubature, $\tilde{y}_k$ is denoted as the predicted state, $\tilde{Q}_k$ is denoted as the associated covariance of errors, the superscript T is denoted as the matrix transpose operation.

The correspondence between the actual state and the expected state is used to build the batch-mode regression form.

$$\tilde{y}_k = y_k - \eta_k \tag{5}$$

Where, η_k is denoted as the prediction error.

Furthermore, the following can be obtained by using the statistical linearization technique on the measurement function.

$$x_k = H_k\left(y_k - \tilde{y}_k\right) + h\left(\tilde{y}_k\right) + v_k \tag{6}$$

Where, $H_k\left(Q_{xy,k}\right)^{T}\left(\tilde{Q}_k\right)^{-1}$ is denoted as the statistical regression matrix.

The compact form of the above both equations are given below:

$$\tilde{y}_k = \tilde{H}_k y_k + \tilde{e}_k \tag{7}$$

The following is the derivation of the covariance matrix $\tilde{e}_k$:

$$\sum\nolimits_k = \mathrm{E}\left[\tilde{e}_k \tilde{e}_k^{T}\right] = S_k S_k^{T} \tag{8}$$

Where S_k is calculable by the Cholesky decomposition technique or the UD factorization.

Both the prediction state vector and the innovation vector need to be created in a two-dimensional matrix Z in order to perform outlier detection and down-weighting.

$$Z_k = \begin{bmatrix} x_{k-1} - h\left(\tilde{y}_k - 1\right) & x_k - h\left(\tilde{y}_k\right) \\ \tilde{y}_k - 1 & \tilde{y}_k \end{bmatrix} \tag{9}$$

Where, the superscripts k and $k-1$ are denoted as the instants of time; $x_{k-1} - h\left(\tilde{y}_k - 1\right)$ and $x_k - h\left(\tilde{y}_k\right)$ are denoted as the innovation vector at time instant $k-1$ and k; $\tilde{y}_k - 1$ and $\tilde{y}_k$ are denoted as the prediction state.

By applying the total influence function technique, one can create and update the estimate error covariance matrix in the following ways to improve the proposed method's resilience against outliers.

$$\tilde{Q}_k = \begin{cases} \tilde{Q}_k - K_k Q_{yy,k} K_k^{T} & if \;\; \max\left(PS_i\right) \le \chi^2_{2,(.0975)} \\ \mu\left(C_k^{T} C_k\right)^{-1}\left(C_k^{T} \Omega_{\varpi} C_k\right)\left(C_k^{T} C_k\right)^{-1}, & otherwise \end{cases} \tag{10}$$

Where, $\tilde{Q}_k$ is denoted as the time-instant state prediction error covariance matrix, $\chi^2_{2,(.)}$ is denoted as the distribution of chi-squares with two degrees of freedom; $\chi^2_{2,(.0975)}$ is denoted as the value of $\chi^2_{2,(.)}$, $Q_{yy,k}$ is denoted as the predicted measurement's covariance matrix, and K_k is denoted as the Kalman gain that is calculated as

$$Q_{yy,k} = \frac{1}{2n}\sum X_{i,k} X_{i,k}^{T} - \tilde{x}_k \tilde{x}_k^{T} + R_k \tag{11}$$

$$K_k = Q_{xy,k} Q_{yy,k}^{-1} \tag{12}$$

Thus, the noise in the input data is eliminated by this procedure. Finally, the pre-processed output is given towards feature extraction.

C. Feature Extraction using Adaptive and Concise Empirical Wavelet Transform (ACEWT)

This section involves applying the ACEWT on the pre-processed data in order to extract features.

The scale-space representation is the division of the Fourier spectrum by the original EWT method. EWT is capable of effectively separating various components in noise-free signals [30]. However, avoiding noise is challenging. EWT is complicated by the fact that the signals are typically non-stationary. The size of the sampling frequency is often proportional to the displayed Fourier spectrum. As the sample frequency rises, more information about the signal is revealed. Similarly, more work in the scale-space representation would be required for a more complex signal. In this section, the distribution of components is displayed using PSD rather than the complex Fourier spectrum.

In actuality, PSD depicts the power distribution with frequency. The signal's Fourier transform $y(f)$ is $\hat{y}(f)$, and its mean power p also be written as follows:

$$p = \lim_{t\to\infty} \frac{1}{2T} \int_{-T}^{T} y(t)^2 \, dt \tag{13}$$

Assuming that the signal's Fourier transform in the range0 to T:

$$\hat{y}_T(f) = \frac{1}{\sqrt{T}} \int_{0}^{T} y(t) e^{-i2\pi ft} dt \tag{14}$$

Thus, we define the power spectral density as

$$S_{yy}(f) = \lim_{T\to\infty} E\left[\left|\hat{y}_T(f)\right|^2\right] \tag{15}$$

An integer with a positive value greater than zero that symbolizes a spectrum that varies in frequency. How the PSD and the spectrum's fluctuation tendency relate is demonstrated by a number of simulated signal sets. The resulting new signal conceals its modulation parameters and information about periodic pulses.

$f_1 = 10Hz, f_2 = 100Hz$ is the modulation signal, which is the first part. The cosine, or $f_3 = 400Hz$, is the second element. The third component consists of the periodic pulses. The following parameters of the pulse are known: sampling frequency ($f_s = 10000Hz$), damping coefficient (g = 0.02), repetition time $T = 0.03s$, and natural frequency (fn = 1600 Hz). The created new signal masks its modulation properties and periodic pulse information.

$$\begin{cases} S_{c1} = 3\cos(2\pi.f_1 t) \times \cos(2\pi.f_2 t) \\ S_{c2} = 3\cos(2\pi.f_3 t) \\ Sc_3 = \sum_{i=1}^{M} 4e^{-g\times 2\pi ft} \times \sin\left(2\pi ft \times \sqrt{1-g^2}\right) \\ S_1 = S_{c1} + S_{c2} + S_{c3} \end{cases} \tag{16}$$

There are three parts to the simulated signal. When the cosine and modulation signals are merged to form a single signal, the resultant signal's Fourier spectrum shows a significant amplitude in two frequency regions at about 1000 Hz. The Fourier spectrum of the third component has a concentration of energy at about 1600 Hz. The signal's Fourier spectrum, which has three components superimposed, exhibits a similar circumstance.

The extracted features are authentication, integrity and trusted authority. Following extraction, the result is sent to the classification stage.

D. Classification using Dual Attention Graph Convolutional Network (DAGCN)

Classification of privacy protection of smart grid against security attacks utilizing DAGCN was discussed in this section [31].The three parts of the DAGCN are the fully connected classifier, the self-attention pooling layer, and the attention graph convolution module. This section addresses the issue with typical GCNs first, and

then suggests our self-attention pooling layer and attention graph convolution module. The system dynamics can be calculated in Eqn (17)

$$W^{j+1} = \phi(\tilde{V}\tilde{D}^{-1}W^{j}U) \tag{17}$$

Where $\tilde{V}\tilde{D}^{-1}$ is the graph structure that has been normalized, $\tilde{D}$ is indicated as the diagonal node degree matrix of $\tilde{V}$, U is represent as the model parameter to be trained, and $\tilde{V} = V + I_m$ is indicated as the self-connection adjacency matrix for every node. W^j becomes a node attributes vector containing j-hop local structure information after this procedure is applied j times.

With the exception of W^j, the outcome of each step in the recurrence of Eqn (17) can only be utilized to produce the subsequent convolution result. Our AGC layer's main goal is to improve the model so that it may take useful information from each hop in addition to relying just on the k-hop convolution result. The key data derived from multiple hop convolution procedures will be included in a hierarchical representation that is the convolution output as a consequence. Display the attention behavior and use Eqn (17) to create the hierarchical node representation of γ_{s_m} that is shown below:

$$\gamma_{s_m} = \sum_{k=1}^{j} \alpha_{ki} W_{s_m}^{j} \tag{18}$$

Using vanilla attention, you can easily ascertain the significance of the aggregate outcome of each hop, where $W_{s_m}^{j}$ stands for node s_m local structure in j -hops and α is the attention weight. The information about the hierarchical structure is contained in the final node representation.

$$\gamma_{s_m}^{n+1} = \sum_{k=1}^{j} \alpha_k W_{s_m}^{j} \tag{19}$$

$$W_{s_m}^{0} = \gamma_{s_m}^{n} + Y \tag{20}$$

Stack m attention convolution layers using the Residual Learning technique, then build a convolutional attention graph module to obtain a better final γ_{s_m} node representation in order to optimize the benefits of deep learning and uncover more hidden features. Each AGC layer receives as input the total of the output from the layer before it and the initial Y.

$$\gamma_{s_m} = Dense\ (\{\gamma_{s_m}^{0}, \gamma_{s_m}^{1}, ..., \gamma_{s_m}^{n}\}, \theta) \tag{21}$$

Where, a dense layer is created by combining the outputs of each attention graph convolution layer called $Dense\ ()$. For all vertices $s \in Q$, the node representation is now γ. For ease of understanding, represent the graph as a matrix Q with a size of m by c, where a node is represented by each row.

$$Q = \left(\gamma_{s_1}, \gamma_{s_2}, \ldots, \gamma_{s_m}\right) \tag{22}$$

Utilize the attention method to produce the weights vector α by using the convolution module's learned graph node representation as the input.

$$\beta = soft\max(\ h_2 \tan w(h_1 Q^T)) \tag{23}$$

The weight matrices h_1 and h_2 have the c-by-c and c-by-r shapes, correspondingly, and r is denoted as a hyper-parameter that determines how many subspaces are needed to understand the node representation and the graph representation. When $r \geq 1, \alpha$ stops being a vector and turns into a weight matrix.

Graph representation matrix: the total matrix yields a complete representation of the graph, and each row represents a graph in a single sub-space. Finally, G is used as the input for a fully-connected layer and a $soft\max$ layer to complete the graph categorization.

$$X = soft\max(ZG + C) \tag{24}$$

Where, the second input dimension is used to conduct the $soft\max$ function.

The optimal input is predicted by proposed DAGCN technique. Finally, the DAGCN classifies the stealthy attack and no attack of the security attack.

E. Optimization using Sun Flower Optimization (SFO)

The ideal parameters of the DAGCN classifier are optimized using the Sunflower optimization method (SFO) [32]. A model inspired by nature, the SFO replicates the process of pollination between the two nearest sunflowers as they get closer to the sun. The features and key steps of the SFO algorithm are covered in the next subsection. A sunflower's cycle is consistent: every day, they awaken and follow the sun like clockwork. At night, they journey in the other way, waiting for their departure the next morning. Flower pollination is the process by which flowering plants reproduce biologically. The writers consider sunflowers' unusual behavior while determining the best orientation to the sun. The flowchart of SFO algorithm is displayed in Fig 2.

Step 1: Initialization

Set the inputs' initial values. In this case, the input parameters are the DAGCN weight parameter, which is indicated as β .

Step 2: Random Generation

Once everything is set up, the random vectors produce the input parameters at random.

$$N=\begin{bmatrix} N_{1,1} & N_{1,2} & \cdots & N_{1,p} \\ N_{2,1} & N_{2,2} & \cdots & N_{2,p} \\ \cdots & \cdots & \cdots & \cdots \\ N_{m,1} & N_{m,2} & \cdots & N_{m,p} \end{bmatrix} \tag{25}$$

Where, m is indicated as rate of molarity, N signified as the population size and p indicate as the rate of pollination.

Step 3: Fitness Calculation

The fitness is selected based on the objective function.

$$F=Optimize\ (\beta) \tag{26}$$

Step 4: Natural Behaviors

The sunflowers face the sun each morning, and this allows the pollination process to happen between the nearest two sunflowers X_i and X_{i+1}. Each sunflower absorbs radiation from the sun. Each sunflower's position in relation to the sun determines the total amount of radiation it receives.

The sunflowers absorb less radiation (heat) from the sun as their distance increases. The following diagram illustrates how much heat each sunflower receives from the sun:

$$Q_i=\frac{W}{4\pi c^2} \tag{27}$$

Here, W is indicated as the sun power, Q_i is denoted as the amount of the received heat and c is represent as the separation of the optimal solution (the sun) X_i and the sunflower X_i.

Step 5: Orientation Adjustment Process

Sunflower orientation vectors are computed as shown in

$$\vec{S}_i=\frac{X^*-X_i}{\left\|X^*-X_i\right\|} \quad i=1,2,\ldots,N \tag{28}$$

Here, X^* is represent as the most effective worldwide solution, X_i is solution i , and N is indicated as the population size.

Step 6: Step Size of the Sunflower toward the Sun

Each sunflower Xi's stride size toward the sun is computed as indicated in

$$d_i=\alpha\times P_i\left(\left\|X_i+X_{i-1}\right\|\times\left\|X_i+X_{i-1}\right\|\right) \tag{29}$$

Here, α represents the inertial displacement of the sunflower, $P_i\left(\left\|X_i+X_{i-1}\right\|\right)$ is indicated as the probability of pollination between X_i and X_{i+1}, the closest two sunflowers. Sunflowers closer to the sun take fewer steps to adjust their placements (exploitation process), but sunflowers further away move at random (exploration process). For every solution, there is a maximum step size for all sunflowers to prevent skipping from the border. Each sunflower's maximum step size is calculated as follows:

$$d_{\max} = \frac{\left\| X_{\max} - X_{\min} \right\|}{2 \times N} \tag{30}$$

Where, $X_{\max}$ is indicated as the upper bound, $X_{\min}$ is denoted as the lower bound, and N is represent as the population size.

Step 7: Fertilization Process

The finest sunflowers will create new ones by fertilizing the area around the sun. Each sunflower's fertilization process can be illustrated as follows:

$$X_{i+1} = X_i + d_i \times \vec{S}_i \tag{31}$$

Here, X_{i+1} is denoted as new generated sunflower.

Step 8: Update Best Solution

As may be seen in, the solutions adjust their position in response to Levy's flight operator.

$$X_{i+1} = X_i + levy(v) \times \vec{S}_i \tag{32}$$

Where $levy(v)$ is indicated as the levy distribution.

Step 9: Termination

Verify the termination criteria; if it is met, the best possible solution has been found; if not, repeat the procedure.

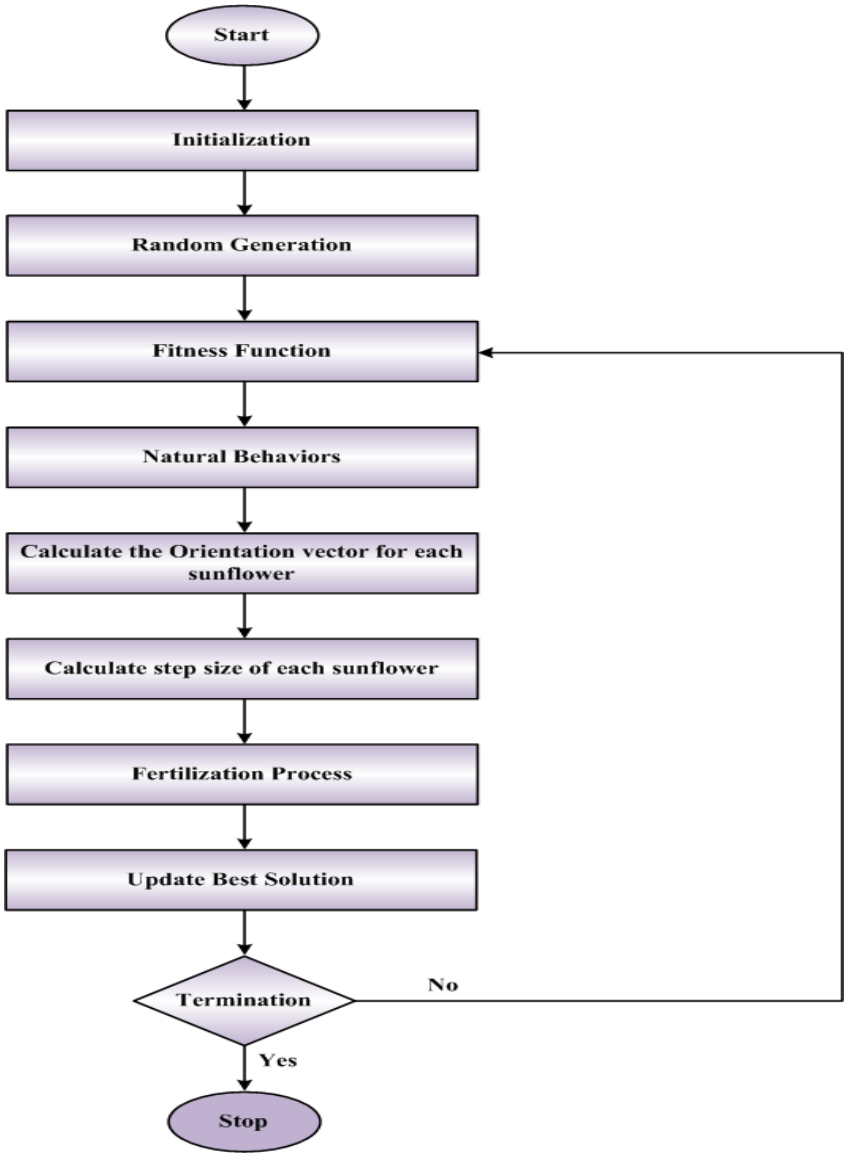

Fig 2: Flowchart of SFO algorithm

IV. RESULT & DISCUSSION

The result of proposed DAGCN optimized with the Sun Flower Optimization Algorithm (SFO) predicting the differential privacy protection mechanism for smart grid (DPSG-DAGCN-SFO) is discussed. By using a Python platform, the proposed approach's performance is verified and contrasted with that of alternative methods already in use. The obtained results of the proposed with DPSG-DAGCN-SFO technique are evaluated with existing techniques like DPSG-BCA, DPSG-SGNA and DPSG-ECDSA methods.

A. Performance Measures

Performance indicators such as accuracy, F1-score, precision, recall, error rate, and sensitivity are calculated in order to assess the performance.

1) Accuracy

Accuracy is defined as the ratio of a precise forecast to the entire number of proceedings in the dataset. The following formula (33) is used to compute accuracy.

$$Accuracy = \frac{(T_P + T_N)}{(T_P + F_P + T_N + F_N)} \tag{33}$$

2) Error Rate

The proportion of misclassification is assessed using error. Error rate is calculated using equation (34)

$$Error = 100 - accuracy \tag{34}$$

3) F1-Score

It evaluates the precision of the model on the dataset. It is determined by equation (35)

$$F1Score = \frac{T_P}{\left(T_P + \frac{1}{2}\left[F_P + F_N\right]\right)} \tag{35}$$

4) Precision

Precision is the positive predict value. Precision is compute by following equation (36)

$$\Pr ecison = \frac{T_P}{T_P + F_P} \tag{36}$$

5) Recall

The ratio of accurate positive predictions to all actual positive samples both those that were correctly and mistakenly forecasted as positive is known as recall. The recall formula is presented in equation (37)

$$\mathrm{Re}call = \frac{T_P}{T_P + F_N} \tag{37}$$

6) Sensitivity

Sensitivity is calculated using the following equation (38)

$$Sensitivity = \frac{T_P}{T_P + F_N} \tag{38}$$

B. Performance Analysis

The simulation results of proposed DPSG-DAGCN-SFO method shows in Fig 3 to 8.Then the proposed DPSG-DAGCN-SFO method is likened with existing systems like DPSG-BCA, DPSG-SGNA and DPSG-ECDSA correspondingly. In order to show the effectiveness of the proposed DAGCN classifier with optimization SFO algorithm, evaluation experiment was carried and the results.

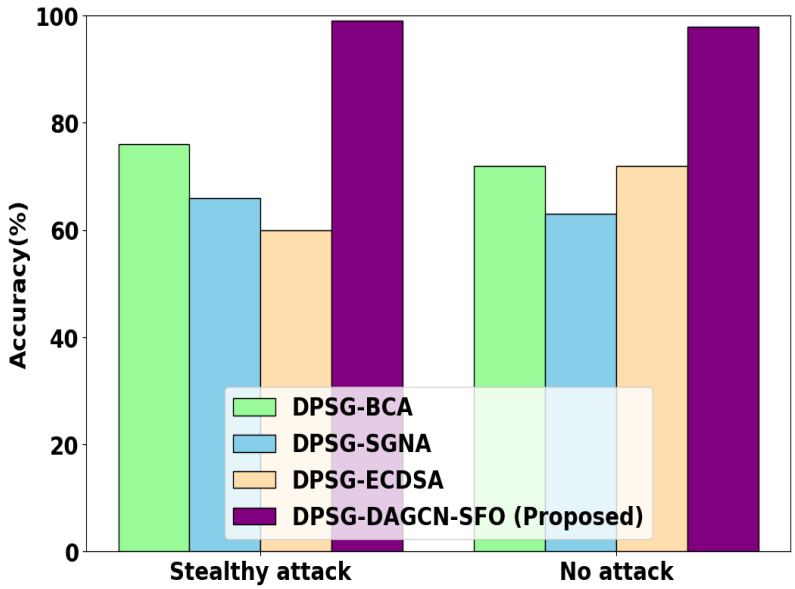

Fig 3: Performance analysis of accuracy

The performance analysis of accuracy is shown in Fig 3.The performance accuracy of different models or approaches used to analyze the privacy protection of smart grid against security attacks. The proposed DPSG-DAGCN-SFO technique of accuracy are 99% stealthy attack and 97% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of accuracy attains 77%, 67%, 60% stealthy attack and 78%, 60%, 70% no attack. The proposed DPSG-DAGCN-SFO method shows higher accuracy compared with other existing methods.

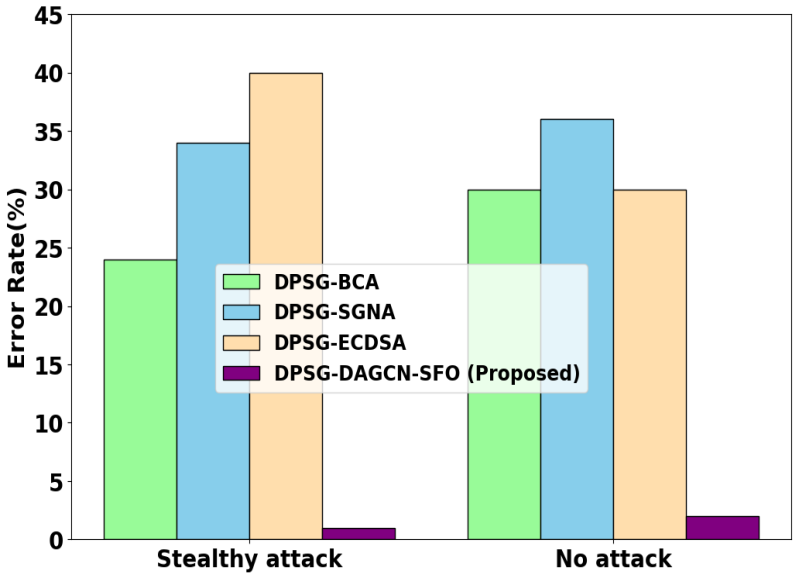

Fig 4: Error rate analysis using proposed and existing methods

The error rate analysis using proposed and existing methods is presented in Fig 4.The proposed DPSG-DAGCN-SFO method error rate are 2% stealthy attack and 4% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of error rate attains 24%, 34%, 40% stealthy attack and 30%, 35%, 30% no attack. The proposed DPSG-DAGCN-SFO method shows lower error rate compared with other existing methods.

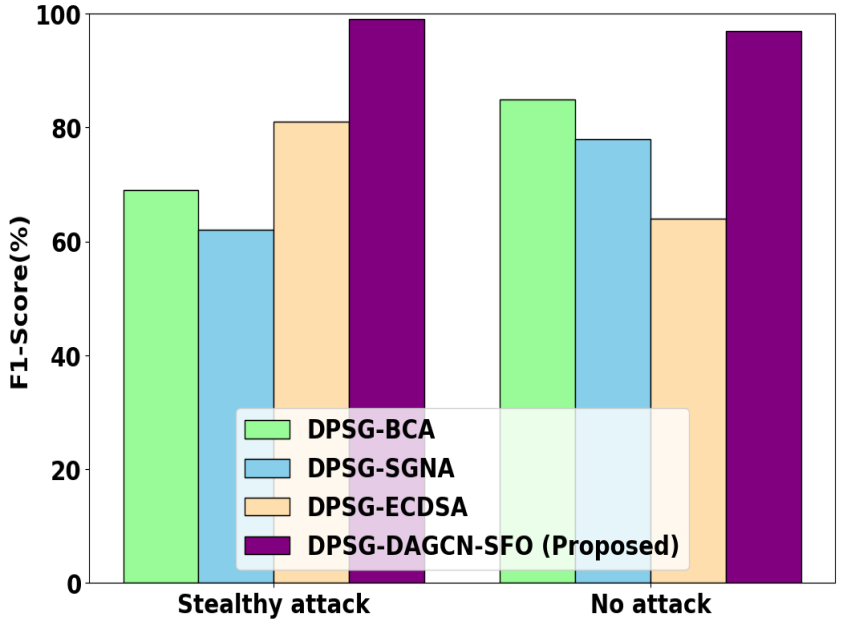

Fig 5:F1-score performance analysis using proposed and existing techniques

The F1-score performance analysis using proposed and existing techniques is presented in Fig 5. The proposed DPSG-DAGCN-SFO technique of F1-score are 99% stealthy attack and 97% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of F1-score attains 70%, 60%, 80% stealthy attack and 82%, 78%, 60% no attack. The proposed DPSG-DAGCN-SFO method shows higher F1-score compared with other existing methods.

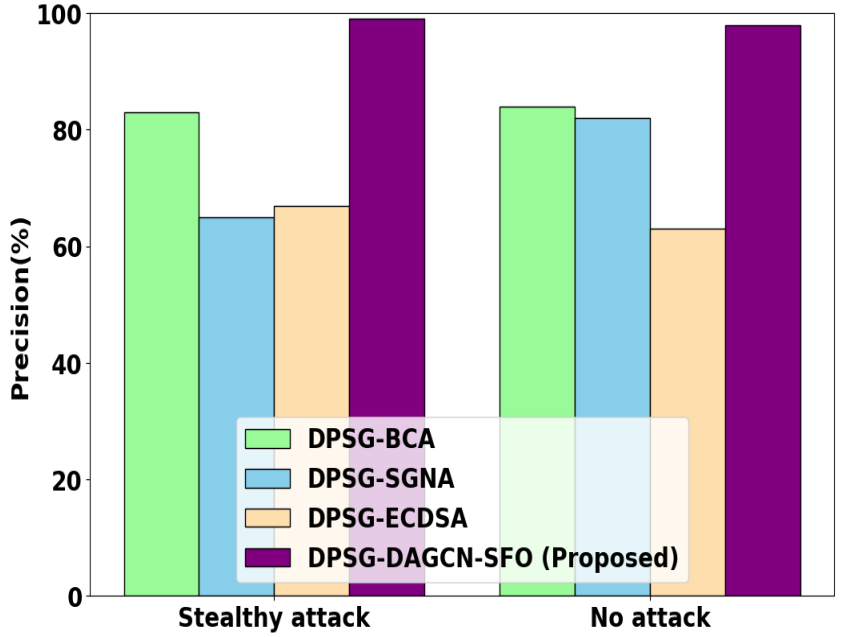

Fig 6: Comparison of the proposed and existing methods' precision

The comparison of the proposed and existing methods' precision is presented in Fig 6.The proposed DPSG-DAGCN-SFO technique of precision are 99% stealthy attack and 98% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of precision attains 83%, 65%, 68% stealthy attack and 84%, 82%, 60% no attack. The proposed DPSG-DAGCN-SFO method shows higher precision compared with other existing methods.

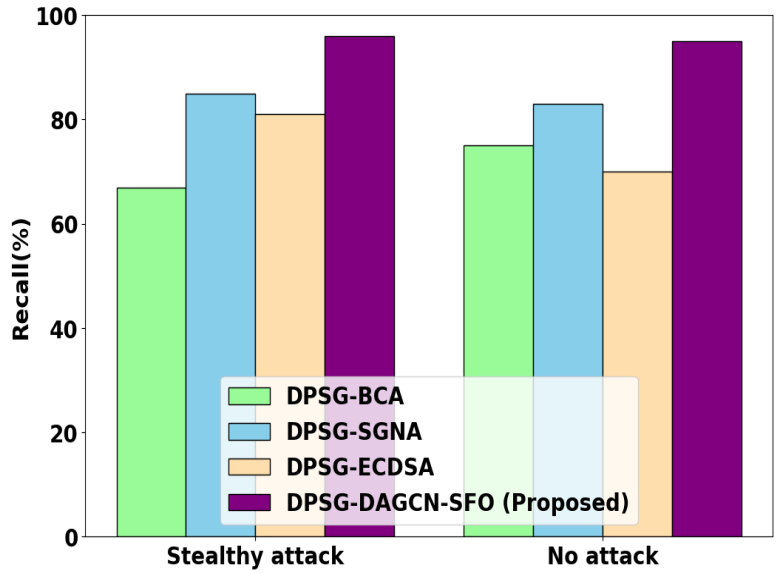

Fig 7: Recall comparison between the proposed and existing methods

The recall comparison between the proposed and existing methods is presented in Fig 7. The proposed DPSG-DAGCN-SFO technique of recall are 97% stealthy attack and 96% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of recall attains 69%, 83%, 80% stealthy attack and 70%, 80%, 69% no attack. The proposed DPSG-DAGCN-SFO method shows higher recall compared with other existing methods.

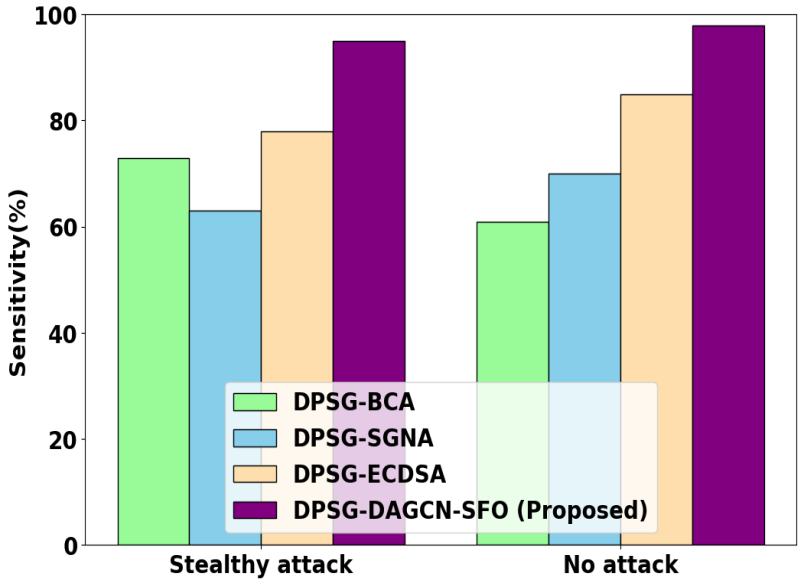

Fig 8: Sensitivity performance analysis using proposed and existing methods

The sensitivity performance analysis using proposed and existing methods is presented in Fig 8. The proposed DPSG-DAGCN-SFO technique of sensitivity are 96% stealthy attack and 98% no attack. The existing methods DPSG-BCA, DPSG-SGNA and DPSG-ECDSA method of sensitivity attains 75%, 60%, 79% stealthy attack and 60%, 70%, 80% no attack. The proposed DPSG-DAGCN-SFO method shows higher sensitivity compared with other existing methods.

V. CONCLUSION

In this section, differential privacy protection in smart grid and its application using DPSG-DAGCN-SFO method was successfully implemented for classifying stealthy attack and no attack of the network security of the grid. The proposed DPSG-DAGCN-SFO method is executed in the python platform utilizing the dataset of NSL-KDD datasets. The DPSG-DAGCN-SFO method's performance is comprised of the following: sensitivity, F1-score, accuracy, precision, recall, and error rate. The proposed DPSG-DAGCN-SFO method attains 99% and 97%, higher accuracy for network security of the grid, respectively. The proposed DPSG-DAGCN-SFO method attains99%, and 97% higher F1-score of network security of the grid, respectively. The proposed

DPSG-DAGCN-SFO method attains2% and 4% lower error rate of network security of the grid. The proposed DPSG-DAGCN-SFO method attains 98% and 98% higher precision of network security of the grid, respectively. The proposed DPSG-DAGCN-SFO method attains97%, and 96% higher recall of network security of the grid, respectively. The proposed DPSG-DAGCN-SFO method attains96% and 98% higher specificity of network security of the grid, respectively. The performance of the proposed DPSG-DAGCN-SFO method is compared with the existing methods such as DPSG-BCA, DPSG-SGNA and DPSG-ECDSA.

REFERENCES

[1] Desai, S., Alhadad, R., Chilamkurti, N., & Mahmood, A. (2019). A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure. *Cluster Computing*, *22*, 43-69.

[2] Fan, W., He, J., Guo, M., Li, P., Han, Z., & Wang, R. (2020). Privacy preserving classification on local differential privacy in data centers. *Journal of Parallel and Distributed Computing*, *135*, 70-82.

[3] Yilmaz, I., Kapoor, K., Siraj, A., & Abouyoussef, M. (2021, April). Privacy protection of grid users data with blockchain and adversarial machine learning. In *proceedings of the 2021 ACM workshop on secure and trustworthy cyber-physical systems* (pp. 33-38).

[4] Ashraf, M. M., Waqas, M., Abbas, G., Baker, T., Abbas, Z. H., & Alasmary, H. (2022). Feddp: A privacy-protecting theft detection scheme in smart grids using federated learning. *Energies*, *15*(17), 6241.

[5] Dawood, B. A., Al-Turjman, F., Hussain, A. A., & Deebak, B. D. (2022). Data protection and privacy preservation mechanisms for applications of IoT in smart grids using AI. In *Sustainable Networks in Smart Grid* (pp. 207-231). Academic Press.

[6] Mirzaee, P. H., Shojafar, M., Cruickshank, H., & Tafazolli, R. (2022). Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). *IEEE access*, *10*, 52922-52954.

[7] Wen, M., Xie, R., Lu, K., Wang, L., & Zhang, K. (2021). Feddetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. *IEEE Internet of Things Journal*, *9*(8), 6069-6080.

[8] Abdulaal, M. J., Mahmoud, M., Bello, S. A., Khalid, J., Aljohani, A. J., Milyani, A. H., ... & Ibrahem, M. I. (2023). Privacy-preserving detection of power theft in smart grid change and transmit (cat) advanced metering infrastructure. *IEEE Access*.

[9] Gope, P., Sharma, P. K., & Sikdar, B. (2022). An ultra-lightweight data-aggregation scheme with deep learning security for smart grid. *IEEE Wireless Communications*, *29*(2), 30-36.

[10] Li, Y., Wang, R., Li, Y., Zhang, M., & Long, C. (2023). Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach. *Applied Energy*, *329*, 120291.

[11] Jeyaraj, P. R., Nadar, E. R. S., Kathiresan, A. C., & Asokan, S. P. (2020). Smart grid security enhancement by detection and classification of non-technical losses employing deep learning algorithm. *International transactions on electrical energy systems*, *30*(9), e12521.

[12] Fan, K., Chen, Q., Su, R., Zhang, K., Wang, H., Li, H., & Yang, Y. (2021). Msiap: A dynamic searchable encryption for privacy-protection on smart grid with cloud-edge-end. *IEEE Transactions on Cloud Computing*, *11*(2), 1170-1181.

[13] Yin, X., Zhu, Y., & Hu, J. (2021). A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids. *IEEE Transactions on Industrial Informatics*, *18*(3), 1957-1967.

[14] Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. *Energies*, *15*(19), 7419.

[15] Khadam, U., Iqbal, M. M., Saeed, S., Dar, S. H., Ahmad, A., & Ahmad, M. (2021). Advanced security and privacy technique for digital text in smart grid communications. *Computers & Electrical Engineering*, *93*, 107205.

[16] Sivakumar, M., Umapathy, K., Dinesh Kumar, T., Omkumar, S., Archana, M. A., & Amannah, C. (2023). Protecting Future of Energy: Data Security and Privacy for Smart Grid Applications Using MATLAB. In *Data Analytics for Smart Grids Applications—A Key to Smart City Development* (pp. 159-178). Cham: Springer Nature Switzerland.

[17] Reka, S. S., Venugopal, P., Alhelou, H. H., Siano, P., & Golshan, M. E. H. (2021). Real time demand response modeling for residential consumers in smart grid considering renewable energy with deep learning approach. *IEEE access*, *9*, 56551-56562.

[18] Thilakarathne, N. N., Kagita, M. K., Lanka, D. S., & Ahmad, H. (2020). Smart grid: a survey of architectural elements, machine learning and deep learning applications and future directions. *arXiv preprint arXiv:2010.08094*.

[19] Pham, Q. V., Liyanage, M., Deepa, N., VVSS, M., Reddy, S., Maddikunta, P. K. R., ... & Hwang, W. J. (2021). Deep learning for intelligent demand response and smart grids: A comprehensive survey. *arXiv preprint arXiv:2101.08013*.

[20] Liu, H., Zhang, X., Shen, X., & Sun, H. (2021). A federated learning framework for smart grids: Securing power traces in collaborative learning. *arXiv preprint arXiv:2103.11870*.

[21] Guan, Z., Lv, Z., Sun, X., Wu, L., Wu, J., Du, X., & Guizani, M. (2020). A differentially private big data nonparametric Bayesian clustering algorithm in smart grid. *IEEE Transactions on Network Science and Engineering*, *7*(4), 2631-2641.

[22] Liu, Z., Lv, H., Li, M., Li, Z., & Huang, Z. (2019). A novel self-adaptive grid-partitioning noise optimization algorithm based on differential privacy. *Computer Science and Information Systems*, *16*(3), 915-938.

[23] Khan, H. M., Khan, A., Jabeen, F., & Rahman, A. U. (2021). Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids. *Sustainable Cities and Society*, *64*, 102522.

[24] Gough, M. B., Santos, S. F., AlSkaif, T., Javadi, M. S., Castro, R., & Catalão, J. P. (2021). Preserving privacy of smart meter data in a smart grid environment. *IEEE Transactions on Industrial Informatics*, *18*(1), 707-718.

[25] Zuo, X., Li, L., Peng, H., Luo, S., & Yang, Y. (2020). Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid. *IEEE Systems Journal*, *15*(1), 395-406.

[26] Guan, Z., Zhang, Y., Zhu, L., Wu, L., & Yu, S. (2019). EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. *Science China Information Sciences*, *62*, 1-14.

[27] Li, S., Xue, K., Yang, Q., & Hong, P. (2017). PPMA: Privacy-preserving multisubset data aggregation in smart grid. *IEEE Transactions on Industrial Informatics*, *14*(2), 462-471.

[28] Ndife, A. N., Mensin, Y., Rakwichian, W., & Muneesawang, P. (2022). Cyber-Security Audit for Smart Grid Networks: An Optimized Detection Technique Based on Bayesian Deep Learning. *J. Internet Serv. Inf. Secur.*, *12*(2), 95-114.

[29] Wang, Y., Sun, Y., Dinavahi, V., Cao, S., & Hou, D. (2019). Adaptive robust cubature Kalman filter for power system dynamic state estimation against outliers. *IEEE Access*, *7*, 105872-105881.

[30] Zhang, K., Ma, C., Xu, Y., Chen, P., & Du, J. (2021). Feature extraction method based on adaptive and concise empirical wavelet transform and its applications in bearing fault diagnosis. *Measurement*, *172*, 108976.

[31] Huang, C. Q., Jiang, F., Huang, Q. H., Wang, X. Z., Han, Z. M., & Huang, W. Y. (2022). Dual-graph attention convolution network for 3-D point cloud classification. *IEEE Transactions on Neural Networks and Learning Systems*.

[32] Raslan, A. F., Ali, A. F., Darwish, A., & El-Sherbiny, H. M. (2021). An improved sunflower optimization algorithm for cluster head selection in the internet of things. *IEEE Access*, *9*, 156171-156186.