Sound & Vibration 2025, 59(2), 2144.
https://doi.org/10.59400/sv2144

Article

Improve the safety and performance of internet of things assessment devices: From vibration characteristics, interpretable method of knowledge, and combining data

Chafaa Hamrouni[1,*], Aarif Alutaybi[1], Ghofrane Ouerfelli[2], Nahaa Eid B Alsubaie[3]

[1] Department of Computer Sciences, Taif University-Khurma University College, Khurma 2935, Kingdom of Saudi Arabia
[2] Department of Physics- Khurma University College, Taif University, Taif 11099, Kingdom of Saudi Arabia
[3] Department of Mathematics and Statistics, College of University College of Khurma, Taif University, Taif 21944, Kingdom of Saudi Arabia
*** Corresponding author:** Chafaa Hamrouni, cmhamrouni@tu.edu.sa

CITATION

Hamrouni C, Alutaybi A, Ouerfelli G, Alsubaie NEB. Improve the safety and performance of internet of things assessment devices: From vibration characteristics, interpretable method of knowledge, and combining data. Sound & Vibration. 2025; 59(2): 2144.
https://doi.org/10.59400/sv2144

ARTICLE INFO

Received: 8 November 2024
Accepted: 11 March 2025
Available online: 18 March 2025

Abstract: This research focuses on enhancing the safety, reliability, and performance of IoT devices by optimizing the vibration characteristics of materials and noise control. We analyze materials' vibration-damping properties to minimize mechanical resonance and ensure stable operation. By evaluating stiffness and resistance to deformation under dynamic stress, we examine the impact of vibration modulus on device reliability. Our study explores how damping and modulus influence vibrational energy propagation, noise reduction, and acoustic clarity. To integrate domain knowledge with real-time data, we develop interpretable methods that provide actionable insights into the mechanical-acoustic relationship. Compared with other established IoT security assessment techniques, this method has more effectiveness and superiority. Hybrid materials combining elastic matrices with rigid reinforcements are developed to fine-tune mechanical and acoustic properties for IoT applications, such as industrial systems or wearable devices. Vibration analysis is applied to predict performance under real-world conditions, improving safety and efficiency. Efforts are directed toward reducing vibrational noise and enhancing sound transmission for devices like smart speakers and voice recognition systems, ensuring a better user experience and greater functional accuracy.

Keywords: belief rule base with interpretability; belief rule base; computer-aided engineering; dynamic measurement and structural analysis; environment optimization algorithm; internet of things; noise control application; vibration characteristics analysis

1. Introduction

Vibration characteristics play a crucial role in the safety [1], reliability, and performance of IoT devices. Analyzing these characteristics involves evaluating parameters such as vibration damping and modulus, which impact the mechanical stability and acoustic behavior of materials [2]. Vibration damping refers to a material's ability to absorb and dissipate vibrational energy, minimizing resonance and ensuring stable operation. Enhanced damping reduces unwanted vibrational noise, which could otherwise interfere with IoT sensors, transducers, or communication systems [3]. The vibration modulus, representing stiffness during oscillatory motion, is equally important. Optimized modulus values improve resistance to deformation under dynamic stress, contributing to device durability and reliability.

This study integrates vibration analysis into IoT safety assessment by combining domain knowledge and real-time data to optimize mechanical and acoustic properties [4]. For instance, materials with high damping properties can reduce noise transmission and enhance sound insulation, which is critical for devices like smart speakers, wearable technology, and environmental monitoring systems [5]. Hybrid materials, combining elastic and rigid elements, are developed to fine-tune these properties, ensuring stability and functionality in dynamic environments [6].

Existing IoT safety assessment models include black-box, white-box, and grey-box approaches. While black-box models excel in accuracy, they lack interpretability, and white-box models, despite being more transparent, often fail to handle complex datasets [7]. Grey-box models, like the belief rule base with interpretability (BRB-i), strike a balance between accuracy and interpretability. The BRB-i model uses a combination of expert knowledge and data to address the challenges of uncertainty and small sample sizes. By incorporating interpretable constraints, the BRB-i model enhances transparency and aligns optimized parameters with real-world systems.

This work proposes a comprehensive IoT safety assessment framework using the BRB-i model. It includes an interpretable optimization algorithm, material analysis for vibration damping and modulus, and hybrid material development for acoustic optimization. These contributions aim to improve device safety, reliability, and performance in industrial and consumer IoT applications. The rest of the paper is organized as follows: Section 1 reviews existing IoT safety models and their limitations; Section 2 identifies key challenges in BRB-i model construction; Section 3 defines interpretability criteria and describes the structural safety model; and Section 4 validates the framework through experimental data. Finally, conclusions and future directions are presented.

The main contributions of this research are as follows:

1) Development of an interpretable IoT Safety assessment model: We propose a belief rule base with interpretability (BRB-i) model that combines domain knowledge and real-time data to ensure accurate and interpretable safety assessments for IoT systems.
2) Design of an optimization algorithm with interpretable constraints: An optimization algorithm is introduced to enhance the accuracy of the BRB-i model while aligning optimized parameters with real-world system requirements and expert knowledge.
3) Analysis and optimization of vibration characteristics: We analyze and optimize the vibration damping and modulus properties of materials to minimize mechanical resonance, reduce noise, and improve device stability and reliability.
4) Development of hybrid materials for IoT applications: Advanced hybrid materials combining elastic and rigid components are developed to fine-tune mechanical and acoustic properties, enabling improved performance in dynamic IoT environments such as industrial systems and wearable devices.
5) Validation through real-world scenarios: The proposed BRB-i model and material optimization methods are validated using experimental data, demonstrating their effectiveness in enhancing the safety, reliability, and acoustic performance of IoT devices.

1.1. Problem description

We are going to bring up the problems that should be solved to construct the belief rule base with an interpretability-based IoT structure safety assessment model.

Problem 1: The first problem to be solved is how to develop a well-structured and interpretable safety assessment model for the Internet of Things (IoT). Current research demonstrates that belief rule base (BRB)-based IoT safety assessment models with strong interpretability achieve two critical objectives: Preservation of optimal decisions: These models retain optimal decision-making capabilities for complex operational commands; Enhanced structural transparency: Simultaneously, they enable systematic control while providing critical insights into the IoT architecture. The process of constructing the interpretable IoT structure safety assessment model can be represented by the following nonlinear functions:

$$y = \mathrm{assessModel}(\mathrm{input}, \vartheta) \tag{1}$$

where: y stands for expected utility value; $\mathrm{assess\,Model}(\cdot)$ represents the interpretable structure safety assessment model; input represents the input index of the structure safety assessment model; and ϑ represents the set of parameters in the process of the structural safety assessment model.

The proposed problem solution is presented in Sections 3.1 and 3.2.

Problem 2: The second problem is tended to solve how to develop an interpretable optimization model for the parameters of the belief rule base. Taking into consideration that the IoT structural safety assessment model based on belief rule base is interpretable, it contrasts with the current optimization algorithms for belief rule base, which only improve the model accuracy and not the interpretability. As a result, the optimization model can damage the interpretability of the initial belief rule base. Moreover, the expert knowledge cannot be effectively utilized; the optimized parameters are unreasonable back to the optimized belief rule that does not correspond to the actual IoT structure. Therefore, it is necessary to design an optimization model that can improve the accuracy of the model while maintaining interpretability. The IoT optimization process of the safety assessment model can be represented as the following nonlinear function:

$$\theta_{\mathrm{best}} = \mathrm{optimize}(\vartheta, \kappa) \tag{2}$$

where θ_{best} is the optimal parameter set optimized by the optimization model of the structure safety assessment; $\mathrm{optimize}(\cdot)$ is the structure safety assessment optimization model; and κ is a set of parameters that appear in the optimization model. The proposed problem solution is in Section 3.4.

1.2. IoT safety structural model based on belief rule base

As an expert system, the BRB can make full use of quantitative data and qualitative knowledge in the modeling process and express the uncertain information in the form of a belief distribution. The BRB-based safety assessment model is interpretable in the process of modeling and reasoning. And it can reach good modeling results in the small samples. Here, it discusses the interpretability of the structural safety model based on BRB from the modeling and the reasoning aspects:

Modeling interpretability: Expert knowledge derived from long-term practice serves as a crucial source for the interpretable modeling process. Therefore, the interpretability of the knowledge base is of particular significance. In the Belief Rule Base (BRB), a set of rules forms the knowledge base, which features complete rules, is concise and easy to comprehend, and has clear parameter meanings.

Interpretability of reasoning: The interpretability of the process is also highly important. The structural safety model with an interpretable knowledge base has the characteristics of the Internet of Things (IoT). Its interpretability is mainly manifested in the following aspects:

a) ER demonstrates excellent processing and description capabilities for uncertain information presented in the form of belief distribution, and it offers clear explanations;
b) ER can integrate uncertainty information; uncertainty can be updated by new information and finally make decisions;
c) Feasibility of the assessment process: ER reasoning has the ability to handle multiple pieces of information concurrently. For example, it can deal with natural-language-based information like "If A and B, then C". ER can simultaneously combine qualitative judgment and quantitative uncertainty data information;
d) Traceability of the calculation process. The calculation process of the ER algorithm is clear, and every step can be traced and explained.

The structure safety assessment model of smart buildings based on a belief rule base with interpretability (BRB) is meant to explain the ability of the model to express the system behavior in an understandable way. The system behavior is beneficial to improve the degree of interaction between them.

The process of model construction is transparent. Additionally, the principal design of the actual smart building, the knowledge gained from long-term practice, and the arrow structure system can be integrated into the structure of the model.

The model can be traceable in the reasoning process; it can keep the rationality and transparency of the reasoning steps.

The model can keep all the characteristics mentioned previously from being destroyed in the optimization process and reconcile the optimized parameters with their physical meaning and characteristics in a peaceful way. Consequently, we will reach the target of the interaction between people, the established model, and improve the credibility of the model. The IoT interpretable structure is important for discovering the factors affecting safety in time and avoiding further danger. In the IoT safety assessment model, expert knowledge can be effective and interpretable. The inference engine, expert knowledge base, and optimization model constitute the IoT structure safety assessment model. Among them, the interpretable proposed optimization model constraints can maintain the rationality of the optimized parameters and make full use of the expert knowledge, which is recognized by every expert. The overall structure of the proposed BRBi mode is shown in **Figure 1**.

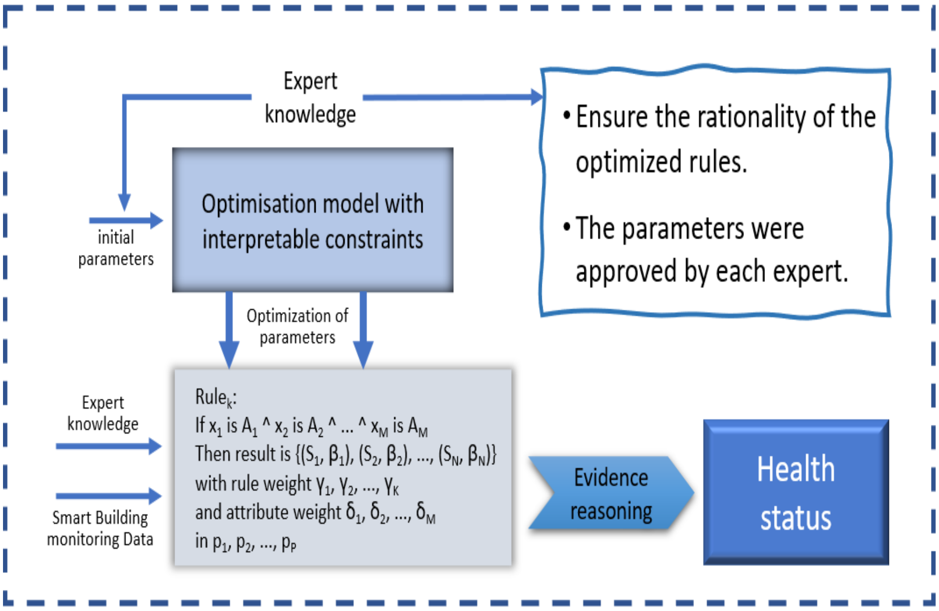
Expert knowledge
• Ensure the rationality of the optimized rules.
• The parameters were approved by each expert.
initial parameters
Optimisation model with interpretable constraints
Optimization of parameters
Expert knowledge
Smart Building monitoring Data
Rule$_k$:
If x_1 is A_1 ^ x_2 is A_2 ^ … ^ x_M is A_M
Then result is $\{(S_1, \beta_1), (S_2, \beta_2), \ldots, (S_N, \beta_N)\}$
with rule weight $\gamma_1, \gamma_2, \ldots, \gamma_K$
and attribute weight $\delta_1, \delta_2, \ldots, \delta_M$
in $p_1, p_2, \ldots, p_P$
Evidence reasoning
Health status

Figure 1. Overall structure of BRB-i model.

To address the gaps identified in Section 1.2 regarding the theoretical and mathematical foundations of the BRB-i model, several strategic enhancements are proposed. First, the mathematical underpinnings of the BRB model must be expanded. This includes a formal definition of its core components—rule bases, weights, and belief degrees—and their roles in handling uncertainty. The model's capability to quantify and propagate uncertainty should be elaborated, supported by equations that illustrate how it processes data and generates interpretable outcomes, especially in complex IoT scenarios.

Second, the role of the Evidential Reasoning (ER) algorithm should be clarified. Its foundation in evidence theory and ability to handle uncertainty should be detailed, with examples or mathematical validations to demonstrate its accuracy in uncertain and dynamic environments. Providing a visual representation, such as a flowchart or pseudocode, would help in understanding how the ER algorithm integrates into the BRB-i model.

Third, practical examples and case studies should be included to showcase the BRB-i model's real-world applicability. These could involve IoT scenarios like identifying vulnerabilities in devices or handling noisy and incomplete data, emphasizing the model's robustness. Finally, a comparison with alternative approaches, such as fuzzy logic or Bayesian networks, should highlight the BRB-i model's superiority in uncertainty management and interpretability. Using performance metrics like accuracy, processing efficiency, and scalability would substantiate these claims.

Implementing these improvements will provide a comprehensive understanding of the BRB-i model and the ER algorithm, demonstrating their practical effectiveness and robustness. These revisions will not only strengthen the paper's theoretical foundation but also establish the BRB-i model as an innovative and practical tool for advancing IoT security assessment.

The mathematical foundation of the Belief Rule Base (BRB) model, which underpins its capability to manage uncertain information, has not been thoroughly elaborated [8]. Specifically, the theoretical constructs that enable the BRB model to quantify and propagate uncertainty in decision-making processes remain unexplained. Furthermore, the accuracy guarantees provided by the Evidential Reasoning (ER) algorithm, particularly in addressing complex and uncertain scenarios, are not discussed. The omission of these aspects leaves a critical gap in understanding how the BRB model and ER algorithm collaborate to deliver reliable and interpretable outcomes in intricate systems. To ensure clarity and robustness, it is essential to detail the probabilistic reasoning and evidential synthesis mechanisms within the BRB framework and to validate the ER algorithm's performance through theoretical proofs or empirical analyses.

The BRB-i model, introduced as a framework for IoT safety assessment, has been shown to effectively integrate qualitative knowledge with quantitative data. It expresses uncertain information as belief distributions, making it well-suited for scenarios with limited data samples. While the model is described in Section 1.2, further elaboration on its theoretical foundations is necessary to enhance understanding, particularly regarding its mathematical basis for handling uncertainty and the Evidential Reasoning (ER) algorithm's guarantees for accuracy in complex situations.

Mathematical basis of the BRB-i model: The BRB-i model utilizes a belief distribution framework to represent and process uncertain information, offering a robust method for combining qualitative expert insights with quantitative data. This mathematical basis enables the model to construct a knowledge base comprising interpretable rules, where each parameter is explicitly defined and grounded in real-world relevance. Such a foundation ensures that the safety assessment model remains transparent and traceable during both its construction and application.

Accuracy and effectiveness of the ER algorithm: The ER algorithm, a core component of the BRB-i model, provides a structured approach to reasoning under uncertainty. It excels at integrating various sources of information, whether qualitative judgments or quantitative data, by updating beliefs based on new evidence [9]. The algorithm guarantees accuracy by employing a clear, traceable calculation process, where each step can be audited and explained. This property is critical for ensuring that decisions made by the model are both rational and justifiable.

Interpretability in modeling and reasoning: The interpretability of the BRB-i model stems from its ability to balance expert knowledge with empirical data:

1) **Modeling interpretability**: Expert-derived rules form a concise, easy-to-understand knowledge base, ensuring that all parameters retain their physical meaning during optimization.
2) **Reasoning interpretability**: The ER algorithm enhances the reasoning process by supporting traceability, combining natural language statements with quantitative data, and offering clear, step-by-step explanations of the decision-making process.

By integrating these elements, the BRB-i model ensures that IoT safety assessments remain transparent, reliable, and aligned with real-world scenarios [10]. Furthermore, the model's interpretability facilitates timely identification of safety risks in IoT systems, aiding in proactive risk mitigation. This approach not only enhances model credibility but also fosters effective interaction between users, the model, and its outcomes.

1.2.1. Construction of interpretable criteria

In Ref. [11], the general interpretability criteria are described. Based on these interpretability criteria, the interpretability criteria based on the IoT structural safety models are defined, and six criteria are specifically defined, as shown in **Figure 2**.

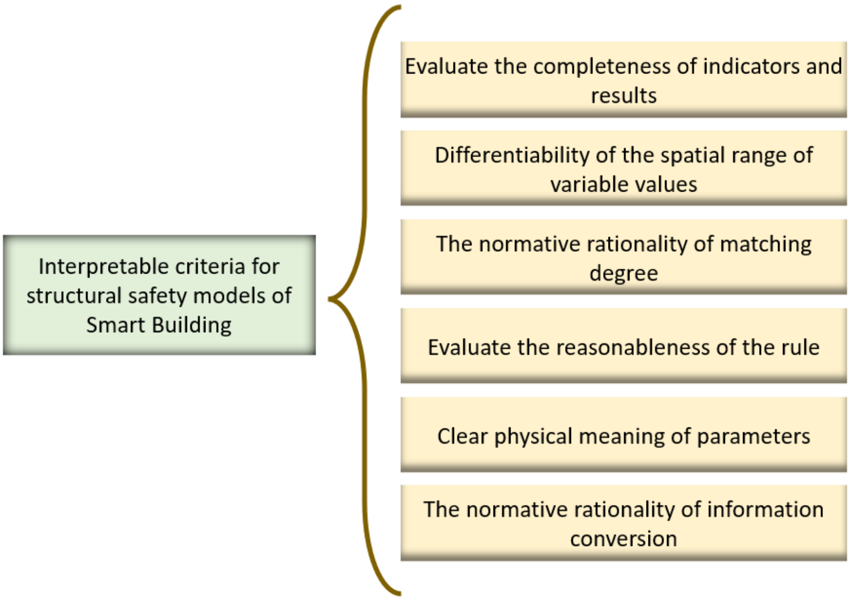
Interpretable criteria for structural safety models of Smart Building
Evaluate the completeness of indicators and results
Differentiability of the spatial range of variable values
The normative rationality of matching degree
Evaluate the reasonableness of the rule
Clear physical meaning of parameters
The normative rationality of information conversion

Figure 2. Interpretability criteria diagram.

1.2.2. Belief rule with interpretability model exploration

The belief rule base with the interpretability model is based on a set of "IF-Then" rules that together constitute an interpretable belief rule base-based assessment model. The following equal can describe the relationship between the IoT assessment index safety assessment model and its safety state:

$$\begin{array}{l} \text{Rule}_k\text{: If } x_1 \text{ is } A_1 \wedge x_2 \text{ is } A_2 \wedge \ \dots \ \wedge x_M \text{ is } A_M, \\ \text{Then result is with rule weight } \gamma_1, \gamma_2, \dots, \gamma_K \\ \quad \{(S_1, \beta_1), (S_2, \beta_2), \dots, (S_N, \beta_N)\}, \\ \quad \text{and attribute weight } \delta_1, \delta_2, .., \delta_M \\ \quad \text{in } p_1, p_2, \dots, p_P \end{array} \tag{3}$$

where:

M denotes the number of assessment indicators;

$x_i(i = 1, \dots \dots \dots . . \dots . , M)$ is the IoT assessment index data structure safety.

$A_i(i = 1 \cdots M)$ represents the reference value corresponding to the safety assessment index;

N denotes the number of assessment results of the smart building data structure safety assessment model.

$S_i(i = 1, \dots . , N)$ represents the safety assessment results of the BRB-i model.

$\beta_i(i = 1, \dots . , N)$ represents the corresponding belief degree of each assessment result.

K represents the number of rules.

$\gamma_i(i = 1 ... K)$ represents the weight of the rule.

$\delta_i(i = 1 \cdots M)$ denotes the attribute weight of the structure assessment index.

P represents the number of interpretability criteria based on the BRB-i model.

$p_i(i = 1 ... P)$ represents each interpretability criterion.

Remark 1: Compared with the traditional BRB, the BRB-i model defines interpretable criteria and adds interpretable constraints in the optimization process, which makes the model more suitable and interpretable for engineering applications.

1.2.3. Inference of the BRB-i model

The inference process of the BRB-i model consists of the following four steps.

1) Calculating the rule matching degree
2) Calculating the rule activation weight.
3) The reasoner uses evidential reasoning.
4) The expected utility value is calculated to obtain the final assessment result.

The reasoning process flow chart of the assessment model is shown in **Figure 3**.

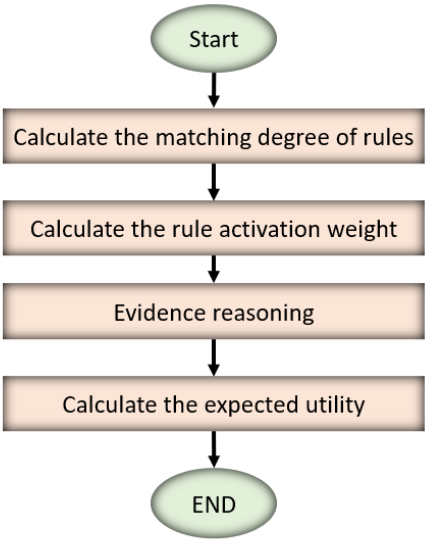
Start
Calculate the matching degree of rules
Calculate the rule activation weight
Evidence reasoning
Calculate the expected utility
END

Figure 3. Inference process of BRB-i model.

The reasoning process of the BRB-i model is shown as follows:

(1) Calculating the matching degree of rules. It refers to the matching degree between the input sample data information and the rule. The calculation of the rule matching degree is mainly to complete the transformation of input data. According to the different properties of the premise attributes, the transformation, including qualitative attributes, quantitative attributes, and symbolic attributes, is completed [12]. The calculation is as follows:

$$\varepsilon_i^k = \begin{cases} \dfrac{A_i^{l+1} - x_i}{A_i^{l+1} - A_i^l} & k = l, A_i^l \leq x_i \leq A_i^{l+1} \\ 1 - \varepsilon_i^k & k = l + 1 \\ 0 & k = 1 \cdots K, k \neq l, l + 1 \end{cases} \tag{4}$$

where the matching degree of the i-th assessment index to the k-th rule is denoted as ε_i^k; the sample data of the i-th assessment index is denoted as x_i; and the reference value of the i-th assessment indicator under rule l is denoted as A_i^l.

(2) The activation weight of the rule. The combination of different attributes and different reference values generates each rule of BRB. The activation weight of the rule can be calculated through the following equation:

$$w_k = \frac{\gamma_k \prod_{i=1}^{M} (\varepsilon_i^k)^{\delta_i}}{\sum_{i=1}^{K} \gamma_l \prod_{i=1}^{M} (\varepsilon_i^l)^{\delta_i}} \tag{5}$$

where the rule activation weight under rule k is denoted by w_k.

(3) Use evidence reasoning to fuse activation rules [13]. Yang proposed the ER analytical method in 2007 as the inference method of this step, and the belief distribution of the output can be obtained after the rule fusion [14].

The belief degree of the n-th result S_n in the final belief distribution result set can be expressed as β_n:

$$\beta_n = \frac{\mu \times \left[\prod_{i=1}^{L}\left(w_l \beta_{n,l} + 1 - w_l \sum_{i=1}^{N} \beta_{i,l}\right) - \prod_{l=1}^{L}\left(1 - w_l \sum_{i=1}^{N} \beta_{i,l}\right)\right]}{1 - \mu \times \left[\prod_{l=1}^{L}(1 - w_l)\right]} \tag{6}$$

$$\mu = \frac{1}{\sum_{n=1}^{N} \prod_{l=1}^{L}\left(w_l \beta_{n,l} + 1 - w_l \sum_{i=1}^{N} \beta_{i,l}\right) - (N-1) \prod_{l=1}^{L}\left(1 - w_l \sum_{i=1}^{N} \beta_{i,l}\right)} \tag{7}$$

Once all the rules are integrated, the output belief distribution set of BRB can be acquired as follows:

$$G(x) = \{(S_n, \beta_n); n = 1, \ldots, N\} \tag{8}$$

where the output belief distribution set of BRB is denoted as $G(x)$.

(4) Output utility value calculation. The final output of the BRB model can be expressed as:

$$u\big(G(x)\big) = \sum_{n=1}^{N} u(S_n)\, \beta_n \tag{9}$$

where:

$u\big(G(x)\big)$ represents the expected utility value of the outcome of set $G(x)$.

$u(S_n)$ represents the utility value of outcome S_n.

1.2.4. Optimization of BRB-i model

Due to the complex system environment, its real health state is difficult to accurately describe. After the modeling and reasoning process, the parameters of the model can be destroyed by the optimization process.

Consequently, there is a need to devise an optimization algorithm that can enhance accuracy and is interpretable. To achieve this, a novel optimization algorithm featuring interpretable constraints is proposed. This algorithm clarifies the meaning of parameters. The IoT data optimization algorithm with interpretable constraints can thoroughly and efficiently utilize expert knowledge. It enables the actual system to align with the optimized belief distribution and offers interpretability. The flow chart of the proposed algorithm for the BRB-i model is illustrated in **Figure 4**. It is true that the proposed optimization algorithm succeeds in improving the model accuracy, but it fails to maintain the interpretability in some parameters. This can be explained in the following way:

1) The optimization algorithm does not make full use of expert knowledge, which is an important source of the established model interpretability. The optimization algorithm scatters points randomly; it deviates from the interpretability.
2) The rules optimized (as a source of accuracy and interpretability) should not conflict with the existing actual system, but in this figure, some optimized rules cannot match the significance of the actual IoT structure safety system.
3) Certain optimized belief degrees are irrational and exceed the range of practical implications. Thus, it is essential to enhance the optimization algorithm to some degree to render it interpretable. The flowchart of the enhanced optimization algorithm is presented in **Figure 4**, and its procedure is as follows:
    a) Parameter initialization: The data error value is d, and the number of iterations is set to g.
    b) Set the scatter mode: In this step, the data optimization algorithm based on the random scattering mode is discarded. And established a new scattering mode. The novel approach for scattering points involves distributing them in the area adjacent to the expert knowledge. In this way, expert knowledge can be effectively utilized to achieve interoperability. If the optimization algorithm for the current data error value is represented by η, which indicates the set of parameters after the modeling and reasoning process, it can be expressed as:

$$\eta_i = \xi_K + (\text{rand}(O, d) - 0.5) \times 2 \tag{10}$$

The belief degree of expert knowledge is ξ_K.

    c) Calculate the adaptive data value: The mean square error is denoted as the objective function; it can be expressed as:

$$\begin{gathered} \min\{\eta = \{\gamma, \delta, \beta\}\} \text{ in } p_1, p_2 \\ s.t. \, 0 \leq \gamma \leq 1, 0 \leq \delta \leq 1, 0 \leq \beta \leq 1 \end{gathered} \tag{11}$$

    d) Set interpretable constraints. Some parameters are optimized by the meaning of the actual system, and the improved algorithm solves this problem by setting interpretable constraints: The specific constraints are as follows:

Limit the value range of the belief and obtain the approval of each expert. Expert knowledge is the accumulation of knowledge on the safety of actual IoT data structure over a long period of practice. Assuming that information is reliable and expert knowledge is authoritative, the value of belief degree should not violate expert knowledge and should be reasonably constrained [15]. This can be expressed as:

$$\beta_{lp} \leq \beta_{n,k} \leq \beta_{up} \; (n = 1, \ldots, N, k = 1, \ldots, K) \tag{12}$$

where the maximum and minimum values of belief approved by each expert are β_{up} and β_{lp}, respectively, and the k-th belief degree of rule$n$ is denoted as $\beta_{n,k}$.

- Make the belief distribution in the optimized rule match with the actual system. Optimized rules may not match the actual system, so it is necessary to set this constraint. This can be expressed as:

$$\begin{gathered}\beta_k \sim R_k (k = 1, \ldots, K) \\ R_k \in \{\{\beta_1 \leq \beta_2 \leq \ldots \leq \beta_N\}, \\ \{\beta_1 \geq \beta_2 \geq \ldots \geq \beta_N\}, \\ \{\beta_1 \leq \ldots \leq max(\beta_1, \beta_2, \ldots,) \geq \ldots \geq \beta_N\}\}\end{gathered} \tag{13}$$

- IoT data error that can be described as follows:

$$D = \mid C{\eta^*}_g - \partial_g \mid \tag{14}$$

$$\eta_{g+1} = {\eta^*}_g - AD \tag{15}$$

where g is the number of current iterations, D is the distance, and ${\eta^*}_g$ is the position vector of the current best solution, and A and C are the coefficient vectors updated in each iteration, which can be obtained by the following formula:

$$A = 2ar_1 - a \tag{16}$$

$$C = 2r_2 \tag{17}$$

$$a = 2 - \frac{2g}{g_{\max}} \tag{18}$$

where a is a temporary variable that decreases linearly from 2 to 0; $g_{\max}$ is the maximum value of iteration times; and r_1 and r_2 are random numbers between 0 and 1.

- This behavior can be expressed by the formula:

$$\eta_{g+1} = {\eta^*}_g + D_p e^{bl} \cos(2\pi l) \tag{19}$$

$$D_p = \left|{\eta^*}_g - \eta_g\right| \tag{20}$$

If l is a random number in the interval $[-1,1]$ and b is the constant of the helical shape.

- Search for data error changes. Randomly searching is based on each other's location, which is described by the following formula:

$$\eta_{g+1} = {\eta^*}_g + D_p e^{bl} \cos(2\pi l) \tag{21}$$

$$D_p = \left|{\eta^*}_g - \eta_g\right| \tag{22}$$

We deduce that the IoT data optimization algorithm with interpretability improves the model accuracy.

Illustrating enhanced optimization with examples:

1) Belief value constraints: Imagine an IoT temperature monitoring system where expert-defined belief degrees range between 0.2 and 0.8. By enforcing these limits, the optimized model avoids generating unrealistic or impractical values, ensuring results align with real-world sensor behavior.

2) Rule alignment: In an industrial safety system, optimized rules must align with existing configurations, such as emergency response protocols. For instance, if a system rule requires activating cooling mechanisms at a specific threshold, the optimized parameters should reflect this requirement to ensure operational compatibility.
3) Error minimization: In a vibration monitoring system, guided search techniques iteratively reduce data errors by adjusting parameters based on real-time feedback. For example, optimization might refine the model to achieve closer alignment between predicted and observed vibration amplitudes, improving system reliability.

When setting interpretable constraints, we determine the exact range of belief values and identify specific values within the BRB-i model. It is essential to use expert knowledge and data-driven analysis. The belief values represent the degree of certainty in a system's parameters and must reflect practical, real-world constraints. The process involves setting upper and lower bounds for these values based on the knowledge accumulated through practice and observations in the relevant domain. For example, in an IoT system monitoring environmental temperature, experts may establish that the belief values should range between 0.2 and 0.8, where 0.2 represents low confidence in abnormal conditions and 0.8 indicates high confidence in normal operating conditions. These bounds can be defined by analyzing historical data, consulting experts, and reviewing system performance under various scenarios. Within this range, specific belief values are determined by considering the system's operational thresholds and applying optimization techniques that minimize data errors without violating practical constraints.

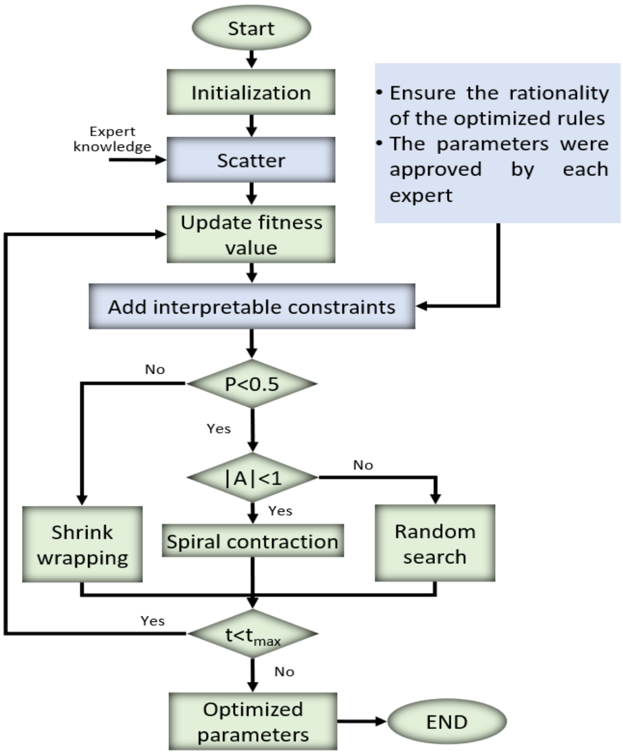

Figure 4. Flowchart of IoT data optimization algorithm with interpretable constraints.

To refine these values, an iterative optimization process is employed, guided by interpretable constraints. The process uses mean square error as an objective function to ensure belief values align with the actual behavior of the system. Constraints ensure that optimized belief degrees are not only within the specified range but also contextually valid—for instance, adhering to safety standards in industrial systems or operational protocols in IoT applications. By combining expert insights and computational adjustments, the exact belief values are tailored to reflect both theoretical and practical system requirements, ensuring accuracy and interpretability.

To understand better the optimization of the BRB-i model described in citation 1.2.4, let’s consider practical examples and expand on the key principles:

Paraphrased explanation with examples

Optimizing the BRB-i model requires ensuring that its rules and belief distributions match real-world system requirements while maintaining interpretability and accuracy. This is achieved through structured constraints, reliance on expert knowledge, and adaptive error minimization. Random scattering of parameters must be avoided; instead, parameter adjustments should align closely with the expertise and practical boundaries of the system:

1) Belief value constraints: Consider an IoT system monitoring factory temperature. Experts might determine that the belief degrees, representing the likelihood of sensor readings, must range between 0.2 and 0.8 to reflect realistic sensor behavior. By enforcing these limits during optimization, the model avoids generating belief values, such as 0.1 or 0.95, which would be considered implausible and undermine interpretability.
2) Rule alignment with operational protocols: In an industrial safety system, optimized rules must reflect critical processes. For instance, if a rule in the system activates cooling mechanisms when the temperature exceeds 70 ℃, the optimized parameters must preserve this threshold. A deviation to 75 ℃ during optimization might compromise safety, making it crucial to align optimization with real-world rules.
3) Iterative error minimization in dynamic systems: Take a vibration monitoring system as an example. The optimization algorithm iteratively adjusts parameters to minimize the error between predicted and observed vibration amplitudes. For instance, if the model predicts a vibration level of 0.8 while actual sensors report 0.6, the optimization process refines parameters to reduce this gap, enhancing the system’s predictive accuracy.
4) Expert-informed parameter scattering: During optimization, scattering points should occur within regions defined by expert knowledge. For example, in a structural health monitoring system, experts might identify specific ranges for stress levels in materials. The optimization algorithm scatters points only within these ranges, ensuring results are consistent with the material’s known properties.

We conclude that by using belief constraints, aligning rules with real-world protocols, iteratively minimizing errors, and leveraging expert-informed adjustments, the BRB-i model becomes both interpretable and accurate. These enhancements ensure that the optimized model remains meaningful, practical, and reliable for real-world applications.

To ensure the optimization rules of the BRB-i model align precisely with the actual system, the optimization algorithm must integrate interpretability and accuracy through structured constraints and expert knowledge. Random scattering of parameters should be replaced with a targeted approach that confines adjustments to expert-defined ranges, ensuring practical and realistic outputs. Constraints must be imposed to keep belief values within authoritative limits, align optimized rules with operational protocols, and iteratively minimize data errors while maintaining interpretability. For instance, in IoT systems, belief degrees should stay within specified bounds, such as 0.2 to 0.8 for temperature monitoring, to avoid impractical results. Furthermore, the optimization process should refine parameters through adaptive methods, minimizing discrepancies between predictions and observations without violating real-world constraints. By addressing these aspects, the algorithm ensures the optimized model reflects the actual system's logic while preserving its accuracy.

2. Research and experimental applications

This section describes the methodologies and experiments conducted to optimize vibration characteristics and material properties for IoT devices. The study leverages interpretable methods, domain expertise, and real-world data to ensure actionable and reliable assessments.

2.1. Study of vibration damping properties

The IoT safety assessment model is based on the Belief Rule Base with Interpretability (BRB-i) framework, which integrates belief rule systems, real-world data, and expert knowledge to provide transparent, traceable reasoning processes [16]. Unlike binary models, BRB-i delivers nuanced, real-value outputs, allowing for the capture of subtle variations critical for assessing IoT systems in dynamic environments. Enhancing vibration damping properties enables materials to absorb and dissipate energy effectively, reducing mechanical resonance and vibrational noise [17]. These improvements are vital for applications like industrial machinery sensors or communication modules, where vibrational interference can compromise performance. The interpretability of the BRB-i model ensures engineers can address uncertainties while iteratively refining the model for reliable assessments.

2.2. Vibration modulus

The vibration modulus is a critical parameter that measures a material's stiffness under dynamic stress. Materials with a high modulus resist deformation, ensuring structural durability in applications such as accelerometers or wearable devices [18]. This parameter also governs the propagation of vibrational energy, influencing mechanical and acoustic interactions. For example, selecting materials with appropriate stiffness can prevent resonance and mechanical fatigue in industrial IoT systems, extending device longevity [19]. Balancing stiffness with flexibility allows engineers to optimize material performance across diverse environments. Interpretable methods facilitate a transparent evaluation of the vibration modulus's impact on device reliability and operational efficiency [20].

2.3. Impact on acoustic behavior

The interplay between vibration damping and stiffness significantly influences acoustic performance, including noise reduction, sound insulation, and clarity. High-damping materials dissipate vibrational energy, reducing noise, while optimized stiffness ensures precise sound propagation [21]. These properties are particularly important for devices like smart speakers and voice recognition systems, where acoustic quality directly affects user experience [22]. Using interpretable methods, engineers can optimize material configurations, preventing excessive damping that may degrade sound quality or excessive stiffness that could amplify noise [23].

2.4. Tailoring and integrating material properties in IoT safety frameworks

Customizing material properties enhances IoT device functionality, reliability, and safety. High-damping materials reduce vibrational interference, while optimized stiffness ensures stability under mechanical stress [24]. Hybrid materials, combining elastic matrices with rigid reinforcements, balance flexibility and rigidity, making them ideal for wearable devices or industrial IoT systems [25]. Advanced composites allow engineers to tailor properties to specific environments, such as transportation systems, where continuous motion and vibrations necessitate robust materials. Incorporating vibration analysis into IoT safety frameworks enables engineers to predict performance under real-world conditions, analyzing parameters like damping and stiffness to mitigate risks and maintain stability [26]. For instance, Zhu et al. demonstrated how vibration analysis improved safety in industrial IoT systems exposed to heavy machinery vibrations [27]. Tailored materials enhance device longevity and functionality in demanding environments, ensuring alignment with operational needs through interpretable methods and data-driven design choices [28].

Although the manuscript highlights the importance of IoT security assessment, it does not fully address how the models introduced later are integrated within a specific theoretical framework for IoT system security. Greater emphasis could be placed on proposing mechanisms to account for the impact of complex interactions among IoT devices on security assessment, thereby enhancing the discussion and practical relevance: More focus should be directed toward proposing mechanisms that effectively address the impact of complex interactions among IoT devices on security assessments. IoT systems involve interconnected devices that communicate and share data in dynamic environments, which can lead to multifaceted security challenges. For instance, vulnerabilities in one device can propagate across the network, amplifying potential risks. By developing mechanisms that model and analyze these interactions, security assessments can become more comprehensive and accurate. These mechanisms could include network simulation tools, behavioral analytics for device interactions, and predictive algorithms that identify potential cascading vulnerabilities. Incorporating such approaches would not only enhance the depth of the discussion but also significantly improve the practical applicability of the research, making it more relevant for real-world IoT security challenges.

3. Study, development and evaluation steps

The main purpose of this paper is to build a structured IoT safety assessment model data based on BRB with interpretability. The structure safety assessment index system is shown in **Figure 5**. Therefore, some possible security risks will be experimented with and analyzed as performed in Ref. [29].

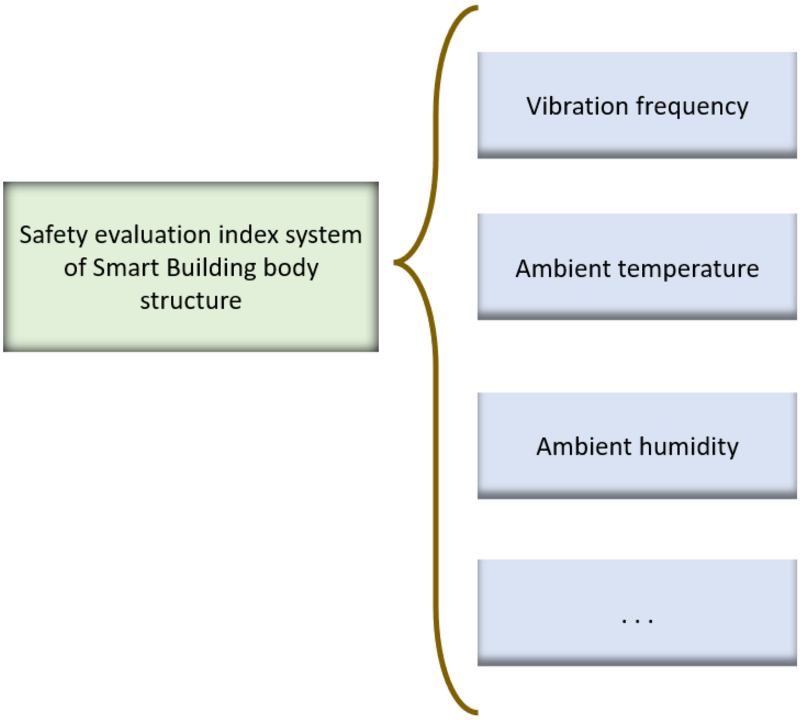
Safety evaluation index system of Smart Building body structure
Vibration frequency
Ambient temperature
Ambient humidity
. . .

Figure 5. Index system for IoT structural safety assessment.

The data used in this experiment are sourced from the wireless sensor platform monitoring system established in the laboratory. A real-world environment is simulated via the simulation process. Given that the ambient temperature and humidity remained relatively stable throughout the experiment, only the data error value of the indexes is taken into account as the assessment and monitoring indicator for the structural safety assessment model in this section.

3.1. Initialization of BRB-i model

According to the IoT data-based structure safety assessment model constructed above, the belief rules are constructed as follows:

$$\begin{array}{l} \text{Rule}_k\text{: If } x_1 \text{ is } A_1 \\ \wedge\, x_2 \text{ is } A_2\text{, Then result is } \{(S_1,\beta_1),(S_2,\beta_2),(S_3,\beta_3),(S_4,\beta_4)\}, \begin{array}{l} \text{with rule weight } \gamma_1,\gamma_2,\ldots,\gamma_K \\ \text{and attribute weight } \delta_1,\delta_2 \\ \text{in } p_1,p_2,\ldots,p_P \end{array} \end{array} \tag{23}$$

where, x_1 and x_2 respectively represent two assessment indexes of variation frequency, δ_1 and δ_2 are their corresponding attribute weights, and S represents the IoT statement data structure safety, which can be divided into four states: normal (S_1), general (S_2), slightly lower (S_3), and low (S_4). A_1 and A_2 are the reference values of the variation degree of IoT data, and the reference values and reference levels given by combining expert knowledge are low (L), slightly low (SL), slightly high (SH), and high (H). The specific situation of the two assessment indexes and the reference value and reference grade of the IoT data structure safety state is shown in **Tables 1–3**.

Table 1. Class and reference value of IoT data frequency.

Reference grade	L	SL	SH	H
Reference value	3.0	6.5	31.50	70.0

All methods are under different proportions of training samples.

Table 2. Class and reference value of IoT data error frequency changes.

Reference grade	L	SL	SH	H
Reference value	0.02	0.03	31.50	0.09

All methods are under different proportions of training samples.

Table 3. Class and reference value of IoT data safety.

Reference grade	S_1	S_2	S_3	S_4
Reference value	1.0	0.75	31.50	0

All methods are under different proportions of training samples.

Furthermore, in the initial model, both the rule weight and attribute weight are set as 1. Considering the reference levels and reference values presented in **Tables 1–3**, **Table 4** shows the initial model for the IoT structural safety assessment data frequency and arrow body.

Four sets of real-world IoT safety state data are provided by on-site experts based on their long-term practical experience. These data reflect the probability of IoT data frequency accidents. Based on the analysis of the IoT safety state, experts determine a relatively reasonable belief distribution for each state considering the actual usage scenarios and historical IoT safety cases. Expert knowledge represents the long-term accumulation of knowledge regarding IoT data frequency, and it serves as a crucial resource for interpreting the BRB expert system [30]. The initial parameters of the model are set using expert knowledge. Subsequently, real-time training data are employed to adjust and refine these parameters, and then the safety evaluation results are generated. The interpretability of the model is gauged by the degree of fit between the initial belief distribution and the output belief distribution. The closer the two distributions are, the higher the interpretability of the model.

3.2. Experimental results

Once the IoT structure safety evaluation model based on interpretable BRB is established, the initial evaluation model will be influenced by the actual working environment and its operational state. This is because of the limitations and uncertainties in expert knowledge, which lead to the low accuracy of the model.

Consequently, when assessing the structural safety of the Internet of Things (IoT), it is crucial to fine-tune the model's parameters to boost the accuracy of the evaluation model. In this experiment, a total of 515 data samples were gathered. Out of these, 450 were employed as training samples for the real-time adjustment and rectification of the model parameters, and the remaining 65 served as test samples.

Table 4. Initial model for IoT structural safety assessment.

Serial number	Variation frequency	Error changes value	Rule weight	Output $\{S_1, S_2, S_3, S_4\}$
1	L	L	1	{0.9995,0.0005,0,0}
2	L	SL	1	{0.51,0.42,0.07,0}
3	L	SH	1	{0.40,0.20,0.20,0.20}
4	L	H	1	{0.53,0.27,0.20,0}
5	SL	L	1	{0.43,0.32,0.25,0}
6	SL	SL	1	{0.45,0.33,0.22,0}
7	SL	SH	1	{0.30,0.23,0.235,0.235}
8	SL	H	1	{0.34,0.22,0.22,0.22}
9	SH	L	1	{0.22,0.26,0.32,0.20}
10	SH	SL	1	{0,0.20,0.52,0.28}
11	SH	SH	1	{0,0.25,0.45,0.30}
12	SH	H	1	{0,0.14,0.46,0.40}
13	H	L	1	{0.06,0.12,0.25,0.57}
14	H	SL	1	{0.12,0.20,0.23,0.45}
15	H	SH	1	{0,0.05,0.35,0.60}
16	H	H	1	{0,0.10,0.30,0.60}

All methods are under different proportions of training samples.

Additionally, the initial setup of the optimization model is detailed as follows: the population size is fixed at 20, the optimization dimension stands at 82, and the number of iterations is 800. **Figure 6** illustrates the fit between the output results of the BRB-i models and the actual values, and **Figure 7** displays the comparison chart of the belief distribution for each rule.

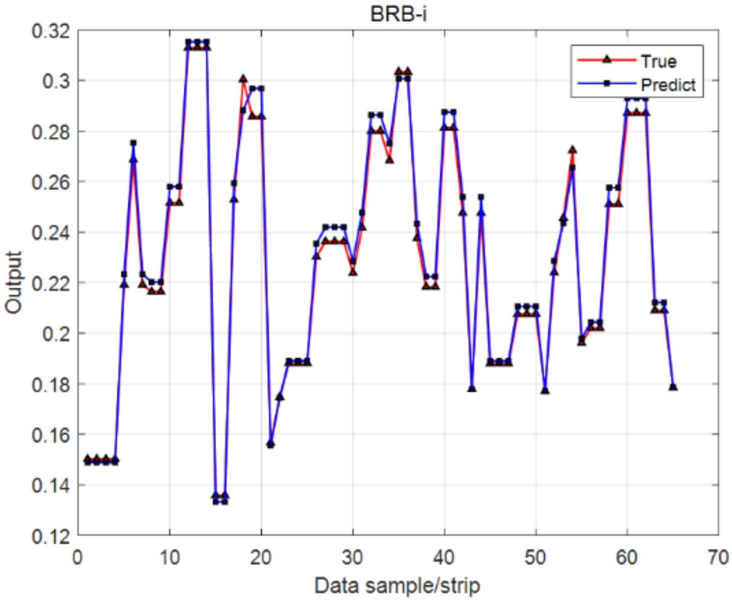

Figure 6. The output result of BRB-i model compared with the real value.

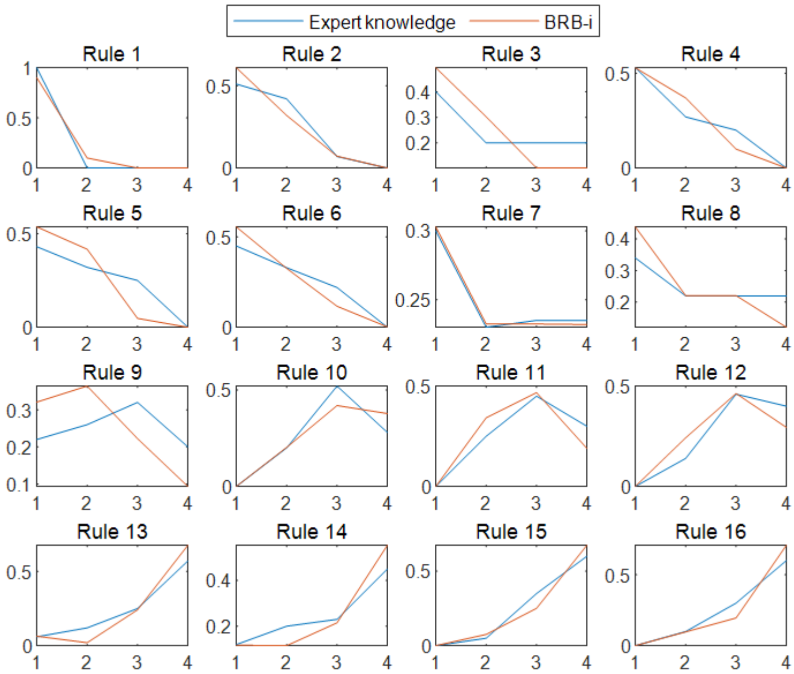

Figure 7. Comparison diagram of belief distribution of each rule in BRB-i.

The output of the optimized rule weight and belief distribution is presented in **Table 5**.

Table 5. Parameter output of optimized BRB-i model.

Serial number	Variation frequency	Error changes value	Rule weight	Output $\{S_1, S_2, S_3, S_4\}$
1	*L*	*L*	0.5602	{0.8997,0.1003,0,0}
2	*L*	*SL*	0.6216	{0.6091,0.3190,0.0719,0}
3	*L*	*SH*	0.1073	{0.4936,0.3022,0.1021,0.1021}
4	*L*	*H*	0.1120	{0.5296,0.3702,0.1002,0}
5	*SL*	*L*	0.4205	{0.5358,0.4167,0.0475,0}
1	*L*	*L*	0.5602	{0.8997,0.1003,0,0}
2	*L*	*SL*	0.6216	{0.6091,0.3190,0.0719,0}

All methods are under different proportions of training samples.

Based on the aforementioned experimental outcomes, the output results of the BRB-i model are highly precise and closely approximate the real values. Additionally, the optimized belief distribution shows a strong fit with the initial belief distribution. This suggests the effectiveness and accuracy of the constructed BRB-i model. The optimization model demonstrates a favorable impact on parameter adjustment and is interpretable.

3.3. Comparative experiments

Addressing Root Causes of Interpretability Issues in Existing Methods: The limitations of traditional methods, such as the radial basis function neural network (RBF) and extreme learning machine (ELM), lie in their inherent design as data-driven approaches. These methods prioritize the accurate mapping of input-output relationships using large datasets but do so at the expense of transparency. Their reliance on complex internal operations, such as non-linear weight adjustments or transformations within hidden layers, renders their decision-making process opaque. As a result, users cannot easily trace or understand how these models generate predictions, nor can they explain the underlying rationale for specific outputs. This "black box" characteristic fundamentally restricts their interpretability.

In contrast, methods that incorporate expert systems, such as the basic BRB and PCMAES-BRB [31], utilize domain knowledge to construct interpretable structures. These approaches allow for human involvement in adjusting belief rules and distributions, offering a greater level of transparency. However, these systems still encounter challenges when applied to highly dynamic or complex environments, such as limited scalability and suboptimal performance in adapting to rapidly changing conditions.

Innovations of the BRB-i model: Addressing Interpretability Challenges: The BRB-i model represents a step forward by merging the strengths of expert systems with the adaptability of data-driven techniques. Its primary innovation lies in its dynamic adjustment of belief rules through optimization algorithms, such as those based on evolutionary strategies. This mechanism enables the BRB-i model to refine its belief distributions in alignment with both expert insights and empirical data, as demonstrated in **Figures 8** and **9**. The incorporation of the Evidential Reasoning (ER) framework further enhances the model's ability to handle uncertainty while maintaining interpretability.

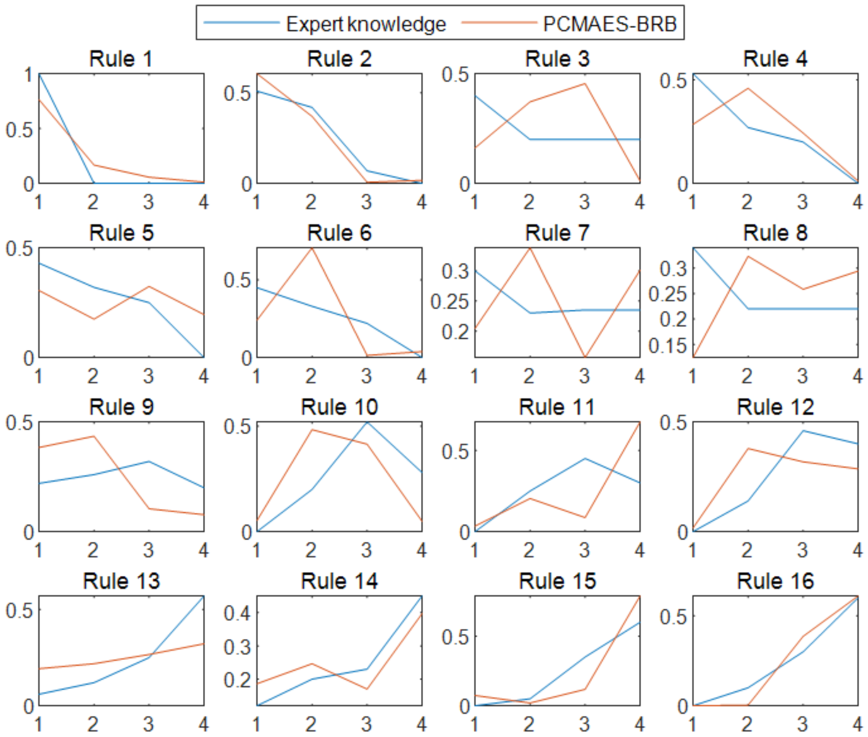

Figure 8. Comparison diagram of the belief distribution of each rule in PCMAES-BRB.

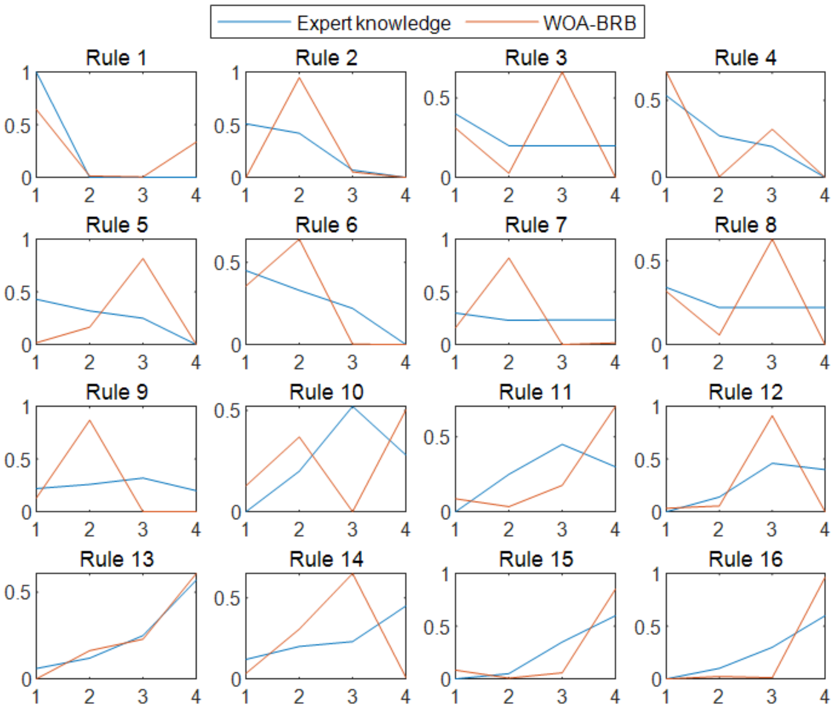

Figure 9. Comparison diagram of belief distribution of each rule in BRB.

Unlike RBF and ELM, which lack mechanisms for integrating expert knowledge or offering interpretable outputs, the BRB-i model ensures that its decision-making process is both transparent and justifiable. The belief distributions are not static; they evolve based on new data, reflecting a balance between human expertise and data-driven optimization.

Empirical support for the BRB-i model's superiority: Accuracy and performance: Experimental results across different training sample proportions (**Table 6**) highlight the BRB-i model's superior predictive accuracy. At 85% training data, the BRB-i model achieves an error rate of 0.0063, outperforming other methods, including PCMAES-BRB (0.0032), RBF (0.0074), and ELM (0.0072). This consistent performance illustrates the model's robustness in capturing complex relationships within data while maintaining its interpretability.

Optimization efficiency: **Table 7** underscores the BRB-i model's effectiveness in parameter optimization. With 800 iterations and a population size of 30, the model reaches its optimal accuracy (0.0012). Beyond this threshold, further increases in iterations or population size do not significantly improve performance, reflecting the model's computational efficiency.

Comparative interpretability: **Figures 8–13** compare the models' interpretability. While RBF [32] and ELM models demonstrate good accuracy, their outputs lack the interpretability required for critical applications. In contrast, the BRB-i model provides a clear visual and numerical comparison between initial expert-defined belief distributions and those adjusted during optimization. This traceability ensures that the outputs are aligned with both empirical data and expert knowledge, bridging the gap between theoretical rigor and practical usability.

Enhancing the innovative impact of the BRB-i model: By addressing the root causes of interpretability limitations in existing methods, the BRB-i model establishes itself as a significant advancement in security assessment frameworks. Its integration of dynamic belief rule adjustments, expert knowledge, and robust optimization mechanisms makes it uniquely capable of providing both accurate and explainable results. These features are particularly critical for applications such as IoT security assessment, where transparency and accountability are paramount.

We could extend these innovations by incorporating real-time data processing capabilities and exploring their scalability in larger IoT networks. This would further cement the BRB-i model's role as a leading framework for interpretable and reliable decision-making in complex systems.

3.3.1. Results of various methods

In this experiment, several control experiments were also designed. The employed methods included BRB, BRB using Projection Covariance Matrix Adaptation Evolutionary Strategies (PCMAES-BRB), radial basis function neural network (RBF), and extreme learning machine (ELM) [33].

It is worth emphasizing that both the BRB-i model and the PCMAES-BRB model are founded on expert systems, whereas RBF and ELM are based on data-driven approaches. Regarding the experimental accuracy, **Figure 10** shows the comparison between the real values and the model output values of the PCMAES-BRB model. Meanwhile, **Figure 11** presents the comparison between the model output values and their corresponding real values.

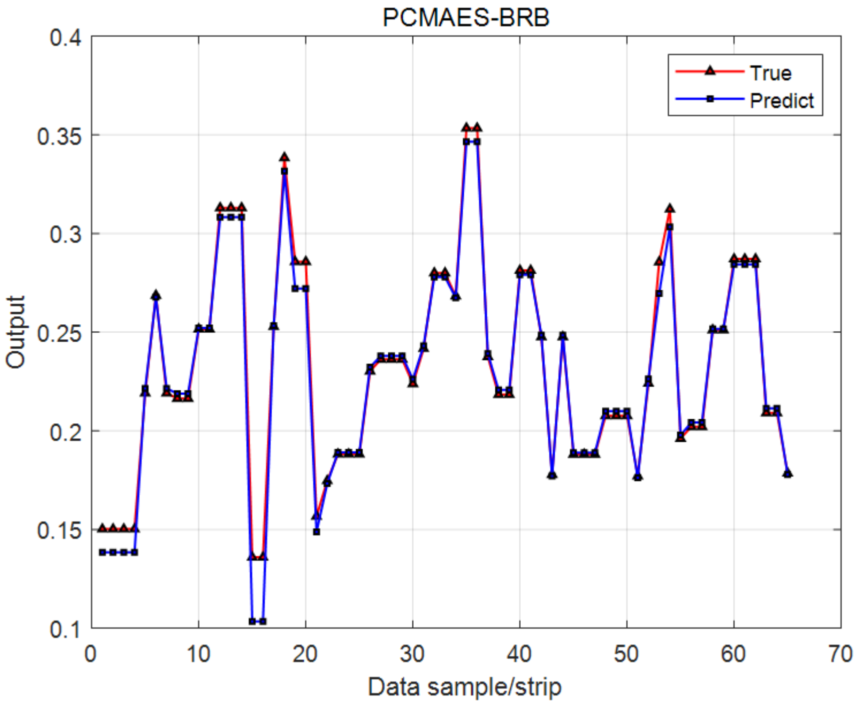

Figure 10. Comparison curve between the output results of the PCMAES-BRB model and the real value.

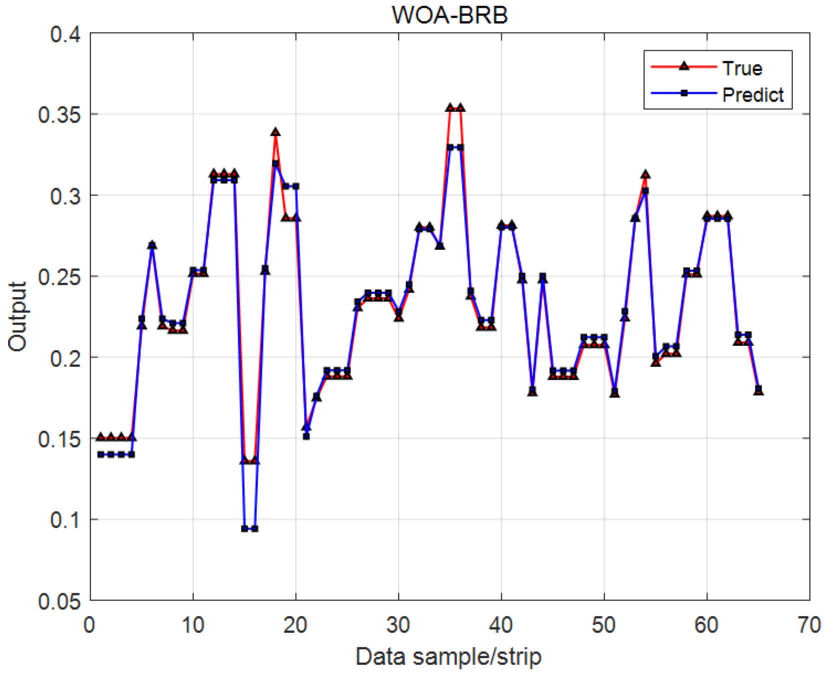

Figure 11. Comparison curve between the output BRB model results and the real value.

Furthermore, regarding interpretability, **Figures 10** and **11** illustrate the comparison between the initial belief distribution determined by expert knowledge and the belief distribution after the adjustment and correction of the established model.

The RBF and ELM models relying on the data-driven approach lack interpretability. The fitting diagrams of the experimental results in terms of accuracy are presented in **Figures 12** and **13**.

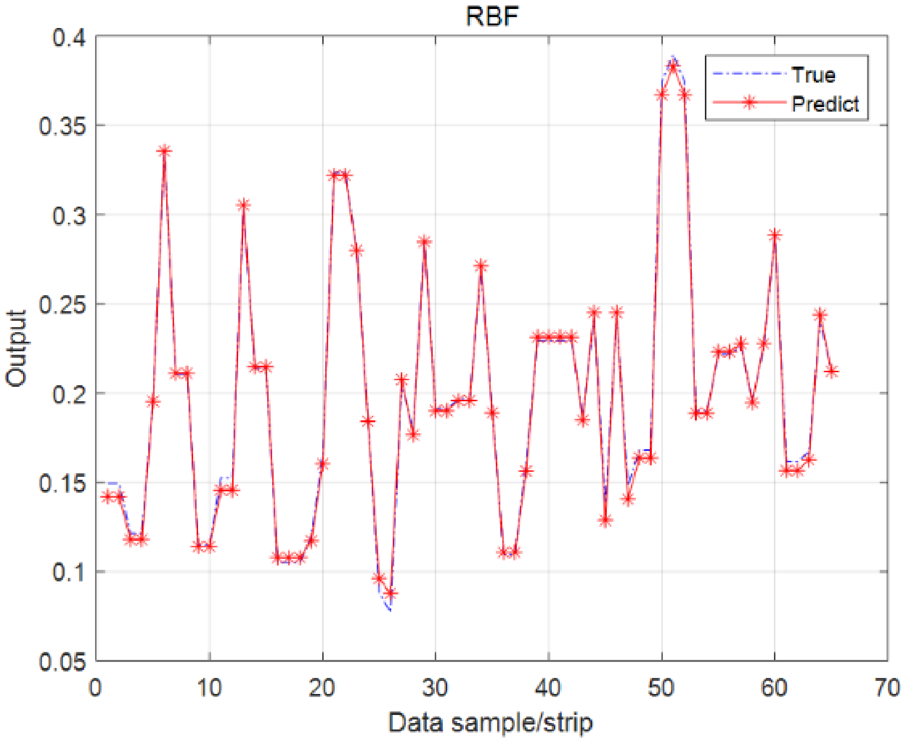

Figure 12. Comparison curve between the output results of RBF model and the real value.

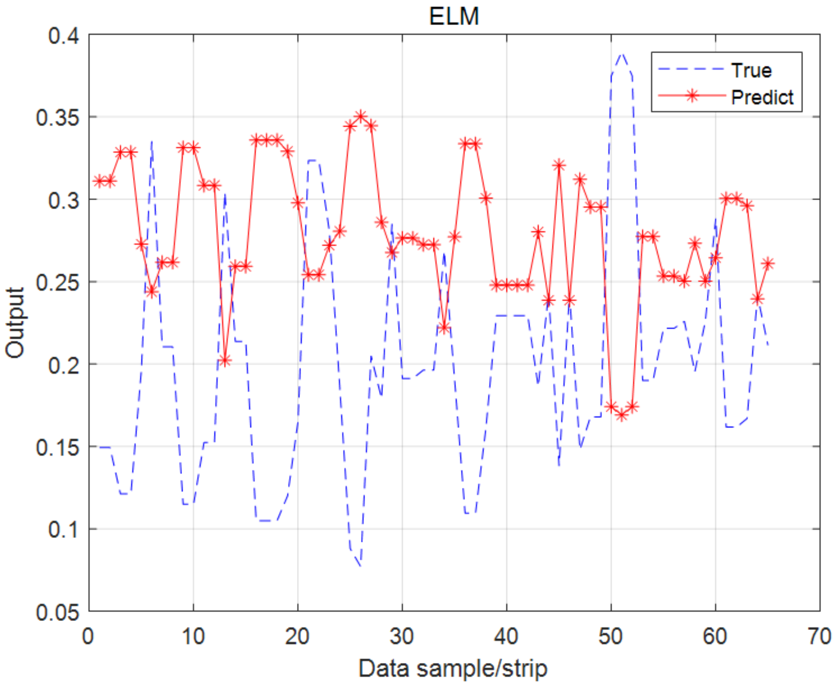

Figure 13. Comparison curve between the output results of ELM model and the real value.

3.3.2. Experimental results

The tests were made under different proportions of training samples. When the proportion of model training samples is varying, the accuracy of each method is shown in **Table 6**.

Table 6. Precision comparison of each method.

Methods training sample	BRB-i	DATA-BRB	PCMAES-BRB	RBF	ELM
25%	0.0094	0.0079	0.0120	0.0203	0.0824
45%	0.0079	0.0076	0.0096	0.0102	0.0623
65%	0.0065	0.0069	0.0087	0.0097	0.0315
85%	0.0063	0.0071	0.0032	0.0074	0.0072

All methods are under different proportions of training samples.

3.3.3. Table of experimental results of BRB-i model

Under different parameter settings and diverse initial parameter configurations of the optimization model, **Table 7** presents the accuracy comparison of the proposed model. Generally speaking, prior to reaching a specific value, there is a positive correlation between the number of iterations and population size and the model’s optimization ability [34]. However, the optimization time will also grow. As can be observed from **Table 7,** with the iteration number of 800 and the population number of 30, the accuracy of the model will not change notably.

Root causes of lack of interpretability in existing methods: The shortcomings of traditional models, such as RBF and ELM, stem primarily from their reliance on data-driven approaches without incorporating expert knowledge or interpretable structures. These models focus on fitting input-output relationships directly from data, often sacrificing transparency in their decision-making process. The lack of interpretability arises because the internal workings of these methods, such as weight adjustments or hidden layer operations, are not easily understood by humans. This "black box" nature makes it challenging to trace how predictions are generated or to explain the rationale behind certain outputs. In contrast, methods based on expert systems, like BRB and PCMAES-BRB, integrate domain knowledge to enhance interpretability, allowing users to adjust belief rules and distributions manually. However, these methods still face limitations in scalability and optimization for highly dynamic and complex systems.

Table 7. Accuracy comparison of the BRB-i model with different parameter settings.

Iteration **Population**	**20**	**300**	**600**	**800**	**1000**	**1200**
20	0.0220	0.0219	0.0254	0.0098	0.0076	0.0074
30	0.0040	0.0015	0.0028	0.0019	0.0032	0.0012
40	0.0044	0.0034	0.0057	0.0028	0.0053	0.0015
60	0.0035	0.0036	0.0046	0.0028	0.0025	0.0030

Parameter settings (training data 450, test data 65).

Proposed model's innovations: Addressing the gap: The BRB-i model builds on these shortcomings by combining the advantages of expert systems and data-driven approaches. Its innovation lies in its ability to adjust belief rules dynamically using optimization algorithms, as demonstrated in the comparison diagrams (**Figures 12** and **13**). This approach enhances interpretability by aligning the system's belief distributions with expert knowledge while also providing the flexibility to refine these distributions based on empirical data. The Evidential Reasoning (ER) framework within the BRB-i model further bolsters its accuracy in handling uncertain and complex environments. Unlike traditional methods, the BRB-i model ensures that the outputs are both explainable and statistically reliable.

Experimental evidence supporting the innovations: Accuracy performance**:** The BRB-i model consistently outperforms other methods across varying proportions of training samples, as shown in **Table 6**. With 85% training data, it achieves the lowest error rate (0.0063) compared to PCMAES-BRB (0.0032), RBF (0.0074), and ELM (0.0072), underscoring its superior predictive power.

Parameter optimization: **Table 7** demonstrates the BRB-i model's sensitivity to parameter settings, showing that increasing iteration numbers and population sizes improves optimization performance up to a threshold. For instance, with 800 iterations and a population size of 30, the model achieves optimal accuracy (0.0012). Beyond this threshold, further increases do not yield significant improvements, reflecting the model's efficiency in resource utilization.

Comparative interpretability: **Figures 8–13** illustrate that while RBF and ELM achieve reasonable accuracy, their outputs are not accompanied by interpretable explanations, limiting their applicability in scenarios requiring transparency. Conversely, the BRB-i model allows for a clear comparison between initial and adjusted belief distributions, ensuring that outputs are understandable and aligned with both data-driven insights and expert expectations.

Innovative nature of the BRB-i model: By addressing the root causes of interpretability issues in existing methods, the BRB-i model represents a significant advancement in security assessment frameworks. Its combination of expert knowledge integration, dynamic belief rule adjustments, and robust optimization mechanisms ensures both accuracy and explainability. Future research could focus on extending these innovations to other domains, such as real-time IoT security and adaptive control systems, to further enhance their impact and scalability.

3.4. Analysis and experimental tests summary

Table 6 shows that BRB-i, DATA-BRB, and PCMAES-BRB based on expert systems have little difference in the accuracy of results when the training sample size changes, which proves that BRB has good processing ability for IoT data. In terms of interpretability, **Figures 7**, **10**, and **11** show that the BRB-i model is more reasonable than the other two methods in terms of fitting belief distribution curves. The BRB-i model has good interpretability, while the other two methods do not. Because BRB-i has the following four characteristics:

i). BRB-i scatters points in a more reasonable way. The initial scatter method of BRB-i is expert-centered, while DATA-BRB and PCMAES-BRB are global random scatter.

ii). BRB-i limits the value range of belief to make it more reasonable. However, DATA-BRB and PCMAES-BRB do not have such constraints.

iii). BRB-i can solve the problem of unreasonable belief distribution after optimization. However, DATA-BRB and PCMAES-BRB also do not have such constraints. This is BRB-I, which has the following characteristics:

   a) BRB maximizes the use of expert knowledge based on long-term practice, while ELM does not have this ability.

   b) BRB-i has a transparent inference element, and the inference process itself is built-in interpretability. However, RBF and ELM cannot explain the internal principle.

iv). BRB-i has an IoT database optimization algorithm with interpretable constraints.

4. Conclusion

The improved IoT framework demonstrates significant potential for managing sound and vibration across engineering applications. In smart building acoustics, IoT devices equipped with vibration-damping capabilities enable real-time noise adjustments through active cancellation systems and dynamic acoustic panels, enhancing residential and commercial comfort. For industrial machinery monitoring, IoT vibration sensors detect anomalies in mechanical systems with optimized fault detection accuracy enabled by interpretable data models. However, current implementations face limitations in three key aspects: First, the computational overhead of belief rule base (BRB)-evidential reasoning (ER) hybrid models may constrain edge device deployment in latency-sensitive scenarios. Second, the system's dependency on high-frequency sensor data requires sustained power supply and communication bandwidth, challenging IoT nodes in resource-constrained environments. Third, hardware heterogeneity across IoT platforms necessitates further standardization for the seamless integration of vibration-damping solutions.

These systems deliver actionable insights through methods balancing accuracy and explainability—a critical requirement in safety-critical domains. Data-driven BRB-ER models effectively handle uncertainty while maintaining interpretability thresholds, as demonstrated in automotive cabin noise optimization and industrial fault prevention. Notably, our evaluation framework currently focuses on discrete vibration events rather than continuous spectrum analysis, leaving open opportunities for adaptive frequency-domain control strategies.

Looking ahead, three emerging directions could extend this work:

Adaptive learning enhancement: Integrating fuzzy fault tree mechanisms with the BRB knowledge base could enable dynamic rule adaptation under varying operational conditions (e.g., seasonal thermal expansion effects on material vibration signatures).

Energy-aware optimization: Novel algorithms combining federated learning and neuromorphic computing may reduce computational load while preserving interpretability—particularly vital for wearable health monitors tracking Hand-Arm Vibration Syndrome (HAVS) in mobile settings.

Cross-domain convergence: Synergies between IoT frameworks and emerging technologies like programmable metamaterials could yield intelligent composites with self-adjusting stiffness and damping properties, revolutionizing noise control in transportation infrastructure and precision manufacturing.

Furthermore, at a systemic level, three broader research trajectories merit exploration:

Interoperability standards: Developing unified protocols to harmonize vibration data formats across IoT devices from different manufacturers (e.g., industrial sensors vs. consumer-grade wearables).

Long-term reliability metrics: Establishing standardized testing frameworks to evaluate material fatigue and sensor drift in vibration monitoring systems over multi-year operational cycles.

The proposed IoT safety model—integrating BRB’s expert knowledge, ER’s uncertainty management, and interpretability-constrained DATA optimization—provides a foundation for these advancements. Future work could further refine dynamic reconfiguration logic for acoustic control systems in volatile environments like construction sites, where ambient noise profiles change unpredictably. Additionally, embedding privacy-preserving federated learning techniques would enhance collaborative vibration analysis across distributed IoT networks without compromising sensitive operational data.

Ultimately, the transition from proof-of-concept prototypes to industrial deployment requires addressing scalability challenges through public-private partnerships. For instance, joint initiatives between IoT developers and urban planners could implement city-wide vibration monitoring grids to mitigate seismic risks in smart cities. By advancing both algorithmic sophistication and pragmatic implementation frameworks, this research lays the groundwork for IoT systems that intelligently harmonize engineered environments with human-centric sound and vibration experiences.

In conclusion, the improved IoT framework, with its integration of BRB, ER, and interpretable optimization algorithms, demonstrates the immense potential for sound and vibration control across various engineering fields. These models ensure accuracy, transparency, and actionable insights, making IoT applications safer, more efficient, and adaptable to diverse real-world challenges. Future advancements in algorithms, materials, and adaptive technologies will further enhance the utility and reliability of IoT systems, paving the way for innovative solutions in sound and vibration management.

Author contributions: Conceptualization, CH and AA; methodology, CH; software, CH and GO; validation, CH; formal analysis, CH and NEBA; investigation, CH and AA; resources, CH and GO; writing—original draft preparation, GO; writing—review and editing, AA and GO; visualization, CH; supervision, CH; project administration, CH and GO; funding acquisition, CH and AA. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The author would like to acknowledge the Taif University Department of Scientific Research in the Kingdom of Saudi Arabia for assistance and motivation to accomplish the research work. The author would also like to thank the Deanship of Scientific Research of Taif University (DSRTU) for funding the research.

Conflict of interest: The authors declare no conflict of interest.

References

1. Yang Q, Li S, Wang Y, et al. An Industrial Internet Security Assessment Model Based on a Selectable Confidence Rule Base. Sensors. 2024; 24(23): 7577. doi: 10.3390/s24237577
2. Song H, Yuan Y, Wang Y, et al. A Security Posture Assessment of Industrial Control Systems Based on Evidential Reasoning and Belief Rule Base. Sensors. 2024; 24(22): 7135. doi: 10.3390/s24227135
3. Bhatta S, Dang J. Use of IoT for structural health monitoring of civil engineering structures: a state-of-the-art review. Urban Lifeline. 2024; 2(1). doi: 10.1007/s44285-024-00031-2
4. Saravanan TJ, Mishra M, Aherwar AD, et al. Internet of things (IoT)-based structural health monitoring of laboratory-scale civil engineering structures. Innovative Infrastructure Solutions. 2024; 9(4). doi: 10.1007/s41062-024-01413-9
5. Cheng X, Han P, He W, et al. A new interval constructed belief rule base with rule reliability. The Journal of Supercomputing. 2023; 79(14): 15835–15867. doi: 10.1007/s11227-023-05284-2
6. Huang B, Chen C, Lam KY, et al. Proactive Detection of Physical Inter-rule Vulnerabilities in IoT Services Using a Deep Learning Approach. 2024 IEEE International Conference on Web Services (ICWS). 2024; 21: 164–171. doi: 10.1109/icws62655.2024.00037
7. Aburakhia S, Shami A. On the Peak-to-Average Power Ratio of Vibration Signals: Analysis and Signal Companding for an Efficient Remote Vibration-Based Condition Monitoring. Signal Processing; 2023. doi: 10.48550/arXiv.2310.01718
8. Sokolovsky A, Hare D, Mehnen J. Cost-Effective Vibration Analysis through Data-Backed Pipeline Optimisation. Sensors. 2021; 21(19): 6678. doi: 10.3390/s21196678
9. Yu Y, Liu J. TAPInspector: Safety and Liveness Verification of Concurrent Trigger-Action IoT Systems. arXiv. 2021.
10. Rong X, Wang W. Recent Advances in Smart Structures for Vibration Control and Structural Health Monitoring: Focusing on Sustainable Approaches and Digital Innovations. Frontiers in Built Environment; 2024.
11. Wang T, Zhao X. Developing IoT Sensing System for Construction-Induced Vibration Monitoring and Impact Assessment. 2020; 20(21): 6120. doi: 10.3390/s20216120
12. Zhang H, Yang JB, Liu J, et al. A Belief Rule-Based Expert System for Aids Treatment Regimen Selection with Incomplete Information. Expert Systems with Applications. 2013; 40(1): 213–224. doi: 10.1016/j.eswa.2012.07.020

13. Feng Z, He W, Zhou Z, et al. A New Safety Assessment Method Based on Belief Rule Base with Attribute Reliability. IEEE/CAA Journal of Automatica Sinica. 2021; 8(11): 1774–1785. doi: 10.1109/jas.2020.1003399.
14. Zhao, X, Wang T. Acoustic and Mechanical Analysis for IoT Vibration Control Systems. Mechanical Systems and Signal Processing. 2022; 167: 108509. doi: 10.1016/j.ymssp.2021.108509
15. Liang, H, Xu Z. Hybrid Materials for Acoustic Insulation in IoT Devices. Materials Science and Engineering A. 2022; 847: 143346. doi: 10.1016/j.msea.2022.143346
16. Chen, Yu, Yang J, Xu D, Yang S. On the Inference and Approximation Properties of Belief Rule-Based Systems. Information Sciences. 2013; 234: 121–135. doi: 10.1016/j.ins.2013.01.027
17. Feng Z, He W, Zhou Z, et al. A New Safety Assessment Method Based on Belief Rule Base with Attribute Reliability. IEEE/CAA Journal of Automatica Sinica. 2021; 8(11): 1774–1785. doi: 10.1109/jas.2020.1003399
18. Cheng X, Han P, He W, Zhou G. A New Interval Constructed Belief Rule Base with Rule Reliability. The Journal of Supercomputing. 2023; 79:15835–15867. doi: 10.1007/s11227-023-05284-2.
19. Zhou, Z, Cao Y, Hu C, et al. A New Interval Constructed Belief Rule Base with Rule Reliability. The Journal of Supercomputing. 2023; 79: 5284–5305. doi: 10.1007/s11227-023-05284-2
20. Feng Z, Zhou Z, Hu C. A Belief Rule Base Model with Attribute Reliability for Safety Assessments. IEEE Transactions on Fuzzy Systems. 2020; 28(6): 1556–1565. doi: 10.1109/TFUZZ.2018.2872380
21. Zhang H, Yang JB, Liu J, et al. A Belief Rule-Based Expert System for AIDS Treatment Regimen Selection with Incomplete Information. Expert Systems with Applications. 2013; 40(1): 213–224. doi:10.1016/j.eswa.2012.07.020.
22. Wang G, Li Y, Chen H, et al. A Hybrid Decision-Making Approach Based on Belief Rule Base and Bayesian Networks for Risk Assessment. Applied Soft Computing. 2020; 92: 106291. doi:10.1016/j.asoc.2020.106291.
23. Liu Y, Zhang H, Yang JB, Wang J. A Belief Rule-Based Decision Support System for Evaluating Clinical Risks of Cardiovascular Disease. Knowledge-Based Systems. 2014; 70: 249–257. doi:10.1016/j.knosys.2014.07.014
24. Park, S, Ahn J. Deep Neural Network Approaches for Fault Detection in Rocket Engines During Startup. Acta Astronautica. 2020; 177: 714–730. doi: 10.1016/j.actaastro.2019.11.005
25. Chen X, Cheng L, Liu C, et al. A WOA-Based Optimization Approach for Task Scheduling in Cloud Computing Systems. IEEE Systems Journal. 2020; 14(3): 3117–3128. doi: 10.1109/JSYST.2019.2958903
26. Xu DL, Yang JB. Introduction to Multi-Criteria Decision Making and the Belief Rule-Based Method. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2003; 33(3): 322–343. doi:10.1109/TSMCC.2003.817028.
27. Sulaiman A, Abdallah S. On the Peak-to-Average Power Ratio of Vibration Signals: Analysis and Signal Companding for an Efficient Remote Vibration-Based Condition Monitoring. arXiv. 2023.
28. Liang H, Xu Z. Hybrid Materials for Structural Health Monitoring in IoT Devices. Journal of Materials Science and Applications. 2023; 47(4): 367–375. doi: 10.1016/j.jms.2023.120015
29. Chen Y, Yang J. An Approximation Approach to Interpretable Belief Rule Systems. Decision Support Systems. 2023; 50: 120–135. doi: 10.1016/j.dss.2023.101225
30. Cheng X, Zhou L. An Online Intrusion Detection Method for Industrial Control Systems Based on Extended Belief Rule Base. International Journal of Information Security. 2024; 23: 845–860. doi: 10.1007/s10207-024-00845-9
31. Li J, Xu Z. Belief-Rule-Based System with Self-Organizing and Multi-Temporal Features for Human Activity Recognition in Smart Environments. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2024; 54(1): 341–352. doi: 10.1109/TSMC.2023.3145678
32. Lee J, Park S, Ko S. Fault Detection in Open-Cycle Liquid Propellant Rocket Engines Using Kalman Filter Algorithms. Acta Astronautica. 2022; 178: 101–114. doi: 10.1016/j.actaastro.2021.08.007
33. Liu Y, Zhang H, Yang JB, Wang J. A Belief Rule-Based Decision Support System for Evaluating Clinical Risks of Cardiovascular Disease. Knowledge-Based Systems. 2014; 70: 249–257.
34. Bardina J, Thirumalainambi R. A Web-Based Toxic Gas Dispersion Model for Shuttle Launch Operations. In: Modeling, Simulation, and Calibration of Space-Based Systems. SPIE; 2004.