Hybrid Anomaly Detection in OS Kernel Interfaces for Power Monitoring Systems Using Fuzzy Logic and Deep Belief Networks

Tianyu An[1*], Changlin Lv[1], Manpo Li[1], Shugui Zhang[2]
[1]Northeast Branch of State Grid Corporation, 110180, Liaoning, China
[2]Sichuan Energy Internet Research InstituteTsinghua University, Chengdu 610218, Sichuan, China
E-mail: antianyunesgcc@163.com, lvchanglin@ne.sgcc.com.cn, limanpo@ne.sgcc.com.cn, aix@zhutkj.cn
*Corresponding author

Keywords: Operating system (OS), kernel interfaces, power monitoring systems, anomaly detection, embedded system, security, Data analytics for energy-cost efficient system operation.

Received: June 6, 2025

Anomaly detection in operating system (OS) kernels is critical for the stability and security of embedded systems, particularly in power monitoring applications. OS kernel behavior is complicated, and typical anomaly detection algorithms frequently fail to detect smaller anomalies, especially in power-sensitive applications where energy efficiency is critical. The goal of this research is to create an effective anomaly detection framework capable of reliably identifying abnormalities in the Chinese OS kernel's behavior through power monitoring, assuring consistent system performance and security. The framework includes several critical steps: First, gather a dataset of system call sequences and power usage logs from the OS kernel. Data pre-processing is utilized to clean and normalize the dataset, ensuring it is formatted consistently for investigation. Feature data extraction is then carried out via the Kernel Principal Component Analysis (Kernel PCA) method that uses such important kernel interaction characteristics as the frequency of system calls and the power consumption behaviour. A novel technique, Fire Hawk Optimizer Fused Fuzzy Logic-Based Deep Belief Networks (Fire-Fuzzy DBN) is a hybrid approach that combines FHO to optimize system parameters, Fuzzy Logic to handle uncertainty in system behavior, and DBNs to extract complex patterns, resulting in a robust, adaptive, and effective solution for detecting kernel anomalies. The outcomes reveal that the proposed Fire-Fuzzy DBN strategy, which was implemented in Python, significantly improves kernel anomaly detection accuracy by 99% over previous techniques. The research data analytics for energy-cost efficient system operation establishes the efficacy of fuzzy testing technology in detecting anomalies in OS kernel interfaces for power monitoring systems, therefore improving embedded system dependability and security.

Povzetek: Prispevek obravnava zaznavanje anomalij v jedrnih vmesnikih operacijskega sistema v energijsko občutljivih vgrajenih sistemih za nadzor porabe. Avtorji združijo dnevniške zapise sistemskih klicev in meritve porabe energije, iz katerih s Kernel PCA razvijejo hibridni model Fire-Fuzzy DBN, ki povezuje mehko logiko, DBN ter Fire Hawk Optimizer za optimizacijo parametrov.

1 Introduction

Strong anomaly detection methods are gaining more and more significance to provide cell stability and dependability, as power monitoring systems see an explosive proliferation to the current electronic devices [1]. Hardware interface and the OS kernel are vital when it comes to the movement of data and system performance monitoring on Chinese systems. Anomalies can be generated by complex interactions, and this can prejudice the performance of the system. Such anomalies can be collected to improve the efficiency and reliability of system interface points at the kernel level [2]. Fuzzy testing technology is one of the most common techniques that are adapted to locate vulnerabilities, detect abnormal behaviors of a system. Fuzzy testing is distinct to existing or rather conventional systems of testing since they use known inputs and outputs whereas fuzzy systems test defaults to introduce anomalies through the use of corrupted data sources [3]. Energy-cost efficiency of operation of a system using data analytics would allow the identification of obscure strengths, edge cases that might not be addressed in conventional methods, and would be able to solve anomalies in power usage within a system through fuzzy testing of the Chinese OS kernel interface with a power monitoring system [4]. The operations in kernels are dynamic which can more often than not leave the traditional anomaly detection methods unusable due to

unexpected events that occur within a kernel. In the traditional approaches, sensitivity or freedom of degree was lacking; in terms of energy savings, the way systems or monitoring power is sustained is of essence in systems of large-scale and devices that are embedded [5]. The fuzzy testing technology is more precise and effective due to the anomaly detection which provides random and mutated input data that explores the unusual behaviors, which resolves the historical obstacle of scarce anomaly detection and improves efficiencies of the system by resolving the unanticipated situations [6]. Fuzzy testing helps make the anomaly detecting mechanisms more sensitive by simulating a wide variety of scenarios. The importance of these kinds of systems as that of the Chinese OS kernel interfaces is that when the testing protocol is carried, it does not usually test them against all the anomalies. By identifying minor weak points early enough, fuzzy testing of the system increases reliability and prevents any potential latent faults that may lead to performance or efficiency degradation [7]. The aim of the research would be based on fuzzy testing technologies to develop an anomaly detection system on power monitoring systems. In a bid to enhance the dependability and the power efficiency of the system, the analysis tries to identify and correct the mismatches at OS kernel interface level. It aims to offer this type of a robust solution that will increase the overall reliability and effectiveness of the power monitoring systems.

The motivation behind this work stems from the increasing complexity of OS kernel behavior in embedded power monitoring systems, where even minor anomalies can lead to significant security risks or system failures. Traditional detection methods often overlook subtle deviations, especially under energy constraints. Therefore, developing a more accurate and adaptive anomaly detection framework is essential to ensure system reliability, efficiency, and security. This Fire-Fuzzy DBN addresses a critical gap by introducing a robust solution tailored for power-sensitive, kernel-level anomaly detection. The key contributions of this work are as follows.

Key contribution

- Realistic Kernel Dataset Utilization: The performance of embedded systems in power-sensitive contexts was accurately modeled by using a real-world OS kernel anomaly collection that included power logs and system call traces.
- Strong Pipeline for Preprocessing Data: To guarantee high-quality input for analysis, extensive preparation was used, including data cleaning, management of missing values, and Z-score normalization.
- Effective Kernel PCA Feature Extraction: Through reducing high-dimensional data while maintaining crucial characteristics like call frequency and power consumption, kernel PCA improved the system's sensitivity to minute irregularities.
- Proposed Fire-Fuzzy DBN Model: Developed a hybrid anomaly detection model that handles uncertainty, learns deep features, and improves detection precision by merging Fire Hawk Optimizer, Deep Belief Networks, and Fuzzy Logic.
- Cost-Effective Energy Use: The framework is ideal for power-sensitive and real-time integrated technologies in industrial or utility-based uses since it was designed to identify abnormalities while consuming the least amount of energy possible.

The following sections comprised the remainder of the section: In Part 2, the relevant works are presented. Part 3 covers the material and methods, Part 4 includes the findings and discussion, and Part 5 provides a conclusion.

2 Related work

The core network's attack surface was increased by the 5G network, raising security risks. Intrusion Detection Systems (IDSs) were utilized to identify anomalies to safeguard the network. However, conventional techniques have trouble identifying the relationship between attack behaviors and traffic characteristics [8]. A novel intrusion detection technique based on multiple-kernel clustering (MKC) methods was presented to overcome problems. The approach provided more tolerance for low-quality traffic sampling data, and decreased sensitivity to increase classification accuracy. The growth of Internet of Things (IoT) devices raised security and privacy issues, making anomaly detection essential. Manufacturers frequently refuse to correct vulnerable devices because of vulnerabilities. A useful last line of security was provided by the host-based anomaly detection system for IoT devices (HADES-IoT), which prevented malicious programs from being launched [9]. It is compatible with Linux-based IoT devices and offers impermeable security. Through a memory usage of about 5.5% and minimal Control Process Unit (CPU) resources, HADES-IoT proved to be an efficient method for identifying IoT malware. Although the Internet of Medical Things (IoMT) has transformed healthcare, there remain risks. Anomaly-based Intrusion Detection Systems (AIDS) were among the innovative security measures required to handle. The research used novelty and outlier detection techniques to provide a revised hybrid AIDS design for IoMT networks [10]. The findings of performance evaluations indicate that all integrated machine learning (ML) algorithms have low computational expenditures and that certain algorithms have strong detection performance. The effectiveness of the strategy was illustrated by the details of implementation on devices. Table 1 presents a comparison of existing anomaly detection methods, highlighting their

outcomes, benefits, and relevance to kernel interface monitoring.

Table 1: Comparative overview of advanced anomaly detection techniques relevant to kernel interface monitoring

Reference	Method	Result	Advantage	Limitation
Nalini et al., [11]	GSMPSO-MM-RCNN (Grid Search-based Multi-population PSO with Regional CNN)	Achieved 90% accuracy across four high-dimensional datasets	Reduces overfitting, improves pattern detection, lowers estimation time	Might need high computational resources; lacks external validation.
Wang etal., [12]	Ensemble Learning for System Logs	Improved precision, recall, and F1-score in anomaly prediction	Effective in handling large-scale logs, it enhances prediction accuracy	Be limited to cloud log context; generalizability unclear.
Zacaron et al., [13]	DL-based IDS for SDN	Eliminated 89% of abnormal flows	Detects and blocks threats in real-time, improves SDN network security	Only tested on two benchmark datasets; simplicity might limit scope.
Ahmadi et al., [14]	Super Learning Ensemble for ICS	Achieved high abnormal recall and maximum F1-score	Low error rate, adaptable to smart city/ICS domains	Focused on one-class classification; might not generalize to multiclass scenarios.
Soni et al., [15]	NelPareto AVOA + CDAD (ITAO System)	Detected complex traffic anomalies, improved energy efficiency	Multi-objective optimization enhances traffic flow and safety	Domain-specific, traffic-centric system fuly not generalize outside urban contexts.

3 Materials and methods

The proposed anomaly detection methodology for power monitoring systems involving Chinese OS kernel interfaces proposes novel strategies, such as data preprocessing, Z-score normalization, and Fire-Fuzzy DBN. These strategies improve the ability to identify anomalies under dynamic Chinese OS kernel interfaces with greater accuracy, flexibility, and robustness. The KPCA dimensions are reduced to information, and the Fire-Fuzzy DBN strengthens the robustness of the system. Figure 1 displays the flow of the method used in the proposed system. Figure 1 displays the flow of the method used in the proposed system.

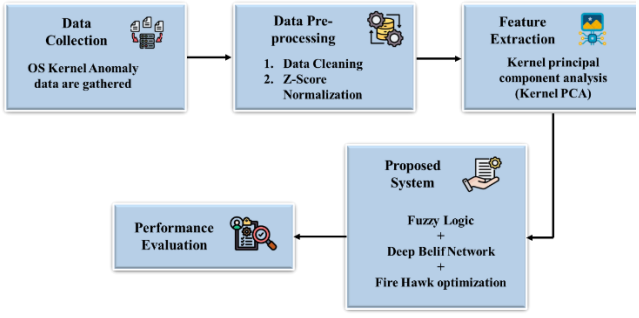

Figure 1: Flow of the recommended technique

3.1 Data collection

The dataset was collected from the open-source Kaggle website https://www.kaggle.com/datasets/ziya07/os-kernel-anomaly-dataset/data. The dataset is created for assessing OS kernel anomaly detection within the context of embedded power monitoring systems. It contains many variables that could be useful for the examination of hybrid models since it represents the relation of power consumption patterns with the increased frequency of system-level events. Data size is 65.77 kB, and a total of 1000 were recorded. Table 2 shows the Dataset Structure and Description.

Table 2: Overview of dataset structure and description

Attribute Name	Description	Data Type	Example Value
timestamp	UNIX timestamp of the system event	Integer	1624982374
process_name	Name of the kernel or user-level process generating the event	String	kernel_thread, pm_monitor

cpu_ usage	CPU utilization at the time of the event (%)	Float	35.72
memory_ usage	Memory usage in MB	Float	412.5
power_ usage	Instantaneous power consumption in Watts	Float	5.61
Syscall _ sequence	Encoded sequence of recent system calls prior to the event	String (encoded)	open, read, mmap, close
event_ type	Type of system event (e.g., syscall, I/O, memory operation)	Categorical	syscall, memory, I/O
anomaly _ label	Class label indicating anomaly presence (0 = normal, 1 = anomaly)	Integer (binary)	0 or 1

3.2.1 Data exploration

Fuzzy testing technology was used to develop an anomaly detection method for the Chinese OS kernel interface in a power monitoring system, focusing on CPU, memory, and power consumption features, enhancing detection accuracy and reliability, particularly in extreme operating conditions. The feature importance is shown in Figure 2.

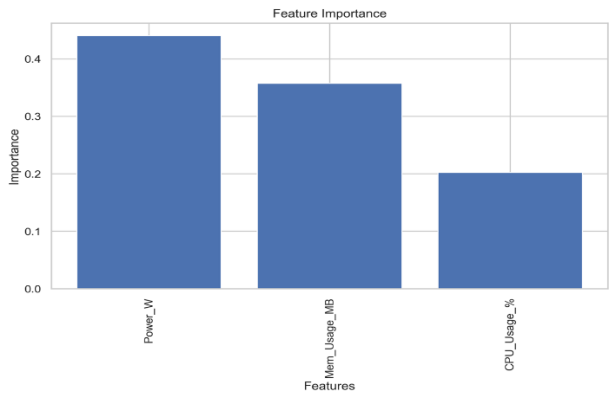

Figure 2: Feature importance scores for CPU, memory, and power consumption in detecting anomalies in the OS kernel power monitoring system.

3.2.2 Data preprocessing

Data preprocessing involved cleaning to remove noise and irrelevant entries, ensuring dataset integrity. Z-score normalization was applied to standardize features, centering them around a mean of zero with unit variance. This choice improved model convergence and highlighted subtle anomalies by equalizing feature scales, which is essential for effective feature extraction and accurate kernel anomaly detection.

Data cleaning: Data cleansing is a very important preprocessing phase in which the errors in data is being identified & correct as well as data become more consistent & more accurate. It is crucial in statistical instrumental control, anomaly detection and energy monitoring systems as anomaly finding and pattern finding is dangerous. Fuzzy testing technology enhances system robustness by allowing flexible approximation reasoning. Integrating data cleansing and anomaly detection improves the reliability and efficiency of power monitoring systems.

3.2.3 Z-score Normalization: Normalization is crucial in the preprocessing stage for power monitoring and anomaly discovery using the Chinese OS kernel. It ensures uniformity across features by transforming information into a standardized format. Z-score normalization is applied for scaling feedback qualities like power consumption readings and system performance metrics. The method allows the fuzzy testing-based anomaly detection system to analyze the data by converting the original values to a normalized form, where the standard deviation equals 1 and the mean value equals 0. Eq 1 presents the formula for Z-score normalization:

$$x' = \frac{x_j - G_j}{std\ (G)} \quad (1)$$

Description: x' = Normalization value results, x = The attribute's value that has to be normalized, G_j = The attribute's mean value, $and\ std\ (G)$ = Attribute G for the standard deviation.

3.3 Kernel principal component analysis (Kernel PCA)

To increase detection accuracy and system responsiveness in the context of the Chinese OS kernel for anomaly detection for kernel interfaces in power monitoring systems, effective data handling is essential. Datasets can be made less dimensional by using the widely utilized KPCA method before being fed to anomaly detection techniques. KPCA performs most effectively in linear systems. The KPCA combines a nonlinear kernel technique with the traditional approach to provide better performance in complicated, nonlinear situations like

kernel interface procedures, and data analytics for energy-cost efficient system operation. The primary components of the updated dataset created by KPCA comprise variables that preserve most of the information from the initial collection of data. By removing components with inadequate data, KPCA lowers the dimensionality of the dataset without significantly sacrificing any important features. The first step is to standardize the initial dataset W_{std}. Eq (2) is used to calculate the primary components that represent the new dataset W_{new}.

$$W_{new} = W_{std}R \tag{2}$$

The standardized original dataset is denoted by W_{std}, and the matrix of eigenvectors sorted by the covariance matrix of W_{std} is R. KPCA expands on this technique by implementing a linear with the higher-dimensional feature space after first mapping the input data to it using nonlinear transformations.

3.4 Proposed system

A hybrid anomaly detection architecture called the Fire-Fuzzy DBN was created to enhance stability and identify issues in Chinese OS kernel interfaces used in power monitoring systems. It blends the FHO, DBNs, and fuzzy logic. By converting input data, such as CPU, memory, and power consumption, into fuzzy values, fuzzy logic controls system behaviour uncertainty. Then, to distinguish between normal and aberrant activity, DBNs learn intricate, hidden patterns. By effectively looking for anomaly indicators and adjusting DBN parameters, FHO improves the model by imitating the fire hawk's hunting technique. In dynamic embedded contexts, this connection facilitates adaptive decisions in real time, enhances detection precision, and encourages energy-effective execution, guaranteeing dependable power management and system safety.

3.4.1 Fuzzy Logic

The initial stage of the anomaly detection algorithm uses fuzzy logic to deal with input data unpredictability, such as fluctuations in CPU activity or power consumption. Using participation processes, it transforms numerical values into degrees of belonging to various categories (such as "low," "medium," or "high") in place of employing physical thresholds. After that, a rule-based system assesses the likelihood that an input may depict anomalous behavior. Even in cases when the input is chaotic or incompatible, this enables the system to make more intelligent and adaptable judgments.

Fuzzy logic is a systematic method for managing inconsistencies and imprecision in Chinese OS kernel interfaces of power monitoring systems. It comprises four components: input fuzzification, fuzzy inference engine, fuzzy rule base, and output defuzzification. The research uses a Mamdani-type fuzzy logic system with a linguistically expressed rule basis. This is how a general fuzzy rule Q_l can be explained as follows by eq (3)

$$Rule\ Q_l: \boldsymbol{IF} w_j\ is\ B_1^l \boldsymbol{AND}\ \dots\ \boldsymbol{AND} w_m\ is\ B_m^l \boldsymbol{THEN} z_l\ is\ A^l \tag{3}$$

The fuzzy sets associated with the j^{th} input and output of the l^{th} rule are represented by A_1^l and A^l, appropriately; m indicates the dimensionality of the input vector w, while z_l is the corresponding output variable. Utilizing a suitable classification function (such as Gaussian, triangular, or trapezoidal), each input w_j is first fuzzified. Fuzzification gives a membership grade $\mu_{A_1^l}(w_j)$ to every input. For rule Q_l, the minimum is used to calculate the degree of disciplining in eq (4).

$$\mu_{Q_l}(\vec{w}) = min\left\{\mu_{A_1^l}(w_j)\right\}, j = 1 \dots, m \tag{4}$$

The output fuzzy set A can be obtained by aggregating the consequents of all terminating rules using an operator, such as the maximum operator. A thorough description of the fuzzy inference procedure was identified. Defuzzification techniques like the centroid technique are used to get an obvious outcome for anomaly detection decision-making. The crisp output z is computed by discretizing the output domain to M samples, as follows in eq (5):

$$y = \frac{\sum_{j=1}^{M} z_j \mu_A(z_j)}{\sum_{j=1}^{M} \mu_B(z_j)} \tag{5}$$

In the dynamic and frequently random nature of kernel interface operations in power monitoring systems, this fuzzy logic framework makes it possible the Chinese OS kernel to identify anomalies more reliably and adaptively, contributing to energy-cost efficient system operation.

3.4.2 Deep Belief Networks (DBN)

The DBN, a type of DL model composed of multiple layers of Restricted Boltzmann Machines (RBMs), receives input data that has been preprocessed using fuzzy logic. By identifying patterns and relationships among various system activities, the DBN learns from this fuzzified data. Through its layer-by-layer learning approach, the DBN is capable of detecting complex and hidden anomalies that might be overlooked by simpler methods.

Precise portrayal of the uncertainty with the input domain is dynamic to facilitate effective anomaly detection in the Chinese OS kernel interface of power monitoring systems about energy-cost efficient system operation. The domain values are converted to fuzzy representations with the

correct membership functions to receive as inputs to the DBN, retaining the system's obscurity using eq (6).

$$\mu_{AD}(W) = \begin{Bmatrix} 0 & (w < b) or (w > c) \\ \frac{w-b}{a-b} & b \le w \le a \\ 1 & b \le w \le d \\ \frac{c-w}{c-d} & d \le w \le c \end{Bmatrix} \quad (6)$$

A DBN is a type of deep neural network (DNN) comprising multiple layers of belief networks, which are generally implemented as RBMs in each level. The sequential stacking of the RBMs in the DBN structure establishes a robust deep structure that can learn hierarchical features. Belief networks and RBMs are the two primary network types that are integrated by DBNs. Layers of random binary units combined by weighted, directed boundaries constitute a belief network. The network can enhance its representation capabilities by learning patterns in the input information by modifying the inter-unit weights according to the belief networks. $\mu_{AD}(W)$ represents the anomaly detection in the investigation; the binary units are assumed to be in 0 or 1.

A DBN is a divided undirected graphical model that incorporates visible and hidden binary units. The only connections between the units are between different categories. The distributions of probabilities across the hidden (Hd) and visible Vs layers are characterized by energy functions, which are expressed as follows in the eqs (7-9):

$$Prob\ (Vs, Hd) = \frac{1}{y} \exp\big(-Eg(Vs, Hd)\big) \quad (7)$$

$$Y = \sum_{Vs,Hd} \exp(-Eg(Vs, Hd)) \quad (8)$$

$$Eg\ (Vs, Hd) = -\sum_j va_j\, Vs_j - \sum_i hb_j\, Hd_j - \sum_j \sum_i Vs_j\, , wt_{j,i}, Hd_i \quad (9)$$

Vs represents the visible elements, (Hd),the implicit components, wt the weight ratio among the present phase and the previous level, hb the hidden biased of the concluding level, and va the visible bias. According to logistic regression, the consequent probability $Prob\ (Vs_i = 1|Hd)$ and $Prob\ (Hd_i = 1|Vs)$ have activating when the unobserved matrix $Hd(Hd_1, \ldots, Hd_i, .., Hd_n)$ is identified. The expected number of the j^{th} visible unit may be determined using the following formula, which is followed by equation (10):

$$Prob\ (Vs_i = 1|Hd) = \sigma\big(va_i + \sum_{i=1}^{m} wt_{j,i}\, Hd_j\big) \quad (10)$$

The stimulation frequency of the i^{th} hidden units may also be determined by using the following expression for a collection of visible vectors $vs\ (vs_1, \ldots, vs_j, \ldots, vs_m)$ followed by (11):

$$Prob\ (Hd_i = 1|Vs) = \sigma\big(hb_i + \sum_{j=1}^{n} wt_{j,i}\, , Vs_j\big) \quad (11)$$

where $wt_{j,i}$ represents the association strength between a j^{th} exposed units and the i^{th} hiding device, hb_i is the hiding perception connection, and σ is the sigmoid activation function. Maximizing the joint probabilities among the set of training inputs is essential for anomaly detection for a power monitoring system's kernel interface to properly learn the typical operational behavior using eq (12).

$$\arg max_{wt} \prod_{vs \in Vs} Prob(Vs) \quad (12)$$

Where the set of all training input samples obtained from the kernel interface data is represented by Vs. Using fuzzy testing technology for energy-cost efficient system operation, the system can efficiently differentiate between typical and unusual behavior patterns by maximizing this probability, improving the security and dependability of power monitoring activities.

3.4.3 Fire Hawk Optimizer (FHO)

The FHO improves the DBN's performance by adjusting its settings automatically. Inspired by how fire hawks search for prey, this method searches for the best values for learning, such as weights and biases, so the DBN can detect anomalies more accurately. It tries different combinations, compares their results, and moves toward the best solution. This optimization makes the system faster and more accurate in finding kernel-level issues.

The FHO algorithm was inspired by fire hawks' foraging habits, specifically the ability to initiate and spread flames. The FHO method initializes a set of candidate solutions (W) that reflect possible practical conditions of the system to discover anomalies in the Chinese OS kernel interface of a power monitoring system. To efficiently investigate a variety of patterns of typical and anomalous system behavior, the starting positions of the fire hawks and prey, represented as position vectors inside the search space, are allocated at random using eqs (13-14).

$$W = \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_j \\ \vdots \\ W_M \end{bmatrix} = \begin{bmatrix} W_1^1 W_1^2 & \cdots & W_1^i & \cdots & W_1^c \\ W_2^1 W_2^2 & \cdots & W_2^i & \cdots & W_2^c \\ \vdots \quad \vdots & \cdots & \vdots & \ddots & \vdots \\ W_j^1 W_j^2 & \cdots & W_j^i & \ddots & W_j^c \\ \vdots \quad \vdots & \cdots & \vdots & \cdots & \vdots \\ W_M^1 W_M^2 & & W_M^i & & W_M^c \end{bmatrix} \begin{cases} j == 1,2, \ldots, M. \\ i = 1,2, \ldots, c. \end{cases} \quad (13)$$

$$x_i^j(0) = x_{i,min}^j + rand.(x_{i,max}^j - x_{i,min}^j)\begin{cases} j == 1,2,\dots,M. \\ i = 1,2,\dots,c. \end{cases} \quad (14)$$

Here M is the overall number of solution individuals that represent the various Chinese OS kernel interface operating asserts in the power monitoring system; W_j is the j^{th} solution candidate in the search space; c is the dimensionality of the anomaly detection problem; $x_i^j(0)$ is the initial position of the i^{th} decision variable for the j^{th} solution candidate; W_j^i is the i^{th} decision variable linked to the j^{th} solution prospective; and the evenly distributed random number $rand$ is in the range $(0, 1)$; the minimum and maximum bounds for the i^{th} decision variable of the j^{th} candidate solution are represented by $x_{i,min}^j$ and $x_{i,max}^j$, respectively, guaranteeing the system's practicable operating range for Chinese OS kernel for anomaly detection, respectively.

Whereas PR_l indicates the l^{th} potential anomaly found in the search space out of a total of n potential anomalies, FH_k indicates the k^{th} candidate anomaly detector (fire hawk) with the entire search space of m fire hawk recruits. Throughout the subsequent portion of the detection method, the distance between each fire hawk (anomaly detector) and its matching prey (possible anomaly) is determined. The distance, D_k^l, is described by the following equation. Where (w_2, w_1) and (z_2, z_1) indicate the coordinates of the FHO in the search space, respectively; D_k^l indicates the total distance between the k^{th} fire hawk and the l^{th}; n and m indicate the aggregate number of FHO in the search space, followed by eqs (15-17).

$$PR = \begin{bmatrix} PR_1 \\ PR_2 \\ \vdots \\ PR_l \\ \vdots \\ PR_n \end{bmatrix}, \quad l = 1,2,\dots,n. \quad (15)$$

$$FH = \begin{bmatrix} FH_1 \\ FH_2 \\ \vdots \\ FH_k \\ \vdots \\ FH_m \end{bmatrix}, \quad k = 1,2,\dots,m \quad (16)$$

$$D_k^l = \sqrt{(w_2 - w_1)^2 + (z_2 - z_1)^2}, \quad \begin{cases} k = 1,2,\dots,m \\ l = 1,2,\dots,n \end{cases} \quad (17)$$

Where GB represent for the greatest anomaly identification solution found in the search space, which is regarded as the most important anomaly indicator; q_1 and q_2 are uniformly distributed random numbers in the range $(0, 1)$ that are used to simulate the movement of anomaly detection devices in the direction of primary anomaly and the surrounding detection categories; and FH_{Near} demonstrates a neighboring anomaly detector in the search space using eq (18).

$$FH_k^{new} = FH_k + (q_1 \times GB - q_2 \times FH_{Near}), k = 1,2,\dots,m. \quad (18)$$

The following is the mathematical expression for SP_k and SP, implementing to account that in the context Chinese OS kernel for anomaly detection, an optimal location is an ideal area where several kernel interface behaviors cluster to maintain system stability through anomalous incidents, data analytics for energy-cost efficient system operation. The l^{th} detected anomaly occurrence in the kernel interface monitoring area is indicated by PR_l, while PR_r denotes the r^{th} anomaly-related behavior reported associated with the l^{th} Chinese OS kernel for anomaly detector, followed by eqs (19-20).

$$SP_k = \frac{\sum_{r=1}^{q} PR_r}{q}, \begin{cases} r = 1,2,\dots,q. \\ k = 1,2,\dots,m. \end{cases} \quad (19)$$

$$SP = \frac{\sum_{l=1}^{n} PR_l}{n}, \quad l = 1,2,\dots,m. \quad (20)$$

The FHO successfully detects anomalies in the Chinese OS kernel interface using the data analytics for energy-cost efficient system operation and foraging behaviors of fire hawks to search for possible vulnerabilities of the system. The Fire-Fuzzy DBN enhances the power monitoring system's Chinese OS kernel interface, abnormality detection, and stability by integrating hierarchical learning from DBN, Fuzzy Logic uncertainty management, and the adaptive anomaly detection feature of FHO, thereby maximizing fire hawk distance movement. By a novel blending of techniques, this hybrid method efficiently identifies faults and optimizes system stability.

4 Experimental evaluation and discussion

Effectiveness assessment and the outcomes of the algorithm's adoption are discussed in the next part. The efficacy of the suggested Fire-Fuzzy DBN is demonstrated by the accuracy outcomes of the study's compared to the conventional and Extended Berkeley Packet Filter Intrusion Detection/Prevention Systems (iKern-IDPS) [16]. Table 3 summarizes the key components and hyperparameter configurations used in the proposed Fire-Fuzzy DBN anomaly detection framework.

Table 3: Hyperparameter configuration of Fire-Fuzzy DBN Framework

Component	Hyperparameter	Value / Description
Fuzzy Logic	Number of Input Variables	3 (CPU, Memory, Power Usage)
	Membership Function Type	Triangular
	Membership Levels per Input	3 (Low, Medium, High)
	Total Fuzzy Rules	9 (3×3 combinations)
	Defuzzification Method	Centroid method
	Rule Evaluation Method	Mamdani Inference System
Kernel PCA	Number of Components	5 (retaining 95% cumulative variance)
	Kernel Type	Radial Basis Function (RBF)
DBN (Deep Belief Network)	Input Layer Size	10 (from fuzzified + reduced features)
	Hidden Layer 1 Size	64 neurons
	Hidden Layer 2 Size	32 neurons
	Output Layer Size	2 (Normal, Anomaly)
	RBM Pretraining Epochs	10
	Learning Rate (RBM)	0.01
	Fine-tuning Optimizer	Adam
	Fine-tuning Epochs	20
	Batch Size	128
Fire Hawk Optimizer (FHO)	Population Size (N)	30 fire hawks
	Maximum Iterations	50
	Search Space Range	[-1, 1] (for weight initialization)
	Distance Metric	Euclidean distance
	Randomization Factors	Uniform [0, 1] for search variation
	Fitness Function	DBN validation accuracy
Training Dataset	Dataset Size	45,672 records
	Anomaly Ratio	~9% anomalies
	Train/Test Split	80% / 20%
	Normalization Method	Z-score

4.1 Experimental configuration

Python installations and system settings are used for Power monitoring systems that use fuzzy testing technologies to detect anomalies in the OS kernel interface. The experimental environmental configuration is shown in Table 4.

Table 4: Implementation environment details

Components	Descriptions
RAM	25 GB
CPU	Intel Xeon Processor (2.4 GHz)
GPU	NVIDIA Tesla V100
OS	Ubuntu 20.04 LTS
System Programming	Python 3
DL Framework	PyTorch 1.8

4.2 Correlation and confusion matrix

The correlation matrix assesses the covariance between power consumption, CPU usage, and memory usage. The correlation matrix indicates a low correlation between the power and memory usage. The confusion matrix analyzes the accuracy of an anomaly detection technique. It shows that the classification accuracy was better, as there were only a few misclassifications in the power monitoring system.

Correlation matrix: Fuzzy testing method is employed in the investigation to examine anomaly detection in the power monitoring system's Chinese OS kernel interface. Power consumption, CPU usage, and memory usage relations are shown on the correlation heatmap. Power and memory usage can't be closely related, evidenced by the lack of a strong association between memory usage and power consumption and CPU usage. The analysis optimizes power management and detects anomalies in the system.

Confusion matrix: The performance of the operational efficiency of the anomaly detection method using the Chinese OS kernel interface for power monitoring systems is illustrated in this confusion matrix shown in Figure 3. The model correctly labeled 180 normal instances and 8 anomaly cases, incorrectly classified 10 anomalies as normal and 2 normal instances as anomalies. The fuzzy testing technology utilized for anomaly detection is efficient in distinguishing between normal and anomalous behavior within the system, a fact that is proved by its relatively high accuracy and low rate of incorrect classification.

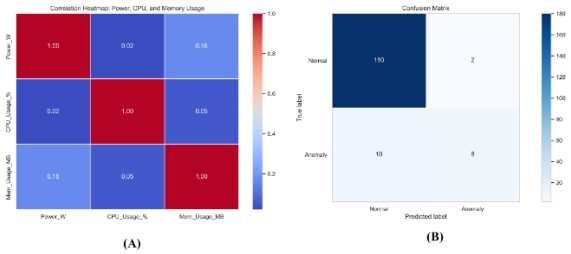

Figure 3: (A) Correlation matrix, (B) Confusion matrix evaluation

4.3 Process and label distribution for anomaly detection in power monitoring system

The procedure and label distribution for the anomaly detection task for a Chinese OS kernel interface in a power monitoring system are shown in this Figure 4. The system process distribution is dominated by kernel_ thread and pm_ monitor, but there's a significant label imbalance, with most cases classified as normal and a few anomalous, which could hinder the framework's training and classification of anomalies.

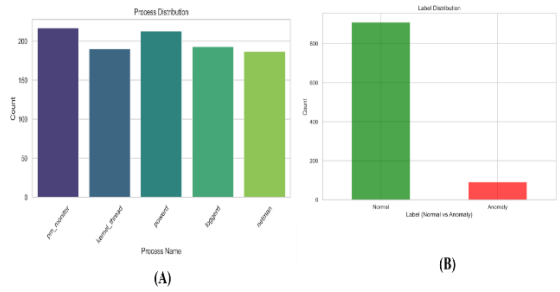

Figure 4: (A) Process distribution, (B) Label distribution outcome performance

4.4 Fuzzy testing-based anomaly detection in Chinese OS kernel interfaces for energy monitoring

The anomaly detection framework employs fuzzy testing technologies to attack Chinese OS kernel interfaces in power monitoring systems (Figure 5). Fuzzy testing evaluates system strength and vulnerabilities by detecting anomalies in CPU and power consumption. It enables early failure or inefficiency detection through pattern analysis, enhancing the protection and stability of energy-monitoring systems by detecting kernel-level interaction inefficiencies.

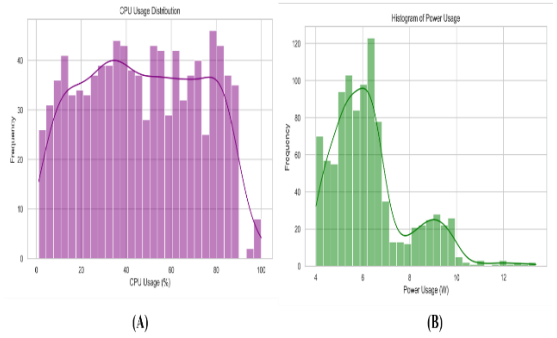

Figure 5: (A) CPU usage distribution, (B) Histogram of power usage of outcome performance

4.5 Time-series analysis of kernel power in fuzzy testing for anomaly detection

To detect anomalies in the power consumption patterns of Chinese OS kernel interfaces, the time series of employed fuzzy testing is shown in Figure 6. The system monitors the kernel's stress response using unplanned or warped inputs. Variations in power consumption are analyzed, revealing anomalous spikes and erratic patterns. Rolling mean analysis identifies deviations from normal usage patterns, enhancing the reliability and robustness of the power monitoring system.

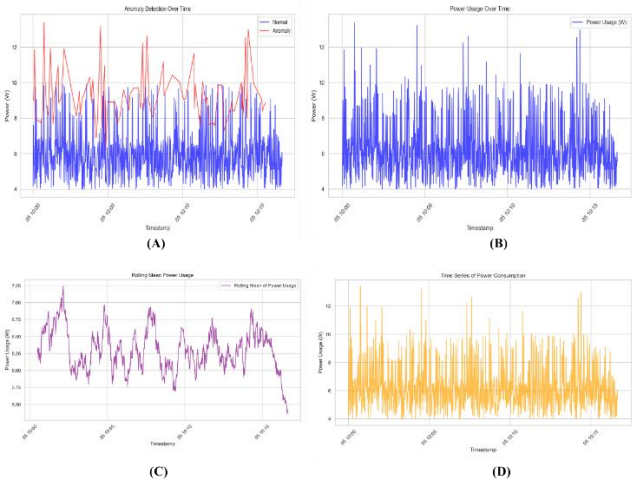

Figure 6: (A) Anomaly detection over time, (B) Power usage over time, (C) Rolling mean power usage, and (D) Time series of power consumption

4.6 Multivariate anomaly detection in kernel-level power monitoring using Fuzzy testing

The fuzzy testing-based anomaly detection method at Chinese OS kernel interfaces under power management scenarios is displayed in Figure 7. The technique uses fuzzy testing to identify unexpected behavior in power consumption and system parameters like CPU, memory usage, and time. It uses multivariate analysis to detect concealed defects and abnormal system responses, improving fault tolerance, system stability, and operating efficiency in real-time power monitoring systems.

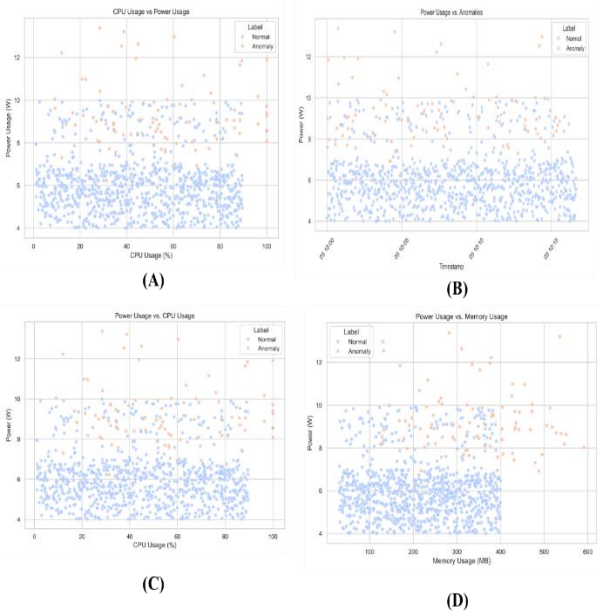

Figure 7: (A) CPU usage vs power usage, (B) Power usage vs anomalies, (C) Power usage vs CPU usage, (D) Power usage vs memory usage

4.7 Performance of Fuzzy testing-based anomaly detection using ROC analysis

A fuzzy testing-based approach for anomaly detection from Chinese OS kernel interfaces in a power monitoring system is illustrated through the use of a Receiver Operating Characteristic (ROC) curve, as shown in Figure 8. The model effectively distinguishes normal and abnormal behavior, with high sensitivity and specificity, and excellent classification performance, achieving an Area Under Curve (AUC) of 0.94, proving the effectiveness of fuzzy testing in early anomaly detection and system security enhancement.

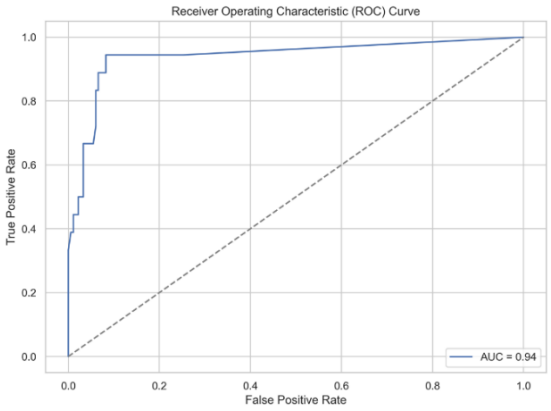

Figure 8: Evaluation performance of ROC curve

4.8 Comparative evaluation for accuracy

Accuracy in anomaly detection refers to how accurately a system detects outliers or behaves unusually in the dataset provided. The Chinese OS kernel interface of the OS fundamental structure is often tailored for certain Chinese hardware or software environments for data analytics for energy-cost efficient system operation. Fuzzy testing technology is testing systems with approximations by introducing variables and testing the system under multiple conditions to ensure increased robustness and fault tolerance. The existing technique, iKern-IDPS scored 98.84%, and the proposed Fire-Fuzzy DBN method improves accuracy to 99%. The outcomes demonstrate that the recommended strategy has the highest accuracy when compared to the current techniques. Table 5 and Figure 9 show the outcome performance of the existing and proposed techniques for accuracy.

Table 5: Comparative performance of accuracy

Methods	Accuracy (%)
iKern-IDPS [16]	98.84
Fire-Fuzzy DBN [Proposed]	99

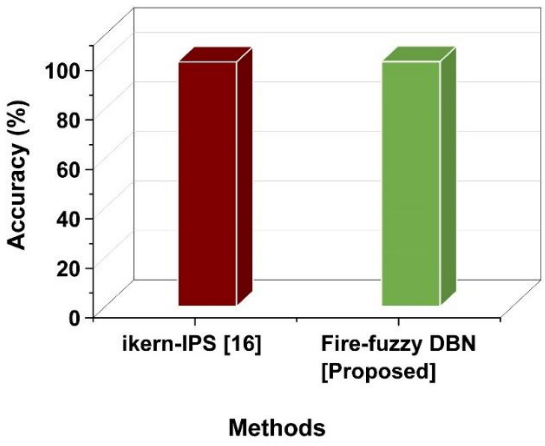

Figure 9: Outcome performance of accuracy

The method would face scalability concerns if applied to vast datasets, which is an area of research limitation. In addition to that, the effectiveness of the model under scenarios such as these with missing logs would be subject to its assumption regarding log quality data [12]. The research could investigate techniques to deal with data as making it more scalable. The drawback is that in dynamic, volatile network situations where attack signatures change continuously, the proposed IDS cannot perform as well. Using benchmark datasets adequately captures the diversity of vectors and the complexity present in the data [13]. Such issues should be addressed by the assignment with diverse real-world data and more accommodating detection mechanisms.

The challenges of this research pertain to the fact that the iKern-IDPS cannot incorporate that may or could be a real attack paradigm, as it is more oriented around anomalies at the kernel interface. Also, the ability of the fuzzy testing technology to be configurable to dynamic and evolving OS environments remains untested over a timeline of exploit activity. The limitation of the Kernel-level trac was that it relied exclusively on simulated test environments, which cannot accurately model real-world conditions. The method cannot capture all potential kernel-level anomalies, which can limit detection capabilities. To address these challenges, the Fire-Fuzzy DBN approach could incorporate the detection of dynamic attacks while adapting the current OS environment through continual learning. Incorporating combined simulation and scenarios could broaden the coverage of anomalous detection, along with continual improvements in accurate detection over time.

5 Conclusion

The anomalous behavior of the system is to determine the purpose of anomaly detection for Chinese OS kernel interfaces for Power Monitoring Systems. Fuzzy testing

technology is used to discover and detect anomalies resulting from the use of fuzziness or imprecise logic. The method helps ensure consistent operation, energy-cost efficient system operation and energy utilization monitoring in the system. The Fire-Fuzzy DBN method achieved the greatest performance and was superior in terms of performance in accuracy (99%). Fuzzy testing for anomaly detection is ultimately constrained by its limitations in determining all of the possibilities available to the system and its applicability being limited to a few platforms.

Limitation and future scope

While the proposed Fire-Fuzzy DBN framework demonstrates high accuracy, it has limitations. The integration of fuzzy logic and deep networks can lead to increased computational overhead, potentially impacting real-time performance. Additionally, scalability in large-scale or diverse kernel environments remains a concern, necessitating further optimization and testing to ensure robustness in practical, real-world deployments. To provide adaptive, self-learning anomaly detection in dynamic power monitoring systems, further improvements may include integrating reinforcement learning, extending detection capabilities across more OS components, and optimizing the model for real-time deployment.

References

[1] Wu, Y., Wang, S., Chen, H., Peng, D., & Yuan, Z. (2024). Kernelized fuzzy-rough anomaly detection. *IEEE Transactions on Fuzzy Systems*, *32*(8), 4285-4296.https://doi.org/10.1109/TFUZZ.2024.3393710

[2] Duan, G., Fu, Y., Cai, M., Chen, H., & Sun, J. (2023). DongTing: A large-scale dataset for anomaly detection of the Linux kernel. *Journal of Systems and Software*, *203*, 111745.. https://doi.org/10.1016/j.jss.2023.111745

[3] Zhang, H., Liu, Y., Gui, F., & Yang, X. (2023). A universal aquaculture environmental anomaly monitoring system. *Sustainability*, *15*(7), 5678.https://doi.org/10.3390/su15075678

[4] Shi, Y. (2025). FAT-Net: A Spectral-Attention Transformer Network for Industrial Audio Anomaly Detection Using MFCC and Raw Features. *Informatica*, *49*(26).https://doi.org/10.31449/inf.v49i26.8746

[5] Wang, R., Qiu, H., Cheng, X., & Liu, X. (2023). Anomaly detection with a container-based stream processing framework for industrial internet of things. *Journal of Industrial Information Integration*, *35*, 100507.https://doi.org/10.1016/j.jii.2023.100507

[6] Liu, J., Guogang, W. A. N. G., Zong, X., Bowei, N. I. N. G., & He, K. (2025). EfficientTransformer: A Dynamic Anomaly Detection Model for Industrial Control Networks. *IEEE Access*.https://doi.org/10.1109/ACCESS.2025.3545659

[7] Halimi, K., Hadjadj, A., Kouahla, Z., & Farou, B. (2025). A Fuzzy Logic-Driven Semantic and Binary Tree-Based Indexing Framework for Scalable IoT Data Storage and Retrieval. *Informatica*, *49*(24).https://doi.org/10.31449/inf.v49i24.8039

[8] Hu, N., Tian, Z., Lu, H., Du, X., & Guizani, M. (2021). A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3129-3144. https://doi.org/10.1007/s13042-020-01253-w

[9] Breitenbacher, D., Homoliak, I., Aung, Y. L., Elovici, Y., & Tippenhauer, N. O. (2021). HADES-IoT: A practical and effective host-based anomaly detection system for IoT devices (extended version). *IEEE Internet of Things Journal*, *9*(12), 9640-9658. https://doi.org/10.1109/JIOT.2021.3135789

[10] Zachos, G., Mantas, G., Porfyrakis, K., Bastos, J. M. C., & Rodriguez, J. (2025). Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation and ML Algorithms Evaluation. *IEEE Access*.. https://doi.org/10.1109/ACCESS.2025.3547572

[11] Nalini, M., Yamini, B., Fernandez, F. M. H., & Priyadarsini, P. U. (2024). Enhancing anomaly detection Efficiency: Introducing grid searchbased multi-population particle Swarm optimization algorithm based optimized Regional based Convolutional neural network for robust and scalable solutions in High-Dimensional data. *Biomedical Signal Processing and Control*, *96*, 106651.https://doi.org/10.1016/j.bspc.2024.106651

[12] Wang, B., Hua, Q., Zhang, H., Tan, X., Nan, Y., Chen, R., & Shu, X. (2022). Research on anomaly detection and real-time reliability evaluation with the log of cloud platform. *Alexandria Engineering Journal*, *61*(9), 7183-7193.https://doi.org/10.1016/j.aej.2021.12.061

[13] Zacaron, A. M., Lent, D. M. B., da Silva Ruffo, V. G., Carvalho, L. F., & Proença Jr, M. L. (2024). Generative adversarial network models for anomaly detection in software-defined networks. *Journal of Network and Systems Management*, *32*(4), 93. https://doi.org/10.1007/s10922-024-09867-z

[14] Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Aggoun, A. (2022). Super learner ensemble for anomaly detection and cyber-risk quantification in industrial control systems. *IEEE Internet of Things Journal*, *9*(15), 13279-13297.https://doi.org/10.1109/JIOT.2022.3144127

[15] Soni, R., Soni, S., & Nagwanshi, K. K. (2025). Efficient cluster-based deep anomaly detection based traffic analysis and multi-objective optimization for smarter traffic control. *Evolving Systems*, *16*(1), 5.https://doi.org/10.1007/s12530-024-09636-y

[16] Hadi, H. J., Adnan, M., Cao, Y., Hussain, F. B., Ahmad, N., Alshara, M. A., & Javed, Y. (2024). ikern: Advanced intrusion detection and prevention at the kernel level using ebpf. *Technologies*, *12*(8), 122.. https://doi.org/10.3390/technologies12080122