#### Heliyon 10 (2024) e30185

Contents lists available at ScienceDirect

# Heliyon



journal homepage: www.cell.com/heliyon

# Research article

5<sup>2</sup>CelPress

# Algorithm for community security risk assessment and influencing factors analysis by back propagation neural network

Shuang Zhou<sup>a,\*</sup>, Meiling Du<sup>a</sup>, XiaoYu Liu<sup>b</sup>, Hongyan Shen<sup>a</sup>

<sup>a</sup> School of Public Administration, Tianjin University of Commerce, Tianjin, 300134, China

<sup>b</sup> School of International Business, University of International Business and Economics, Beijing, 100029, China

#### ARTICLE INFO

Keywords: Back propagation neural network Community security risk Nodes in the hidden layer Model fitting degree Risk assessment

#### ABSTRACT

This paper aims to accurately assess and effectively manage various security risks in the community and overcome the challenges faced by traditional models in handling large amounts of features and high-dimensional data. Hence, this paper utilizes the back propagation neural network (BPNN) to optimize the security risk assessment model. A key challenge of researching community security risk assessment lies in accurately identifying and predicting a range of potential security threats. These threats may encompass natural disasters, public health crises, accidents, and social security issues. The intricate interplay of these risk factors, combined with the dynamic nature of community environments, presents difficulties for traditional risk assessment methodologies to address effectively. Initially, this paper delves into the factors influencing safety incidents within communities and establishes a comprehensive system of safety risk assessment indicators. Leveraging the adaptable and generalizable nature of the BPNN model, the paper proceeds to optimize the BPNN model, enhancing the security risk assessment model through this optimization. Subsequent comparison experiments with traditional models validate the rationality and effectiveness of the proposed model, with hidden layer nodes set at various levels like 10, 15, 20, 25, 30, and 35. These traditional models include Convolutional Neural Network (CNN), Long Short-Term Memory Network (LSTM), Bidirectional Encoder Representations from Transformers (BERT), Generative Pre-trained Transformer (GPT), and eXtreme Gradient Boosting (XGBOOST). Experimental findings demonstrate that with 20 hidden layer nodes, the optimized model achieves a remarkable final recognition accuracy of 99.1 %. Moreover, the optimized model exhibits significantly lower final function loss compared to models with different node numbers. Increasing the number of hidden layer nodes may diminish the optimized model's fit and accuracy. Comparison with traditional models reveals that the average accuracy of the optimized model in community risk identification reaches 98.5 %, with a maximum accuracy of 99.6 %. This marks an improvement of 9%-11 % in recognition accuracy across various risk factors compared to traditional models. Regarding system response time and resource utilization, the optimized model exhibits a response time ranging from 100 ms to 120 ms and consistently lower resource utilization rates across all scenarios, underscoring its efficiency in community security risk assessment. In conclusion, this experiment sheds light on the underlying mechanisms and patterns of community safety risk formation, offering novel perspectives and methodologies for researching community safety risk assessment. The paper concludes by presenting recommendations and strategies for addressing community safety risks based on experimental analysis.

\* Corresponding author.

E-mail address: zhoushuang\_8706@163.com (S. Zhou).

https://doi.org/10.1016/j.heliyon.2024.e30185

Received 27 February 2024; Received in revised form 19 April 2024; Accepted 22 April 2024

Available online 24 April 2024

<sup>2405-8440/© 2024</sup> Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

#### 1. Introduction

Community safety risk assessment is a vital field of study that focuses on analyzing and predicting potential security threats faced by communities. These threats can range from criminal activities to accidents and natural disasters, all of which jeopardize community stability and residents' quality of life [1]. With the rapid pace of societal development and urbanization, these safety risks are becoming more prominent, posing significant challenges to both community development and residents' well-being. Hence, accurately assessing a community's safety risk level and analyzing the factors influencing it are crucial for devising effective security measures and emergency plans. When identifying risk factors, it is essential to consider various parameters or variables. These include community crime rates, traffic accident occurrence rates, fire incidence rates, the likelihood of natural disasters, resident population density, regional economic conditions, level of infrastructure development, and community emergency response capabilities. The selection of these variables aims to provide a comprehensive reflection of the multidimensional nature of community safety risks. Traditional methods of community safety risk assessment typically involve qualitative analysis, quantitative analysis (such as fault tree analysis, and event tree analysis), and hybrid approaches. These methods encounter the following challenges when dealing with high-dimensional data and dynamic community environments. First, when dealing with large and complex data sets, traditional methods often struggle to effectively process them. This is because they were not designed to account for the characteristics of high-dimensional data, such as complex interactions between features, which can result in ineffective risk identification and evaluation [2-4]. Next, community environments are constantly changing, with new risk factors potentially emerging at any time. Traditional methods often lack the ability for real-time updates and learning, making it difficult to adapt to such dynamic changes, which may result in reduced accuracy and timeliness of risk assessment. Finally, many traditional risk assessment methods focus more on identifying and evaluating existing risks rather than predicting future risks. This limits their effectiveness in preventing potential security threats. Henceforth, this paper introduces a groundbreaking algorithm for community safety risk assessment and influencing factor analysis, rooted in the Back Propagation Neural Network (BPNN). The aim is to revolutionize the accuracy and dependability of assessments through cutting-edge computing technology and algorithms, offering a more scientific and comprehensive decision-making framework for community safety management. The existing constraints of the current community security risk assessment system often stem from limitations in data availability, integrity, and accuracy, particularly prevalent in communities with scarce resources or inadequate information sharing. Furthermore, the ever-evolving community environment and the dynamic nature of security risks demand a level of flexibility and adaptability that the current evaluation system may lack, thereby impeding real-time accuracy in assessment results.

Renowned for its prowess in pattern recognition, prediction, and classification, BPNN stands as a formidable machine learning (ML) algorithm. Its adaptive learning capability, adeptness in nonlinear mapping, and robustness render BPNN exceptional in tackling intricate relationships and nonlinear quandaries [5–7]. The reason for choosing BPNN over other ML models to optimize the security risk assessment model lies primarily in several prominent advantages of BPNN. First, the multi-layer structure of BPNN allows them to capture and model complex nonlinear relationships, which is particularly important for the multiple variables and high-dimensional data involved in security risk assessment. This is because these data often contain complex and nonlinear influencing factors. Next, BPNN can learn universal patterns from training data and effectively apply them to new, unseen data. This means that once the BPNN is well-trained on community security risk assessment data, it can accurately predict unknown or future security risks. Lastly, BPNN can adjust network structures (such as the number of layers and nodes per layer) and automatically adjust weights during the training process to best reflect the complex relationships in the data according to specific requirements. This enables BPNN to maintain excellent performance in different scenarios and conditions. BPNN has demonstrated its strong potential applications in various fields, including but not limited to financial risk assessment, medical diagnosis, image recognition, and language processing. For example, in the financial domain, BPNN is used for credit scoring and fraud detection. In the medical field, it aids in disease prediction and medical image analysis. In computer vision, BPNN supports the recognition and classification tasks of complex images [8]. The remarkable nonlinear mapping prowess of BPNN empowers it to discern and model intricate nonlinear relationships, thus augmenting the precision of evaluation. The significance of this paper lies in the recognition that, amid the rapid evolution of society, community security risks are burgeoning in complexity, rendering traditional assessment methods inadequate to meet contemporary demands. By harnessing BPNN to refine community security risk assessment, potential risks can be identified and forecasted with heightened accuracy. Moreover, the community's capacity to confront diverse security threats can also be significantly bolstered, furnishing robust support for safeguarding community security and residents' well-being. Despite BPNN's widespread utilization in realms such as pattern recognition, prediction, and classification, and its proven efficacy in grappling with intricate relationships and nonlinear challenges, it still grapples with certain constraints when applied to community security risk assessment. On the one hand, BPNN's performance is intricately tethered to the caliber and abundance of training data. In community safety risk assessment, securing high-quality and meticulously labeled data may pose challenges, potentially limiting the efficacy and accuracy of model learning. On the other hand, owing to its complex network architecture, BPNN may occasionally hyper-learn the minutiae and noise within training data, diminishing the model's generalization prowess on novel data. This issue is particularly salient in dynamic community security risk assessment scenarios and warrants mitigation through apt regularization techniques and parameter adjustments.

This paper also faces several challenges in employing BPNN to optimize the security risk assessment model. On one hand, designing a BPNN model that can handle high-dimensional data while adapting to dynamic changes is a formidable task. Careful consideration must be given to network architecture, selection of appropriate activation functions, and adjustment of learning rates to achieve optimal risk assessment performance. On the other hand, high-dimensional data may contain a plethora of noise and irrelevant features, necessitating effective data preprocessing and feature selection before model training to ensure that the model learns the most valuable information. This paper embarks on a transformative journey by first delving into an in-depth analysis of previous research, shedding light on the limitations of traditional methodologies. Subsequently, it ventures into the intricate realm of factors influencing community safety events, constructing a robust framework for community safety risk assessment, inclusive of diverse indicators. The culmination of these endeavors materializes in the development of a novel security risk assessment model, integrating the optimized BPNN, whose rationality and efficacy are rigorously scrutinized through empirical experimentation. In conjunction with the research findings, the experiments posit certain assumptions. Primarily, it is postulated that the risk assessment indicators delineated comprehensively encapsulate the primary determinants of community safety, spanning natural disasters, public health crises, accidents, and social security issues. Moreover, it is conjectured that the BPNN model stands as an apt candidate for community safety risk assessment, adept at processing and analyzing relevant data to discern risk patterns and furnish precise risk predictions. The salient contributions of this paper are threefold. First, it harnesses the nonlinear modeling prowess of BPNN to adeptly capture and portray the intricate relationships inherent in community safety risk. The algorithm dynamically adjusts weights and biases during modeling, enhancing model accuracy and generalization. Next, it attains the capacity to discern and quantify a myriad of potential influencing factors through systematic collection and processing of pertinent data. The BPNN model systematically incorporates these factors, scrutinizing their impact levels on community safety risk. Lastly, the paper undertakes extensive experimentation and performance evaluation of the proposed algorithm, leveraging authentic community datasets, and effectively showcasing the advantages of BPNN in community safety risk assessment. In essence, this paper endeavors to pioneer the development of a BPNN-based community safety risk assessment algorithm, concurrently undertaking a comprehensive analysis of factors influencing community safety. The delineated contributions underscore the significance of this endeavor within the academic discourse. The intended audience for this paper comprises two distinct groups: community managers and policymakers, entrusted with formulating and implementing community safety management measures, necessitating accurate safety risk assessments to guide decision-making. The research findings empower them to comprehend the security risks confronting the community and formulate more effective security strategies and emergency plans. The other group encompasses academic researchers and scholars. Researchers operating in security risk assessment, artificial intelligence, ML, and allied fields may find that the methods and findings of this paper enrich their research endeavors or serve as the foundation for subsequent investigations. The primary avenue for disseminating and exchanging research findings among recipients is through academic publications. Research papers will be disseminated in academic journals and conferences in related fields, facilitating the sharing of research outcomes and garnering feedback and suggestions from peers.

#### 2. Literature review

In the arena of community safety risk assessment research, Ezugwu et al. (2022) introduced a pioneering natural heuristic metaheuristic algorithm known as the Prairie Dog Optimization Algorithm. This innovative approach emulated the behavioral strategies of prairie dogs in their natural habitats to fulfill optimization tasks. Abstracted into two optimization stages, namely exploration and development, this behavior strategy effectively navigated the solution space to identify the optimal solution. By incorporating the natural behavior strategy into the Prairie Dog Optimization Algorithm, the performance of the community safety risk assessment model was enhanced, enabling it to manage complex community safety data more effectively and provide precise and reliable decision support for community safety management [9]. In contrast, Formica (2022) fused hazard factors with the vulnerability of exposed elements, elucidating their intricate interplay in risk assessment contexts. Employing sequential analysis, weight coefficients were computed for each hazard factor and the vulnerability of exposed elements. Furthermore, a method was devised for calculating weight coefficients in the absence of certain data. This approach culminated in the determination of a comprehensive risk value for the community [10]. Acknowledging the heightened population density in communities, Adomah et al. (2022) advocated for a multifaceted approach to disaster risk assessment. This approach integrated hazard factors, the vulnerability of exposed elements, and residents' protective capacity. The assessment embraced the fusion of multiple data sources, leveraging linear fusion and fuzzy entropy weighting methods. Utilizing the fuzzy comprehensive evaluation method, a set of evaluative comments was established, and a single-factor evaluation fuzzy matrix was constructed. The entropy weighting method was then employed to ascertain the weight of factors to be assessed, resulting in a comprehensive evaluation [11]. Conversely, Agushaka et al. (2022) proposed the Mongoose Optimization Algorithm, a novel meta-heuristic algorithm aimed at solving classical and CEC 2020 benchmark functions and 12 continuous/discrete engineering optimization problems. The algorithm adapted compensatory behavior, considering prey size, space utilization rate, population size, and food supply. The application of the Mongoose Optimization Algorithm could simulate complex traffic flow and determine optimal paths by mimicking the hunting and social behavior of mongooses [12].

Agushaka et al. (2023) introduced the Gazelle Optimization Algorithm, a novel population-based meta-heuristic algorithm inspired by the resilience of gazelles in predator-dominated environments. This breakthrough held profound significance in the development of intelligent transportation systems capable of real-time responsiveness to dynamic changes in traffic conditions [13]. Meanwhile, Sheng and Gengxin (2022) delved into the realms of artificial intelligence, employing the Recurrent Neural Network (RNN) and the Convolutional Neural Network (CNN). However, it is worth noting that while these models were designed for network security monitoring and defense, their application in community safety risk assessment and impact factor analysis remains relatively unexplored [14]. On a different front, Wang et al. (2023) pioneered the optimization of network systems through blockchain technology. They constructed a robust risk management system via smart contracts and leveraged risk correlation tree technology to track public sentiment through smart ledgers. The outcomes of their experiments underscored the efficacy of these innovative approaches in conducting risk prediction and credibility detection [15]. Meanwhile, Zhang et al. (2022) found that utilizing deep learning methods to analyze community safety data could effectively enhance the accuracy and timeliness of disaster prediction, especially in complex and dynamically changing urban environments [16]. Wu et al. (2023) discovered that by integrating geographic information systems and ML technology, security risks could be pinpointed more accurately, and emergency response plans were optimized. It was particularly crucial in managing natural disasters such as floods and earthquakes [17]. Li et al. (2023) revealed that community residents' involvement was vital for improving the effectiveness of community safety risk assessment models. Data collection through community participation significantly enhanced the model's ability to predict locally specific risks [18].

Table 1 illustrates the details.

Traditional methods of community safety risk assessment often fail to adequately account for the intricate relationships and nonlinear dynamics among various factors, leading to limited accuracy in assessment outcomes. Moreover, these conventional models may struggle to offer precise and generalized insights across diverse community settings. In contrast, this paper presents a pioneering approach by integrating BPNN into the realm of community safety risk assessment, leveraging its robust data processing capabilities and nonlinear modeling advantages to significantly enhance the accuracy and reliability of risk assessment outcomes. By systematically incorporating multidimensional factors such as community safety risk assessment index system. This not only amplifies the breadth of assessment coverage but also enhances the scientific rigor and practical applicability of the assessment findings.

#### 3. Establishment of community safety risk assessment indicator system

# 3.1. Analysis of influencing factors of community safety accidents

A community is a geographic and activity-centered human settlement comprising residents with specific associations within a defined geographical area. In the context of this country, risk is typically defined as the impact of uncertainty on targets, encompassing both process uncertainty and the uncertainty of events that influence the degree of impact on the target [19]. Community safety risk primarily refers to the consequences of uncertainty on the community, with a predominant focus on adverse impacts, exploring the likelihood and consequences under specific hazardous conditions. In this context, safety considerations are paramount, and identical consequences can yield varied outcomes for different communities. The determination of community safety risk largely revolves around identifying risks that pose a threat to the community itself [20].

The origins of risk events, known as risk sources, are fundamental components of prevailing evaluation models in community safety risk assessment [21]. These sources encompass factors directly contributing to the loss of life or property, capable of inflicting damage on community structures and their surroundings. This encompasses considerations such as the duration, intensity, and type of disasters. The diverse nature of disasters necessitates distinct approaches to mitigation, with variations in intensity and duration leading to differing impacts on community safety [22]. Understanding the characteristics of disasters is pivotal in grasping community risk. A thorough understanding of these characteristics facilitates the implementation of targeted measures to mitigate risk sources. Consequently, the primary thrust of community risk management efforts lies in identifying these risk sources [23]. The criteria for selecting risk sources in this paper adhere to principles encompassing scientific rigor, comprehensiveness, operational feasibility, rationality, and a synthesis of quantitative and qualitative logic. Fig. 1 displays the details.

Over the past half-decade, a comprehensive compilation of community safety incidents occurring within the domestic sphere has been meticulously curated. This compilation process involved harnessing platforms like the Safety Management Network and the China Occupational Safety and Health website, with a rigorous analysis conducted on data sourced from statistical yearbooks. Table 2 meticulously outlines the paramount community safety incidents identified during this specific timeframe.

The cumulative total of the percentages attributed to the five identified event categories surpasses 50 %, underscoring their substantial impact. Notably, high-altitude falls have consistently emerged as the predominant factor influencing both community

Table 1		
Summary of literature review.		

Author	Year	Main content
Sheng and Gengxin	2022	Using RNN and CNN, it is mainly designed for network security monitoring and defense. The security of communication and data transmission within the community can be monitored and protected through RNN.
Ezugwu A E, Agushaka J O, Abualigah L, Abualigah L, Mirjalili S, & Gandomi A H.	2022	A meta-heuristic method inspired by nature is proposed to optimize parameter selection and feature weight adjustment in risk assessment model.
Formica S.	2022	The method of sequence analysis and weight calculation can help to accurately evaluate the risk level even if the data is missing.
Adomah E, Khoda Bakhshi A, Ahmed M M.	2022	A multi-faceted disaster risk assessment method is advocated, which combines risk factors, vulnerability of exposed elements and protection ability of residents, and adopts linear fusion and fuzzy entropy weight method.
Agushaka J O, Ezugwu A E, Abualigah L.	2022	The foraging behavior inspiration of the Mongoose optimization algorithm can be used to optimize the algorithm search strategy in community security risk assessment, especially in the face of complex and changeable security risk factors, to improve the search efficiency and the quality of the solution.
Wang Z, Zhang S, Zhao Y, Chen C, & Dong X.	2023	Blockchain technology is used to optimize the network system, the risk management system is built through the smart contract, and the risk correlation tree technology is used to track the public opinion in the smart account book.
Agushaka J O, Ezugwu A E, Abualigah L.	2023	The adaptability and flexibility of the gazelle optimization algorithm may bring additional advantages when dealing with a dynamic environment and high uncertainty risk assessment.



Fig. 1. Statistical analysis of the top five community safety accidents.

safety and building safety in recent years [24–26]. These incidents have presented significant threats to the overall safety of communities. Concurrently, the escalating ubiquity and extensive utilization of electric vehicles in recent years have given rise to a notable surge in fire incidents attributed to electric vehicle charging. This phenomenon has led to a heightened incidence and proportion of fire-related occurrences.

#### 3.2. Building a Community Safety Risk Indicator System

The term "risk sources" in this paper refers to a comprehensive classification encompassing events that can have adverse consequences on the environment crucial to the survival of urban communities and their residents. This classification mainly includes two basic aspects: natural causes and human causes. Natural disasters are the traditional description of disasters stemming from natural factors. In addition, human causes involve disasters caused by human factors, including but not limited to traffic accidents and infectious diseases. The division of risk sources involves four different types of classifications: natural disasters, public health, accidents and disasters, and social security. In the process of establishing a comprehensive system of community safety risk assessment indicators, this paper adopts a hierarchical classification mechanism based on expert knowledge and statistical analysis results. Specifically, through expert interviews and analysis of community safety accident data nationwide, a method combining qualitative and quantitative approaches is used to summarize and classify risk indicators. This approach aims to ensure that the selected indicators are both scientifically based and accurately reflect reality, thereby enhancing the accuracy and practicality of community safety risk assessment. Compared with the study by Richards and Richards (2022), it focuses on supervised classification techniques in remote sensing digital image analysis. Although supervised classification is highly effective in image processing and interpretation, this paper focuses on community safety risk assessment, which involves significantly different types of data and application scenarios from remote sensing image analysis. Community safety risk assessment requires comprehensive consideration of various types of risks and factors, rather than a single classification of image data [27]. Mavrogiorgou et al. (2017) compared the clustering and classification capabilities in data mining. Although data mining techniques have their advantages in identifying patterns and relationships, this paper focuses on building a comprehensive risk assessment system based on expert knowledge and statistical data analysis. Clustering and classification techniques are mainly used in data-driven scenarios. The method in this paper combines data analysis and expert

Table 2						
Statistics	of the	top t	five	security	incident	s.

Number	Proportion in total (%)
90	24.7
50	13.7
37	10.2
31	8.5
30	8.2
	Number 90 50 37 31 30

experience, aiming to construct a more comprehensive and customized risk assessment framework [28]. Meanwhile, Choi and Lim (2020) explored ML techniques for target advertisement classification. Although the findings provided ML solutions for a specific type of data classification, it mainly focused on applications in the advertising field. Compared to the community safety risk assessment in this paper, the two studies had significant differences in application background, objectives, and data types. Community safety risk assessment requires comprehensive consideration of various risk sources, rather than just a single classification task [29]. Accordingly, this paper proposes specific indicators for risk sources as illustrated in Table 3.

# 4. Optimization of the community safety risk assessment algorithm based on the BPNN

# 4.1. Principles of information propagation and training in the BPNN

During the forward propagation of the BPNN, each neuron receives input signals from other neurons, which are then multiplied by their corresponding weights and summed to yield the total input value for the neuron. Following this, the neuron evaluates whether this value exceeds its threshold. If it does, the neuron applies the activation function to produce the output value. The Sigmoid function, depicted by Eq. (1), is the most frequently utilized activation function:

$$Sigmoid(x) = \frac{1}{1 + e^{-x}} \tag{1}$$

In Eq. (2), the function Sigmoid(x) denotes the activation function, x represents the input data, and e represents the natural constant. In the context of backpropagation within BPNN, the core idea revolves around adjusting weights and propagating errors between the output and the desired output from the output layer back to the input layer through the hidden layers in a reverse manner. This process comprises three key steps: error backpropagation, gradient computation, and weight updating. Backpropagation initiates at the output layer once forward propagation, where the difference between the predicted output and the actual value is computed. At this stage, the discrepancy between the actual and expected outputs is evaluated using a loss function, defining the error. This error is then retroactively transmitted through each layer of the network, cascading back to the input layer. During this error backpropagation, the influence of each weight on the loss is assessed using the chain rule, facilitating the calculation of the derivative of a composite function. These gradients signify the partial derivatives of the loss function concerning each weight, revealing how variations in weights impact overall loss. For each weight in the network, its corresponding gradient is computed, guiding the magnitude and direction of weight adjustments required to minimize overall loss. Optimization algorithms like gradient descent are then deployed to update network weights iteratively. Gradient descent, an iterative procedure, refines weights in the opposite direction of their gradients during each iteration. In this update process, the learning rate governs the magnitude of weight adjustments. An excessively large learning rate may lead to over-adjustment and oscillation, whereas a too-small rate may impede learning progress. Backpropagation serves as an efficient algorithm empowering deep neural networks to optimize weights through iterative learning, enhancing predictive accuracy in intricate tasks. Through this mechanism, neural networks learn from errors, perpetually adapting parameters to fulfill given objectives.

From the perspective of neurons within the hidden layer, data traverses from the input layer to the hidden layer. After computing weight parameters, these parameters propagate back to the input layer, while each neuron maintains a threshold. Initially, parameters are randomly set, and the BPNN algorithm iteratively adjusts these initial randomizations towards desired values, thereby completing

Risk factor	Risk source
Natural calamities	Rainstorm
	Strong wind
	Thick fog
	Catkin
	Ground Subsidence
Accident disaster	Traffic accident
	Production safety accidents
	Fire accident
	Gas accident
	Drowning accident
	Electric shock accident
	Public facilities and equipment accidents
	Falling accidents
Public health	Infectious disease events
	Animal invasion
	Food poisoning
	Group unknown diseases
Social security	High-altitude parabolic motion
	Robbery incidents
	Terrorist incidents
	Mass incident

#### S. Zhou et al.

# neural network training [30].

In BPNN, the number of nodes in the input layer corresponds to the count of independent variables directly influencing prediction outcomes. Conversely, the number of nodes in the output layer indicates the quantity of dependent variables serving as the output results [31–35].

# 4.2. Optimization of the community safety risk assessment model based on BPNN

Enhancing the BPNN model for optimizing the process in community safety risk assessment involves the following steps:

Key Indicator Selection: Four main indicators are carefully selected from the index system of community safety risk assessment as input variables for the BPNN model. These indicators include natural disasters, public health, accident disasters, and social security. This step ensures that the model inputs are directly relevant to the core content of community safety risk assessment, thereby enhancing the model's specificity and accuracy.

Data Preprocessing: The selected four key indicators undergo data preprocessing, including normalization and outlier removal, to reduce noise during model training and improve the model's responsiveness to critical risk factors.

Model Structure Adjustment: The structure of the BPNN model is adjusted based on the characteristics of the selected indicators, including the number of hidden layers and nodes in each layer. This step aims to find the most suitable network architecture for community safety risk assessment tasks, enhancing the model's learning efficiency and predictive capability.

Training Parameter Optimization: The model's training process is optimized by adjusting parameters such as learning rate, weight initialization, and regularization parameters. Optimizing these parameters helps accelerate model convergence, reduce the risk of overfitting, and improve the model's generalization ability to unseen data.

Cross-Validation: Cross-validation methods are employed to evaluate the model's performance and stability. This step involves training and testing the model on different data subsets to ensure the accuracy and consistency of model predictions and assess the reliability of the model in real-world applications.

Fig. 2 presents the data architecture diagram of the optimized BPNN community security risk assessment model. The process of the model running is as follows.

- 1) Input Data: The model receives input data through Placeholder, which typically consists of feature data used for model training and prediction.
- 2) Forward Propagation:

Dense 1: The input data are first passed through a Dense layer, where each input node is connected to all nodes in the subsequent layer.



#### Fig. 2. Optimized BPNN architecture diagram.

(Const: Defines constant values or parameters; Mean: Average value of parameters; Train: The process of learning and optimizing weights and biases; Softmax Cross: Loss function; Placeholder: Dynamically receives input data during runtime; Dimension: Shape of data or size of arrays; Cast: Data type conversion; Equal: Used for comparing whether two values or arrays are equal; Argmax: Selects the category with the highest probability from the output layer's probability distribution; Gradients: Indicates how to adjust parameters to minimize the loss function; RMSprop: Root Mean Square Propagation; Save: Saves the state of the model; Variable: Parameters that can change during the training process; Dense: Layer where each neuron is connected to all neurons in the preceding layer.)

#### S. Zhou et al.

Dense 2: The data then flows to another Dense layer for further feature processing.

#### 3) Loss Calculation:

Softmax Cross: The Softmax cross-entropy function is applied to calculate the difference between the model output and the actual labels, resulting in a loss value.

#### 4) Backward Propagation:

Gradients: The gradients of the loss function with respect to the model parameters are computed, indicating how the parameters should be adjusted to minimize the loss.

RMSprop: The Root Mean Square Propagation optimizer is utilized to update the model parameters based on the gradients.

5) Parameter Update:

Variable: Model parameters (such as weights and biases) that can be changed during the training process are stored. Save: The model's state can be saved at specific time points during the training process.

#### 6) Performance Evaluation:

Argmax: The class with the highest probability from the output layer's probability distribution is selected as the predicted result. Equal: The predicted result is compared with the true labels to assess the model's accuracy.

Cast: Data type conversion may be necessary for comparison.

Dimension: Adjustments to the shape of data or array size may be required for comparison.

Mean: The average accuracy is computed, often used as an indicator for model performance.

# 7) Optimization and Feedback:

Train: It indicates that the model is in the training phase, which includes the aforementioned loss calculation and backward propagation.

Const: The defined constant values or parameters may be used during training to set parameters such as learning rate and regularization terms.

While four key indicators have been chosen as input variables for the model, it is crucial not to misconstrue this as disregarding the significance of other indicators. Community safety risk is a nuanced and multifaceted issue, influenced by numerous additional factors. Therefore, in practical contexts, a comprehensive examination of multiple indicators and factors is indispensable for a thorough assessment of community safety risks and the subsequent implementation of appropriate measures to bolster community safety. This paper presents two hypotheses. First, it posits that the risk assessment indicators outlined herein can comprehensively encompass the primary factors impacting community safety, encompassing natural disasters, public health, accidents, and social security. Next, it proposes that the BPNN model is well-suited for community safety risk assessment. This model is believed to adeptly process and analyze pertinent data, discern risk patterns effectively, and furnish precise risk predictions.

# 4.3. Experimental design

In order to validate the rationale behind the algorithm proposed, experiments are conducted utilizing the Emergency Events Database (EM-DAT), a comprehensive global repository of disaster events maintained by the Catholic University of Louvain in Belgium. EM-DAT meticulously records thousands of disaster occurrences, with continuous updates to accommodate new data each year. These events are categorized into primary types, comprising natural disasters and man-made disasters. Natural disasters are further delineated into meteorological disasters (such as hurricanes and floods), geological disasters (such as earthquakes and volcanic eruptions), and biological disasters (including droughts and disease outbreaks). Meanwhile, man-made disasters encompass industrial accidents, traffic accidents, and other human-induced calamities. The database encompasses a global scope, incorporating data from both developed and developing nations. Each recorded event in the EM-DAT database includes crucial information regarding the affected population, including statistics on fatalities, injuries, missing persons, and overall impact. Moreover, for numerous disaster events, estimations of economic losses are also provided. The EM-DAT database is regularly updated to include the latest disaster events. Data integrity is ensured through rigorous verification processes conducted by expert teams, drawing from reliable sources such as government reports, international organizations, non-governmental organizations, and media outlets. Users can access and download data from the EM-DAT database for tailored inquiries through its official website (http://www.emdat.be/). In order to commence the validation process, disaster event data directly pertinent to community safety are extracted from the EM-DAT database. This selection primarily focuses on the major categories of natural and man-made disasters, encompassing meteorological, geological, and biological disasters, and industrial and traffic accidents. By classifying and further subdividing the data according to the types of disasters, the model conducts a detailed risk assessment. This approach allows for a more nuanced understanding of the various subcategories within natural and man-made disasters, enhancing the accuracy and comprehensiveness of the risk assessment process.

Through the method proposed by Biran et al. (2022), inconsistencies and errors in the data are identified, such as incorrect timestamps or misspelled locations. Rule-based automated data cleaning processes, including standardizing naming conventions, formats, and data types, are applied [36]. Combining this with the research of Mavrogiorgos et al. (2022), natural language processing tools are utilized for the analysis and preprocessing of textual data, such as extracting keywords and phrases, eliminating ambiguity, and removing duplicates. Techniques, like named entity recognition and sentiment analysis, are employed to extract more precise information regarding disaster events [37]. Table 4 presents the specific information on the experimental environment.

The models utilized in the experiment encompass a diverse range of cutting-edge technologies. They are CNN, Long Short-Term Memory Network (LSTM), Bidirectional Encoder Representations from Transformers (BERT), Generative Pre-trained Transformer (GPT), and eXtreme Gradient Boosting (XGBOOST). These models have gained widespread recognition across various fields for their exceptional performance in real-world applications, making them prime candidates for comparative analysis. Importantly, they offer varying levels of complexity, allowing for a thorough examination of performance under different model complexities. Furthermore, these models often serve as benchmarks for evaluating new methodologies, highlighting their comparative advantages and innovative features relative to conventional approaches. In order to optimize data utilization and ensure fairness in the experimental setup, standardized parameters are employed. These parameters include setting the output nodes to 5, defining the initial weight range as (0, 1), maintaining a learning rate ranging from 0.01 to 0.8, fixing the number of iterations at 500, setting the learning rate at 0.0001, establishing a training period of 40, implementing a weight decay of 0.001, and utilizing a batch size of 128. Adopting this approach ensures the rationality of initial weights, mitigates the potential impact of overly large or small weights on model training, and effectively manages model complexity to prevent overfitting.

#### 5. Analysis of community safety risk assessment results using optimized BPNN

#### 5.1. Performance analysis of the community safety risk model

In order to improve experimental precision, performance scores related to natural disasters, public health, accidents, and social security are utilized as input variables. The assessment of losses stemming from community safety risk issues in practical scenarios serves as the anticipated output. A total of two hundred datasets are selected for training. The experiment involves varying the number of nodes in the hidden layer, specifically testing configurations of 10, 15, 20, 25, 30, and 35 nodes. Increasing the number of nodes can bolster the model's learning capacity, but an excessive amount may lead to overfitting, wherein the model becomes overly attuned to the training data and struggles to generalize well to new data. Conversely, too few nodes may result in underfitting, where the model fails to capture complex data patterns. Experimenting with different node quantities allows for pinpointing the optimal balance between model performance and complexity, and understanding the impact of network structure on predictive capability.

Comparative indicators include model accuracy and function loss value. Accuracy gauges the correctness of the model's predictions, representing the proportion of instances correctly predicted out of the total instances. The loss function, also known as the cost function, quantifies the discrepancy between the model's predicted values and the actual values, playing a pivotal role in optimizing model parameters during training. Fig. 3 depicts the accuracy and function loss.

Combining the results from Fig. 3(a) and (b), it can be observed that under the maximum training iterations, compared to the BPNN model with 10 hidden layer nodes, the model using 15 hidden layer nodes achieves higher accuracy and lower loss. Additionally, the model with 15 hidden layer nodes exhibits a faster rate of accuracy improvement during the training process. Upon careful examination of Fig. 3(a), when the number of hidden layer nodes reaches 20, the model's accuracy peaks at 99.1 %, surpassing other node configurations. These findings indicate that increasing the number of hidden layer nodes can enhance model performance. However, Fig. 3(b) suggests that as the number of hidden layer nodes continues to increase, the model's accuracy begins to decline, while the loss also increases. This decline is primarily due to decreased model fitting.

As the number of hidden layer nodes increases, the model's complexity also escalates. Initially, augmenting the number of hidden layer nodes boosts the model's expressive capacity, leading to improved accuracy and reduced loss. However, with further increases, the model may encounter overfitting, wherein it excessively tailors itself to the training data but struggles to generalize well to unfamiliar data, resulting in decreased accuracy and increased loss. Hence, when designing the BPNN model, it is crucial to strike a balance and adjust the number of hidden layer nodes accordingly. Optimal performance is achieved with an appropriate number of nodes, as too many or too few can lead to undesirable outcomes such as increased function loss and decreased accuracy. Determining the ideal number of hidden layer nodes through experimentation is essential for achieving superior model accuracy and generalization capability.

Table 4 Experimental environment.		
Facilities	Model	
Central Processing Unit (CPU)	2.5G	
Operating system	Windows7	
Web	Apache-tomecat6	
Memory	12G	



Fig. 3. Comparative results of model performance under different hidden layer nodes (a) comparative accuracy of models; (b) comparative function loss values of models.

#### 5.2. Comparative analysis of factors affecting the community safety risk model

The experiment utilizes 300 sets of data as input to the model, undertaking identification and analysis of events pertaining to natural disasters, public health, accident disasters, and social security. The evaluation indicators comprise average accuracy and maximum accuracy. Average accuracy gauges the overall precision of the classification model across all categories, representing the mean accuracy across different categories. Meanwhile, maximum accuracy denotes the highest accuracy attained by the model within a single category among all categories. Fig. 4 illustrates the results of both average accuracy and maximum accuracy for various models.

Fig. 4(a) displays the maximum accuracy of the optimized model as 99.6 %, while Fig. 4(b) illustrates the average accuracy of the optimized model as 98.5 %, demonstrating the outstanding performance of the optimized model in identifying community risks. Compared to traditional models, the optimized model presented enhances risk factor identification accuracy by approximately 9 %–11 %. Simulation data underscores that the optimization model outperforms other advanced models across all four scenarios, demonstrating its efficiency and accuracy in identifying and assessing community security risks, particularly in handling complex and dynamic data. The high accuracy underscores the optimization model's applicability and generalization across various community security risk types, be it natural disasters, public health crises, accident disasters, or social security issues. Such accuracy is pivotal for implementing effective prevention and response strategies. Comparisons with advanced models like CNN, LSTM, BERT, GPT, and XGBOOST not only highlight the superiority of the optimization model but also underscore the significance of adopting novel strategies and technologies in model design and optimization. These comparisons offer valuable insights for future research, particularly in enhancing model performance and adaptability. In order to further verify the effectiveness of the optimization model presented,



Fig. 4. Comparative results of model accuracy (a) comparative maximum accuracy of models; (b) comparative average accuracy of models.

comparisons are made regarding system operation response time and resource utilization. Fig. 5 illustrates the experimental findings.

Fig. 5(a) demonstrates that the optimized model exhibits significantly improved response times within the range of 100 ms–120 ms, outperforming the comparison model noticeably. This swift responsiveness is paramount for making critical decisions during emergencies, particularly in the realm of community safety risk assessment, where timely analysis and feedback can mean the difference between saving lives or minimizing losses. The accelerated response time of the optimized model across diverse scenarios can be attributed to its innovative advancements in algorithm optimization, data processing, and model structure. Through strategies such as streamlining calculations, optimizing data flow, and leveraging efficient neural network architectures, the model's processing speed is substantially enhanced. Furthermore, in terms of resource utilization, the optimized model demonstrates superior efficiency compared to other models across all four scenarios. Fig. 5(b) suggests that in the "natural disaster" scenario, the optimized model achieves a resource utilization rate of 75.0 %, whereas competing models range from 80.6 % to 98.2 %. This lower resource utilization not only signifies reduced computing resource requirements for community security risk assessment but also underscores the optimization model's adeptness in tackling complex problems. Such efficiency is particularly valuable for deploying the model in resource-constrained environments, where it ensures maximal resource utilization without compromising performance. As a result, the research hypothesis 2 of this paper is validated.

#### 5.3. Community safety risk assessment and countermeasures

A comprehensive risk assessment is conducted for Community A to further validate the efficacy of the optimized model presented. Risk indicators reaching or surpassing the threshold of 80 denote a heightened risk level within the area, demanding immediate attention and intervention. Meanwhile, indices falling between 60 and 79 signal a moderate risk level, necessitating ongoing monitoring and management efforts. Conversely, indices below 60 indicate a comparatively lower risk level, although vigilance should still be upheld. Table 5 displays the outcomes of the safety risk assessment for Community A.

Based on the insights gleaned from this paper, a series of recommendations and strategies are formulated to address community safety risks across multiple domains, including natural disasters, public health concerns, accident disasters, and social security issues. Hypothesis 1 studied in this paper is verified. Table 6 displays the precise details.

These control methodologies and strategies play a vital role in reducing the risks linked to natural disasters, public health issues, accidents, and social security within communities. It is crucial to implement comprehensive measures, strengthen collaboration and coordination across various sectors, and increase safety awareness and community participation. Continuous monitoring, evaluation, and improvement are essential components to ensure community safety.

#### 6. Discussion

The experimental results indicate that when the training iteration is set to 5000 times, the BPNN model with 15 hidden layer nodes exhibits superior performance compared to 10 hidden layer nodes. When the number of hidden layer nodes increases to 20, the model's accuracy reaches 99.1 %, surpassing other node configurations. Increasing the number of hidden layer nodes enhances the model's representation capability, thereby improving accuracy and reducing loss. However, further increments may lead to overfitting, impairing the model's generalization ability, causing accuracy to decline and loss to increase. The model is highly sensitive to hyperparameters introduced during the training process, such as the number of hidden layer nodes. Excessive or insufficient numbers of nodes may both affect model performance. Overreliance on hyperparameter tuning can elevate model complexity, increase computational resource requirements, and even lead to overfitting. The optimized model provides decision-makers with more reliable



Fig. 5. Comparison of model functional indicators (a) Model response speed (b) Resource utilization rate.

Table 5	
Safety risk assessment results for community A.	

Dimensions	comprehensive risk index
natural disaster	67
public health	64
accident disaster	62
safe society	58

#### Table 6

Control methods and strategies for community safety risk.

Dimension	Countermeasure
Natural calamities	Establish a comprehensive natural disaster warning system, including monitoring equipment, warning mechanisms, and information dissemination channels.
	Improve residents' self-help ability and response awareness, and strengthen community-level organization and cooperation.
Public health	Strengthen the monitoring, prevention, and control of infectious diseases, including early detection, tracking of cases, isolating patients, and promoting health knowledge.
	Strengthen the cleanliness and hygiene management of the community environment, including garbage treatment, sewage treatment, and pest control.
Accident disaster	Strengthen the supervision and control of accidents such as hazardous chemicals and fires.
	Strengthen traffic safety management, including road planning, traffic signals, and traffic education.
Social security	Enhance residents' awareness of safety precautions, organize community watch and assistance, and build neighborhood relationships. Strengthen research and prevention of social issues and promote community harmony and stability.

data by enhancing the accuracy of identifying different risk factors. Despite the complexity of the BPNN model's internal operations, its performance can be partially explained by observable indicators such as accuracy, loss rate, and response time. The optimized model demonstrates advantages in resource consumption and processing speed, indicating its potential application in larger or more complex community environments. Considerations must be made for increasing data volume and the availability of computational resources to ensure stability and efficiency when scaling the model. The application of the optimized model in community safety risk assessment has yielded significant results, which may be applicable to other fields or industries such as natural disaster prediction and public health emergency management. Stakeholders including community managers, policymakers, emergency response teams, and residents benefit from the high accuracy and rapid response of the risk assessment model developed. The research findings can be disseminated to these stakeholders through professional papers, policy reports, workshops, training sessions, and demonstration meetings to facilitate practical applications.

Informed by the experimental discoveries, this paper articulates recommendations and strategies to address community safety risks, recognizing it as a multifaceted and critical endeavor. The proposed methods and strategies spanning natural disasters, public health, accidents, and social security effectively mitigate safety risks within communities, safeguarding residents' lives, properties, and community stability. It is crucial to acknowledge that community safety risk control is an ongoing, long-term process that requires continuous improvement and refinement. Moreover, coordinating and harmonizing methods and strategies across various domains are pivotal in establishing a cohesive community safety management system. Only through such an approach can a novel management system ensure community safety and stability, ultimately enhancing residents' quality of life and well-being. In comparison with Yoon et al.'s study (2023) [38], this paper introduces deep learning technology, notably BPNN, for community security risk assessment. This not only enhances the accuracy of assessment but also enables the model to address more complex nonlinear relationships, thereby effectively identifying and predicting potential security risks. Similarly, compared with Kumar et al.'s study (2023) [39], this paper constructs a comprehensive community safety risk assessment index system, encompassing multiple dimensions such as natural disasters, public health, accident disasters, and social security. This ensures the thoroughness and inclusivity of the assessment, rather than being limited to the evaluation of a single risk factor.

#### 7. Conclusion

Accurately assessing the magnitude of community safety risks and understanding the influential factors are crucial for community development and residents' well-being. Therefore, this paper refines the community safety risk assessment model by enhancing the BPNN. Initially, an analysis of the factors influencing community safety incidents is conducted, leading to the formulation of a comprehensive set of evaluation indicators for community safety risk. Subsequently, the BPNN model undergoes optimization, improving the safety risk assessment model through the application of the refined BPNN. Finally, the proposed model's reliability is validated through experimental investigations. The experimental results reveal that when the model's hidden layer node count is set to 20, the recognition accuracy reaches 99.1 %, accompanied by a significantly lower final function loss compared to models with different node quantities. However, further increasing the number of hidden layer nodes leads to overfitting symptoms, resulting in a decline in accuracy. Compared to conventional models, the optimized model exhibits an average accuracy of 98.5 % in community risk identification, with a maximum accuracy of 99.6 %. This represents an improvement of approximately 9 %–11 % in the identification accuracy of various risk factors compared to traditional models, underscoring the reliability of the proposed optimized model.

#### S. Zhou et al.

Nevertheless, this paper has certain limitations. The dynamic nature of community security risks has not been fully considered, particularly the influence of temporal dynamics on security risk assessment. The theoretical significance of this paper lies in uncovering novel insights and providing a new approach to community safety risk assessment that extends existing risk assessment theories. Additionally, the paper applies and refines the BPNN algorithm, offering fellow researchers new methods and tools for similar research areas. The managerial significance of this paper is evident in providing data-driven decision support, aiding community managers and policymakers in more accurately assessing and managing community safety risks. Furthermore, the findings can guide practical safety management and the formulation of preventive strategies, particularly in the domains of natural disasters, public health, accident disasters, and social security.

In subsequent research, this paper proposes a detailed research plan:

Examine the Impact of Hyperparameters: Short-term (1–3 months): detailed experiments are conducted to determine the specific effects of hyperparameters such as the number of hidden layer nodes and learning rate on model performance. Mid-term (4–6 months): an algorithm for adaptive adjustment of hyperparameters is developed to achieve better model performance and energy efficiency.

Assess Model Generalization Ability: Short-term (3–5 months): the model's generalization ability on unknown data is evaluated using techniques like cross-validation. Mid-term (6–9 months): regularization techniques such as dropout and L1/L2 regularization are employed to reduce overfitting and improve model generalization.

Enhance Model Computational Efficiency: Short-term (1-3 months): the current model's performance is evaluated in terms of energy consumption. Mid-term (4-6 months): model structure is optimized, such as employing sparse connections or weight sharing to reduce computational load.

Explore Integrated Approaches: Mid-term (6–12 months): multiple ML methods are combined, such as ensemble learning, to enhance model accuracy and robustness.

Incorporate Additional Data Sources: Long-term (more than 12 months): additional data sources, such as socioeconomic data or meteorological data, are integrated to improve the accuracy and comprehensiveness of risk assessment.

Expand to Larger Community Environments: Long-term (more than 12 months): the study is expanded to larger or more complex communities to assess the scalability and efficiency of the model.

Potential Cross-Domain Applications: Long-term (ongoing): it is to collaborate with community managers, policymakers, and industry experts to translate research findings into practical applications.

In order to ensure ongoing progress tracking and plan adjustments, monthly checks are conducted to ensure consistency with the research timeline, making necessary adjustments as needed. Quarterly evaluations are conducted to assess the effectiveness of completed work and update research directions based on the latest trends. Throughout the study, particular attention is paid to the energy efficiency of the model, especially in environments with large data volumes and limited computational resources. Finally, research results should be disseminated through various channels to ensure stakeholders such as community managers, emergency response teams, and policymakers understand and apply these findings. This can be achieved through workshops, seminars, academic papers, and social media, providing not only research outcomes but also opportunities for feedback collection and inspiring public engagement, thus offering valuable insights for future work.

#### Funding

This work was supported by the Funds of Major Social Science Projects of Tianjin Municipal Education Commission (Grant No. 2021JWZD35).Tianjin Art and Science Planning General Project (Grant No. D24016).

#### CRediT authorship contribution statement

**Shuang Zhou:** Writing – review & editing, Writing – original draft, Resources, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Meiling Du:** Writing – original draft, Validation, Supervision, Resources, Methodology, Investigation, Formal analysis, Data curation. **XiaoYu Liu:** Writing – original draft, Resources, Methodology, Investigation, Data curation. **Hongyan Shen:** Writing – original draft, Supervision, Resources, Investigation.

# Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

# References

S. Holdsworth, O. Sandri, J. Hayes, Planning, gas pipelines and community safety: what is the role for local planning authorities in managing risk in the neoliberal era, Land Use Pol. 100 (17) (2021) 104890.

<sup>[2]</sup> G. Hu, Y. Guo, G. Wei, L. Abualigah, Genghis Khan shark optimizer: a novel nature-inspired algorithm for engineering optimization, Adv. Eng. Inf. 58 (3) (2023) 102210.

- [3] F.L. Lynch, M.J. Hoopes, B.A. Hatch, M. Dunne, A.E. Larson, K.C. Pears, Understanding health need and services received by youth in foster care in community safety-net health centers in Oregon, J. Health Care Poor Underserved 32 (2) (2021) 783–798.
- [4] S. Jung, G. Kitura, Offenders on judicial orders: implications for evidence-based risk management in policing, J. Commun. Saf. Well-Being 7 (1) (2022) 32–39.
  [5] M. Ghasemi, M. Zare, A. Zahedi, M.A. Akbari, S. Mirjalili, L. Abualigah, Geyser inspired algorithm: a new geological-inspired meta-heuristic for real-parameter and constrained engineering optimization, J. Bionic Eng. 56 (13) (2023) 1–35.
- [6] A. Westall, Exploring the contribution and relationship to policing and community safety of volunteer street patrols, Policing: J. Pol. Pract. 15 (4) (2021) 2083–2094.
- [7] S. Ng, S. Shao, N. Ling, Food safety risk-assessment systems utilized by China, Australia/New Zealand, Canada, and the United States, J. Food Sci. 87 (11) (2022) 4780–4795.
- [8] C. Farmer, R. Evans, Do Police need guns? The nexus between routinely armed police and safety, Int. J. Hum. Right. 25 (6) (2021) 1070–1088.
- [9] A.E. Ezugwu, J.O. Agushaka, L. Abualigah, L. Abualigah, S. Mirjalili, A.H. Gandomi, Prairie dog optimization algorithm, Neural Comput. Appl. 34 (22) (2022) 20017–20065.
- [10] S. Formica, Implementation of a post-overdose quick response team in the rural Midwest: a team case study, J. Commun. Saf. Well-Being 7 (2) (2022) 59–66.
  [11] E. Adomah, A. Khoda Bakhshi, M.M. Ahmed, Safety impact of connected vehicles on driver behavior in rural work zones under foggy weather conditions, Transport, Res. Rec. 2676 (3) (2022) 88–107.
- [12] J.O. Agushaka, A.E. Ezugwu, L. Abualigah, Dwarf mongoose optimization algorithm, Comput. Methods Appl. Mech. Eng, 391 (75) (2022) 114570.
- [13] J.O. Agushaka, A.E. Ezugwu, L. Abualigah, Gazelle optimization algorithm: a novel nature-inspired metaheuristic optimizer, Neural Comput. Appl. 35 (5) (2023) 4099–4131.
- [14] B. Sheng, S. Gengxin, Research on the influence maximization problem in social networks based on the multi-functional complex networks model, J. Organ. End User Comput. 34 (3) (2022) 1–17.
- [15] Z. Wang, S. Zhang, Y. Zhao, C. Chen, X. Dong, Risk prediction and credibility detection of network public opinion using blockchain technology, Technol. Forecast. Soc. Change 187 (2023) 122177.
- [16] Y. Zhang, Q. Zhang, Y. Zhao, Y. Deng, H. Zheng, Urban spatial risk prediction and optimization analysis of POI based on deep learning from the perspective of an epidemic, Int. J. Appl. Earth Obs. Geoinf. 112 (4) (2022) 102942.
- [17] X. Wu, Z. Feng, Y. Liu, Enhanced safety prediction of vault settlement in urban tunnels using the pair-copula and Bayesian network, Appl. Soft Comput. 132 (56) (2023) 109711.
- [18] G. Li, X. Wu, J.C. Han, B. Li, Y. Huang, Y. Wang, Flood risk assessment by using an interpretative structural modeling based Bayesian network approach (ISM-BN): an urban-level analysis of Shenzhen, China, J. Environ. Manag. 329 (102) (2023) 117040.
- [19] M.B. Dhudasia, R.W. Grundmeier, S. Mukhopadhyay, Essentials of data management: an overview, Pediatr. Res. 93 (1) (2023) 2–3.
- [20] G. Hu, Y. Zheng, L. Abualigah, A.G. Hussien, DETDO: an adaptive hybrid dandelion optimizer for engineering optimization, Adv. Eng. Inf. 57 (13) (2023) 102004.
- [21] K. Voulgaris, A. Kiourtis, P. Karamolegkos, Data processing tools for graph data modelling big data analytics. 2022 13th international congress on advanced applied informatics winter (IIAI-AAI-Winter), IEEE 1 (1) (2022) 208–212.
- [22] M. Zare, M. Ghasemi, A global best-guided firefly algorithm for engineering problems, J. Bionic Eng. 5 (2) (2023) 1–30.
- [23] S.E. Whang, Y. Roh, H. Song, J.G. Lee, Data collection and quality challenges in deep learning: a data-centric ai perspective, VLDB J. 32 (4) (2023) 791-813.
- [24] M. Ghasemi, M. Zare, A. Zahedi, Optimization based on performance of lungs in body: lungs performance-based optimization (LPO), Comput. Methods Appl. Mech. Eng. 41 (9) (2024) 116582.
- [25] R.I. Mawby, M. Ozascilar, N. Ziyalar, Risk, safety and security among visitors to Istanbul, Tourism Hospit. Res. 21 (1) (2021) 61–72.
- [26] R.F. Southby, B. del Pozo, Challenges and opportunities in educating law enforcement officers: 2020 and beyond, Law Enforc. Pub. Health: Partn. Commun. Saf. Well-being 5 (1) (2022) 65–73.
- [27] J.A. Richards, J.A. Richards, Supervised classification techniques. Remote Sensing Digital Image Analysis, 2022, pp. 263–367.
- [28] A. Mavrogiorgou, A. Kiourtis, D. Kyriazis, M. Themistocleous, A comparative study in data mining: clustering and classification capabilities, in: Information Systems: 14th European, Mediterranean, and Middle Eastern Conference, EMCIS 2017 vol. 14, Coimbra, Portugal, 2017, pp. 82–96.
- [29] J.A. Choi, K. Lim, Identifying machine learning techniques for classification of target advertising, ICT Express 6 (3) (2020) 175-180.
- [30] A.K. Pitol, T.R. Julian, Community transmission of SARS-CoV-2 by surfaces: risks and risk reduction strategies, Environ. Sci. Technol. Lett. 8 (3) (2021) 263–269.
- [31] S. Jiménez-Oyola, E. Chavez, M.J. García-Martínez, D. Bolonio, F. Guzmán-Martínez, P. Romero, Probabilistic multi-pathway human health risk assessment due to heavy metal (loid) s in a traditional gold mining area in Ecuador, Ecotoxicol. Environ. Saf. 224 (32) (2021) 112629.
- [32] G. Lu, W. Fan, D. Lu, Z. Liu, Lung-inspired hybrid flow field to enhance PEMFC performance: a case of dual optimization by response surface and artificial intelligence, Appl. Energy 35 (5) (2024) 122255.
- [33] I. Bartkowiak-Théron, N.L. Asquith, Law enforcement, public health, and vulnerability, in: Law Enforcement and Public Health: Partners for Community Safety and Well-Being, Cham: Springer International Publishing, 2022, pp. 53–63, 13(1).
- [34] A.R. Foster, D.K. Adjekum, A qualitative review of the relationship between safety management systems (SMS) and safety culture in Multiple-Collegiate aviation programs, Colleg, Aviat. Rev. Int. 40 (1) (2022) 63.
- [35] D.J. Ferreira, N. Mateus-Coelho, H.S. Mamede, Methodology for predictive cyber security risk assessment (PCSRA), Procedia Comput. Sci. 219 (112) (2023) 1555–1563.
- [36] O. Biran, O. Feder, Y. Moatti, D. Kyriazis, G. Manias, Baroni S. PolicyCLOUD, A prototype of a cloud serverless ecosystem for policy analytics, Data & Policy 4 (2022) 44.
- [37] K. Mavrogiorgos, A. Mavrogiorgou, A. Kiourtis, S. Kleftakis, D. Kyriazis, Automated rule-based data cleaning using NLP, in: 2022 32nd Conference of Open Innovations Association (FRUCT), IEEE, 2022, pp. 162–168.
- [38] S.S. Yoon, D.Y. Kim, K.K. Kim, I.C. Euom, Vulnerability exploitation risk assessment based on offensive security approach, Appl. Sci. 13 (22) (2023) 12180.
- [39] V. Kumar, H.S. Swain, A. Upadhyay, S. Roy, B.K. Das, Bioaccumulation of potentially toxic elements in commercially important food fish species from lower gangetic stretch: food security and human health risk assessment, Biol. Trace Elem. Res. 55 (3) (2023) 1–14.