Multimedia Tools and Applications (2023) 82:18269–18298
https://doi.org/10.1007/s11042-022-14010-8

ANFIS for risk estimation in risk-based access control model for smart homes

Hany F. Atlam[1,2] · Gary B. Wills[1]

Received: 7 December 2021 / Revised: 27 June 2022 / Accepted: 23 September 2022 /
Published online: 4 October 2022

Abstract

The risk-based access control model is one of the dynamic models that use the security risk as a criterion to decide the access decision for each access request. This model permits or denies access requests dynamically based on the estimated risk value. The essential stage of implementing this model is the risk estimation process. This process is based on estimating the possibility of information leakage and the value of that information. Several researchers utilized different methods for risk estimation but most of these methods were based on qualitative measures, which cannot suit the access control context that needs numeric and precise risk values to decide either granting or denying access. Therefore, this paper presents a novel Adaptive Neuro-Fuzzy Inference System (ANFIS) model for risk estimation in the risk-based access control model for the Internet of Things (IoT). The proposed ANFIS model was implemented and evaluated against access control scenarios of smart homes. The results demonstrated that the proposed ANFIS model provides an efficient and accurate risk estimation technique that can adapt to the changing conditions of the IoT environment. To validate the applicability and effectiveness of the proposed ANFIS model in smart homes, ten IoT security experts were interviewed. The results of the interviews illustrated that all experts confirmed that the proposed ANFIS model provides accurate and realistic results with a 0.713 in Cronbach's alpha coefficient which indicates that the results are consistent and reliable. Compared to existing work, the proposed ANFIS model provides an efficient processing time as it reduces the processing time from 57.385 to 10.875 Sec per 1000 access requests, which demonstrates that the proposed model provides effective and accurate risk evaluation in a timely manner.

✉ Hany F. Atlam
h.atlam@derby.ac.uk

Gary B. Wills
gbw@soton.ac.uk

[1] Electronic and Computer Science Department, University of Southampton, Southampton SO17 IBJ, UK

[2] College of Science and Engineering, University of Derby, Derby DE22 1GB, UK

Keywords Risk estimation · ANFIS model · Internet of things · Smart homes · Security risk · Risk-based access control

1 Introduction

Access control is one of the security mechanisms that is used to resolve security issues in the IoT system. Although traditional access control approaches were successfully applied in different environments to solve various problems, these approaches are designed to provide a relationship between information associated with an access control rule logic and a resource for which access is requested. The implementation of an access control approach is subject to manipulation, which can range from an unexpected situation, including poorly written access policies to several malicious entities acquiring access to a set of existing accounts. Therefore, traditional access control approaches cannot handle unpredicted situations as they are based on static and predefined policies [33]. Hence, they do not suit a dynamic and distributed system like IoT, instead, the IoT system needs a dynamic access control model. The core principle of dynamic access control models is that they take into consideration not only access policies to make access decisions, but also dynamic and real-time features that are estimated at the time of the access request [49]. These real-time features can include trust, risk, context, history and operational need [30, 42]. This provides more flexibility and can adapt to varying situations and conditions while making the access decision.

One of the dynamic access control models is the risk-based access control model. This model uses the security risk value associated with each access request as a criterion to make the access decision. This model permits or denies access requests dynamically based on the estimated risk value [9]. This model performs risk analysis on each user access request to make the access decision [17]. The essential stage of implementing a risk-based access control model is the risk estimation process. This process is based on estimating the possibility of information leakage and the value of that information. The main objective of the risk estimation process is to create a way of arranging risks in the order of importance and use risk numeric values to make access decisions under a specific context [4–6]. Several researchers utilized different methods for risk assessment and management but most of these methods were based on qualitative measures. The quantification of security risk especially in the access control context through the literature is extremely challenging since risk estimation without enough data to describe its likelihood and impact is like predicting the future.

One of the risk estimation techniques suggested by the literature to overcome the lack of a dataset to estimate the security risk value associated with each access request was the fuzzy logic system. Therefore, the authors implemented the fuzzy logic system and published it in [4]. The results demonstrated it creates accurate and realistic risk values for access control operations. However, the fuzzy logic system has some limitations. For example, the scalability of the fuzzy logic system seems to be doubtful since it requires a non-trivial time to estimate the security risks of access control operations. Also, the fuzzy logic system cannot learn or adjust itself to a new environment, which will be a major issue for a dynamic and distributed system like the IoT. Therefore, this paper proposed the Adaptive Neuro-Fuzzy Inference System (ANFIS) model to overcome issues associated with the fuzzy logic system.

This paper proposes a novel ANFIS model to build the risk estimation module in the risk-based access control model for the IoT. The proposed ANFIS model was implemented to estimate the security risk value associated with each access request and then evaluated against access control scenarios of smart homes. The results demonstrated that the proposed ANFIS model provides an efficient and accurate risk estimation technique that can adapt to the changing conditions of the IoT environment. To the best of the authors' knowledge, there is no similar work done before to compare against, hence, ten IoT security experts from inside and outside the UK were interviewed to evaluate the applicability and effectiveness of the proposed ANFIS model on access control scenarios of smart homes. The IoT security experts demonstrated that the proposed ANFIS model provides accurate and realistic risk values.

Compared to existing work reviewed in the literature, the proposed ANFIS model provides a novel solution to effectively implement the risk-based access control model in IoT applications. It provides accurate and realistic risk evaluation for access control operations while adding learning ability which allows the risk-based model to adapt to changing circumstances in the IoT environment. It overcomes the issue of existing static access control approaches by utilizing real-time and contextual features from the IoT environment at the time of making the access request. In addition, since there are no available datasets or previously known numeric access decisions that can be used to compare the proposed model against, ten IoT security experts were interviewed to evaluate the applicability and effectiveness of the proposed ANFIS model in smart homes. The results of the interviews illustrated that all experts confirmed that the proposed ANFIS model provides accurate and realistic results with a 0.713 in Cronbach's alpha coefficient which indicates that the results are consistent and reliable. Also, compared to the fuzzy logic system that was implemented and published by the authors in [4], the proposed ANFIS model provides an efficient processing time in which it reduces the processing time from 57.385 to 10.875 Sec per 1000 access requests, which demonstrates that the proposed model provides effective and accurate risk evaluation in a timely manner. The proposed ANFIS model also adds the learning capability which makes the risk estimation technique able to adapt to changes and unpredicted situations in the IoT environment. The contribution of this paper can be summarized as follows:

- Proposing the ANFIS model to overcome flexibility and scalability issues associated with the fuzzy logic system for the risk estimation.
- Implementing the ANFIS model to estimate security risk values associated with access requests using user context, resource sensitivity, action severity and risk history as risk factors.
- Evaluating the efficiency and accuracy of the proposed ANFIS model against access control scenarios of smart homes.
- Validating the applicability and effectiveness of the proposed ANFIS model in smart homes by interviewing ten IoT security experts.

The remainder of this paper is organized as follows: Section 2 presents related work; Section 3 provides an overview of the ANFIS technique; Section 4 presents the risk-based access control model; Section 5 presents the implementation of the proposed ANFIS model; Section 6 presents experimental results; Section 7 presents results' evaluation using access control scenarios of smart home, Section 8 presents the verification of results through expert interviews, Section 9 provides a discussion, and Section 10 is the conclusion.

2 Related work

Risk-based access control models are mostly utilised to give the access control process the flexibility it requires. To combat flexibility and the inability to manage unanticipated events, some researchers considered developing a risk-based access control approach. The Risk-Adaptable Access Control (RAdAC) model was established by McGraw [32], and it is based on assessing security threats and operational needs for granting or denying access. The risk associated with an access request is calculated using this model, which is then compared to the access control policy. Access is granted if the necessary operational needs and policies are met. However, this model does not include information on how to objectively quantify risk and operational needs. Khambhammettu et al. [27] also created a risk-based model based on object sensitivity, subject trustworthiness, and the differential between them. However, the model does not provide a method for quantitatively estimating risk. Furthermore, in the early stages of the risk assessment process, this approach necessitates a system administrator with extensive knowledge to provide an acceptable value for each input.

Choi et al. [12] proposed a paradigm for a risk-based model for medical information systems that is context-sensitive. This paradigm organises data so that the risk value can be calculated, and the risk can be applied using treatment-based authorization profiling and specifications. This framework determines the access decision based on the severity of the situation and treatment. However, this approach does not provide a method for quantitatively estimating risk. The model is also restricted to medical information systems. In addition, a dynamic risk-based access control strategy for cloud computing was presented by Chen et al. [10]. The risk–trust assessment approach was utilized with the attribute-based access control concept. To determine the access decision, the model uses previous records to calculate the risk threshold value. However, this model lacked contextual elements as well as the ability to learn and adapt to unexpected scenarios. It also relies on previous records only to determine the risk threshold which is not enough for effective access decisions.

The risk estimation process, which evaluates the risk value associated with each access request, is a critical step to build a risk-based access control model. It estimates the risk value associated with each access request, then the estimated risk value is used to determine the access decision either granting or denying access. Without an available dataset to describe risk likelihood and impact, it is hard to provide a quantitative or numeric value for the risk. One of the risk estimation techniques suggested by the literature to overcome the lack of dataset was the fuzzy logic system. For example, Chen et al. [9] have employed the fuzzy logic approach to design a fuzzy multi-level security model. This model measures the risk using the difference between object and subject security levels. So, if the difference was large, the risk value will be high. The output risk is represented as a binary value of 0 (permit) or 1 (deny). However, the model does not explain how to estimate the risk quantitively and how fuzzy rules were built. In addition, the model did not mention the scalability, inability to learn and time overhead issues associated with the fuzzy logic system.

In addition, Ni et al. [36] utilized the fuzzy logic system to evaluate security risks. This approach uses subject and object security levels to measure the risk value. However, the proposed approach faces many challenges regarding scalability as it requires a long time to estimate the security risk value, especially with the increasing number of input parameters and fuzzy rules. Also, the proposed approach did not provide any information about the fuzzy rules and how they built them. Also, Li et al. [31] have introduced a fuzzy modelling-based method for evaluating the security risks of a healthcare information system. This model measures the risk related to the access request using action severity, risk history, and data sensitivity. However, the model did not provide information about how to evaluate risk values quantitatively. In addition, it requires prior knowledge about various environment situations to build fuzzy rules and does not involve real-time and contextual attributes to determine the access decision.

Since the current research does not have an available dataset that can be used to estimate the security risk for each access request quantitively, the authors implemented the fuzzy logic system and published it in [4] based on the recommendations of the literature review. Although the fuzzy logic system provided precise and realistic risk values for implementing the risk-based access control paradigm [4], its scalability and inability to learn were significant drawbacks. In addition, one of the problems that exist while implementing the fuzzy logic system was determining the appropriate Membership Function (MF) and other fuzzy logic parameters that need to be selected based on experimentations which were not possible due to the lack of datasets.

To resolve the issues associated with the fuzzy logic system, ANFIS has been utilized. It can provide several advantages as well as resolve issues related to the fuzzy logic system. ANFIS is one of the techniques that has been utilized in risk assessment in several domains. For example, it has been utilized by Kristjanpoller & Michell [28] to combine external factors to estimate the risk of a stock market in the Latin American region. The authors first determined the states of the factors using Markov switching and then utilized ANFIS to identify the individual impact of each factor. The authors demonstrated that their methodology improves the risk prediction rate in the stock market. ANFIS was also utilized by Rajabi et al. [38] for diagnosing Liver disorders. The authors utilized ANFIS with Particle Swarm Optimization (PSW) to tune different parameters of the ANFIS model. The authors illustrated that the performance of the new combined system overfits the accuracy of the traditional fuzzy system and ANFIS. However, both papers neither provided how to estimate the risk quantitatively so it can be used in the access control context nor validated their proposed work on real-life applications.

In terms of risk assessment, ANFIS has been utilized by several researchers. For instance, Shahzadi et al. [41] adopted ANFIS to reduce security risks in cloud computing through building protection techniques to ensure maximum data protection. However, there were no details about the result and how their ANFIS model was implemented and verified. Also, Alawad et al. [1] developed a framework to develop an intelligent and dynamic system for managing risk factors in stations. The framework utilized transfer efficiency and retention rate to identify the risk level that is related to overcrowding. The authors illustrated that the resultant framework provides effective and efficient risk management in the railway station. However, there were no details about the result and how their ANFIS model was implemented and verified.

Yao et al. [26] proposed an ANFIS model to evaluate security risks in healthcare web applications. The authors utilized ANFIS to identify security risks and their assessment during the development of healthcare web applications. They first identified the risk factors and then estimated the risk using ANFIS. The results demonstrated that the ANFIS provides acceptable and accurate risk values. However, the applicability of the results was not verified with real-life applications, especially in the IoT context. Also, Kaur et al. [56] utilized ANFIS to improve authentication in mobile devices. The authors used ANFIS to build an implicit authentication system based on behavioural data collected for 12 weeks from different android users. The experimental results demonstrated that the ANFIS provided an efficient authentication method and reduced manual tuning and configuration tasks since it is capable of self-learning. However, this approach only utilizes past behaviour for authentication which is not efficient and lacks contextual and real-time features that can provide more flexibility to the authentication system and make it adapt to unpredicted changes.

We can conclude that the major research gap to implement a risk-based access control model is providing an effective, accurate and realistic risk estimation technique that evaluates the security risk value associated with each access request quantitively. Due to the unavailability of datasets that describe risk likelihood and impact, the risk estimation process becomes a complex process and seems like predicting the future. To overcome this problem, the authors utilized and implemented the fuzzy logic system successfully with the help of IoT security experts to accurately define the parameters of the fuzzy logic system and published the results in [4]. However, the scalability of the fuzzy logic system seems to be doubtful since it requires a non-trivial time to estimate the security risks of access control operations. Also, the fuzzy logic system cannot learn or adjust itself to a new environment, which will be a major issue for a dynamic and distributed system like the IoT. Therefore, this paper utilizes the ANFIS to overcome issues associated with the fuzzy logic system and add learning capabilities to the risk estimation technique. To the best of the authors' knowledge and after an extensive investigation in various research databases, no research exists that utilizes ANFIS in risk-based access control models. Therefore, this paper provides a novel ANFIS model to implement the risk estimation process in the risk-based access control model for the IoT system.

3 An overview of ANFIS

ANFIS is a multilayer feed-forward network that utilizes Artificial Neural Network (ANN) techniques and fuzzy reasoning to map inputs into an output. It is a Fuzzy Inference System (FIS) implemented in the framework of adaptive neural networks [48]. The ANFIS is a hybrid neuro-fuzzy model that uses the decomposition approach to extract rules at individual nodes within the ANN. Then, the extracted rules are combined to construct global behaviour descriptions [57]. Typically, the ANFIS network consists of connected nodes that depend on parameters that change constantly using the learning techniques to minimize the error. The most common learning techniques in the ANFIS are backpropagation and hybrid learning methods [25, 53].

The main objective of the ANFIS model is to optimize the parameters of the fuzzy logic system by applying a learning algorithm using input-output datasets. The parameter optimization is done in a way such that the error measure between the target and the actual output is minimized [23, 55]. The ANFIS has a higher capability to adapt to its environment in the learning process. Therefore, it can be used to adjust the MFs and reduce the error rate automatically to determine the fuzzy rules of the fuzzy logic system. The ANFIS combines the benefits of the fuzzy logic system and ANN into a single technique [25]. It provides better results for applications where performance is more important than interpretation since the learning results may be difficult to interpret [50, 54].

The ANFIS consists of five layers: fuzzy layer, product layer, normalized layer, defuzzification layer, and summation layer [50], as shown in Fig. 1. Layer 1 is the input layer. The crisp input values are transformed into fuzzy values by the MFs in this layer. The output from each node is a degree of membership value that is given by the input of MFs [44].

Layer 2 is the fuzzification layer. Neurons in this layer represent fuzzy sets used in the antecedents of the fuzzy rules. A fuzzification neuron receives a crisp input and determines the degree to which this input belongs to the neuron's fuzzy set. Every node in this layer is fixed and the node is labelled as $\prod$. The output node is the result of multiplying the signal coming

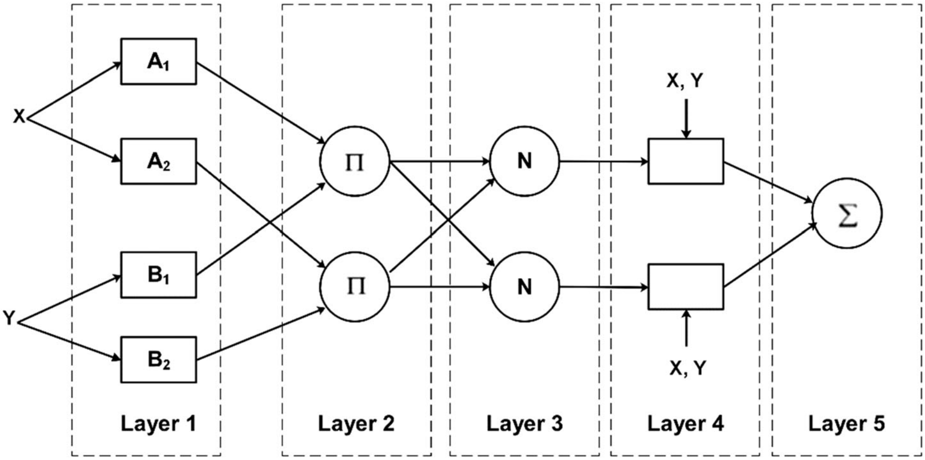


Fig. 1 Architecture of ANFIS [9]

into the node and delivered to the next node. Each node in this layer determines the weighting factor of each rule [19].

Layer 3 is the fuzzy rule layer. Each fuzzy rule is represented by a neuron in this layer. This neuron receives inputs from the fuzzification neurons that represent fuzzy sets in the rule antecedents. Every node in this layer is fixed and the node is labelled as N. Layer 4 is the output membership layer. Neurons in this layer represent the fuzzy sets used in the consequence of fuzzy rules. An output membership neuron combines all its inputs by using the fuzzy operation union [47]. Layer 5 is the defuzzification layer. Each neuron in this layer represents a single output of the ANFIS. It takes the output fuzzy sets with different weights of fuzzy rules and combines them into a single fuzzy set. The single node in this layer provides the overall output as the summation of all incoming signals from the previous node. In this layer, the node is labelled as $\sum$ [50].

4 Risk-based access control model

Unauthorized information disclosure is one of the critical challenges in the IoT system that need to be addressed. Current traditional access control models cannot resolve this challenge since these models are built using static and predefined policies that always give the same result in different situations [29, 31]. Therefore, they are not flexible to resolve the varying behaviour of users, especially in a dynamic environment like the IoT. On the other hand, dynamic access control approaches provide an efficient solution for dynamic environments, like IoT, as they utilize not only access policies but also real-time and contextual features [2].

The risk-based access control model is one of the dynamic models that use the security risk value associated with each access request as a criterion to determine the access decision. It performs a risk analysis to estimate the security risk value for each access request and then uses the estimated risk value to decide either granting or denying access [17, 42].

A dynamic risk-based access control model for the IoT is proposed by the authors and discussed in [4, 6, 7]. The proposed model has four inputs: user/agent context, resource sensitivity, action severity and risk history, as shown in Fig. 2. These inputs/risk factors are

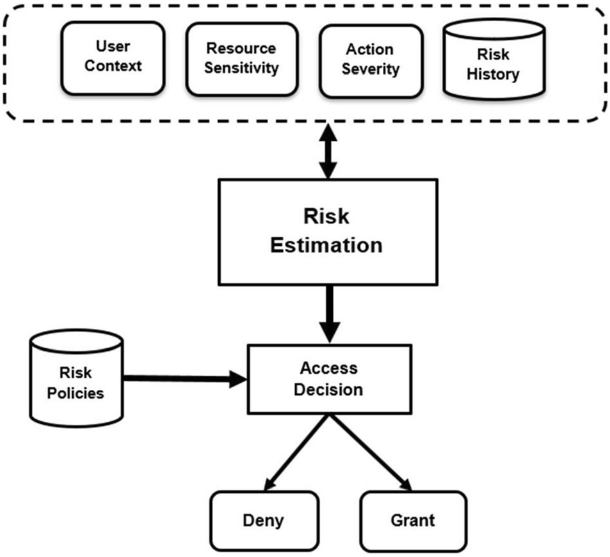


Fig. 2 Dynamic risk-based access control model

used to estimate the security risk value associated with the access request. Then, the estimated risk value is compared against risk policies to specify the access decision. The eventual goal of the proposed risk-based model is to create a system that encourages information sharing to maximize organization benefits while keeping users responsible for their actions and preventing the expected damage that the organization could suffer due to sensitive information disclosure.

5 Implementation of the proposed ANFIS model

The fuzzy logic system is one of the risk estimation techniques that can be used to estimate the security risk value associated with each access request. The fuzzy logic system has many advantages. It is flexible, robust, and based on natural language which makes it easy to understand. It is also tolerant to imprecise data in which it can work even when there is a lack of rules [20, 35]. Some researchers utilized the fuzzy logic system to estimate the security risk in access control models. Chen et al. [9] used the fuzzy logic system to build an MLS access control model to access information of IBM systems. Also, Li, Bai and Zaman [31] presented a fuzzy modelling-based approach for evaluating the risk associated with the access request for healthcare information access. Based on the literature review that recommended using the fuzzy logic system as a risk estimation method when there is no available dataset, we implemented the fuzzy logic system in [4]. The fuzzy logic risk estimation approach was implemented, and the results of access control scenarios of a network router demonstrated it can provide realistic and accurate risk values for access control operation [4].

Although the fuzzy logic system provides accurate and realistic risk values, the scalability of the fuzzy logic system seems to be doubtful since it requires a non-trivial time to estimate the security risks of access control operations [52]. An access control model for the IoT system is intended to serve hundreds or thousands of users. In addition, providing a scalable and able to learn risk estimation technique is one of the main objectives to produce a better and more efficient risk estimation approach. To achieve this target, the Artificial Neural Network (ANN) is proposed to be integrated with the fuzzy logic system. ANN is a low-level computational structure that performs well when dealing with raw data [39, 51]. It can learn to produce output even with incomplete information, after being trained. In addition, it provides parallel processing capabilities that improve overall system efficiency [11]. One of the solutions that integrate ANN with the fuzzy logic system is ANFIS. It combines the parallel computation and learning capabilities of ANN with the human-like knowledge representation and explanation abilities of the fuzzy logic system [18].

Implementing the ANFIS model requires defining linguistic expressions for both input and output, defining fuzzy sets for input and output, specifying MFs, building the fuzzy rules, and training the neural network. Since linguistic expressions, fuzzy sets, MFs, and fuzzy rules were specified based on the interviews conducted earlier in this research, as detailed in [4], we will discuss the training and testing of the risk estimation technique with ANFIS directly. The ANFIS model of the proposed risk estimation technique was trained to determine the appropriate number of epochs, MF, and learning methods that produce the lowest error and the best fit with the learning process. Figure 3 shows the structure of the ANFIS model of the proposed risk estimation technique.

As shown in Fig. 3, the ANFIS model of the proposed risk estimation technique has five layers. The input layer contains four risk factors of the proposed risk-based access control model involving user context, resource sensitivity, action severity, and risk history. The second layer contains fuzzy sets of each input in which each risk factor is represented by three fuzzy sets. The third layer represents the fuzzy rules of the risk estimation technique, which are 81 rules. The fourth layer represents the output MF, which was represented by five fuzzy sets. The fifth layer represents the output layer which is the estimated risk value of the risk estimation process. The specifications of the proposed ANFIS model can be shown in Table 1.

The main objective of training the ANFIS model of the proposed risk estimation technique is to tune different MFs and determine the appropriate MF that produces the lowest error and the best fit with the learning process. In addition, adding the learning capability to the risk

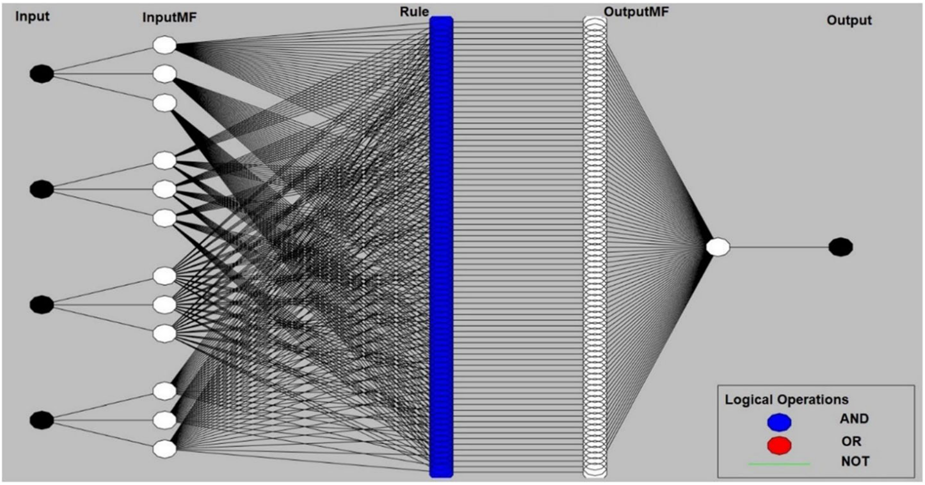


Fig. 3 The structure of the proposed ANFIS model for the risk estimation

Table 1 Specifications of the proposed ANFIS model

Parameter	Description/Value
Structure of FIS	Sugeno FIS
Number of inputs	4
Number of outputs	1
Number of input membership functions	3, 3, 3, 3
Optimization method	Backpropagation and Hybrid
Number of MFs	8 (TriMF, TrapMF, GbellMF, GaussMF, Gauss2MF, PiMF, DsigMF, and PsigMF)
Training epoch number	20, 100, 300

estimation process to adapt to new changes in various IoT applications and increase the accuracy of resultant risk values for future access requests.

6 Experimental results

Several experiments were carried out to train the ANFIS model of the proposed risk estimation technique to increase the accuracy of the output risk, tune different MFs and identify the appropriate MF that can lead to the lowest error and the best fit with the learning process at different number of training epochs. All training functions and experiments were coded and executed using MATLAB software. All experiments and measurements are coded using MATLAB on Intel(R) Core (TM) i7–2600, 3.40 GHz CPU with 16 GB RAM running Windows 10.

6.1 Data collection

Implementing the ANFIS model requires having a dataset or examples for training. A dataset containing 160,000 records was utilized to train the ANFIS. To avoid possible bias in the sample data to the ANFIS model, the dataset was randomized and divided into two sets using the cross-validation method.

- **Training set**: This set contains 112,000 data records (70% of the dataset) to train the ANFIS model.
- **Testing set**: This set contains 48,000 data records (30% of the dataset) to test the ANFIS model.

6.2 Performance Evaluation

The ANFIS model was trained and the performance was evaluated using Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), correlation coefficient (R), and coefficient of determination (R-square or R^2), as recommended in related ANFIS models [21, 46]. The performance of the ANFIS model of the proposed risk estimation technique was tested at three different epochs; 20, 100, and 300 to observe error rates at different epochs and observe the performance when increasing the number of epochs.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(O_i - P_i\right)^2} \tag{1}$$

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left(O_i - P_i\right) \tag{2}$$

$$R = \frac{n\sum_{i=1}^{n} O_i P_i - \sum_{i=1}^{n} O_i \sum_{i=1}^{n} P_i}{\sqrt{\left(n\sum_{i=1}^{n} O_i^2 - \left(\sum_{i=1}^{n} O_i\right)^2\right)\left(n\sum_{i=1}^{n} P_i^2 - \left(\sum_{i=1}^{n} P_i\right)^2\right)}} \tag{3}$$

$$R^2 = 1 - \left(\frac{\sum_{i=1}^{n}\left(O_i - \overline{O}\right) \times \left(P_i - \overline{P}\right)}{\sqrt{\sum_{i=0}^{n}\left(O_i - \overline{O}\right)^2} \times \sqrt{\sum_{i=0}^{n}\left(P_i - \overline{P}\right)^2}}\right)^2 \tag{4}$$

Where n is the total number of data, Oi is the observed (target) value, Pi is the predicted value,$\overline{O}$ is the mean observed value, and $\overline{P}$ is the mean predicted value.

6.3 Training ANFIS model

The performance of most machine learning techniques is improved by training. The training dataset is a set of input and output vectors. Two vectors are used to train the ANFIS system: the input vector and the output vector. The training dataset is used to find the premise parameters for the MFs. A threshold value for the error between the observed and predicted output is determined to be 0.05 [3]. The consequent parameters are decided using the least-squares method. If this error is larger than the threshold value, then the premise parameters are updated using the gradient descent method. The process is terminated when the error becomes less than the threshold value. The checking dataset is then used to test the ANFIS model with the actual data [25].

The ANFIS model of the proposed risk estimation technique was trained using both hybrid and backpropagation learning methods. Eight MFs were utilized in the training process to determine the appropriate learning method as well as the appropriate MF to implement the risk estimation process of the proposed risk-based model. These MFs include TriMF, TrapMF, GbellMF, GaussMF, Gauss2MF, PimF, DsigMF, and PsigMF.

After the training was completed, the performances of the ANFIS model were evaluated to determine the best fuzzy parameters with the lowest error and the best fit. The trained FIS of each MF was utilized to produce the predicted output. Then, the predicted output was compared with the observed output to determine the error using MAE and RMSE and determine the best fit with the learning process using R and R^2. Several experiments were carried out to train the ANFIS model and evaluate the performance of the trained FIS.

The training dataset was used to train the ANFIS, whereas the testing dataset was used to test the accuracy of the trained ANFIS model. To produce the lowest error and the best fit with the learning process, the ANFIS model was trained at three different epochs: 20, 100, and 300. In the next section, the results of training the ANFIS model at 20, 100, and 300 epochs will be discussed.

6.3.1 Training using backpropagation learning method

Backpropagation is a common learning method in the ANN. It is a method of training multilayer ANNs by using the process of supervised learning. Supervised algorithms are based on errors in which the external reference signal is used to produce an error signal by comparing the produced output with the reference signal. Using the generated error signal, the ANFIS updates its parameters to improve the system performance [40]. The backpropagation method learns by evaluating the output layer to extract errors in the hidden layers. Due to its flexibility and learning capabilities, it has been implemented successfully in multiple applications [24].

The ANFIS model of the proposed risk estimation technique was trained using the Backpropagation learning method at three different epochs numbers 20, 100, and 300 to investigate the learning rate of the ANFIS model with different epochs and determine the best MF that produces the lowest error and the best fit with the learning process.

The ANFIS model was trained using the Backpropagation learning method at 20 epochs with eight MFs to determine the best MF that produces the lowest error and the best fit with the learning process. After the ANFIS model was trained, the entire dataset was utilized to check the performance and accuracy of the ANFIS model. RMSE and MAE values were used to indicate the error value between the predicted values obtained from the trained ANFIS model against the original values. In addition, R and R^2 were used to show the model fitness with the training process. Results of training the ANFIS model at 20 epochs can be shown in Table 2.

As shown in Table 2, the results showed that the backpropagation learning method produced a decrease in both training and testing errors. All eight MFs showed a large decrease in both training and testing errors. However, the results showed that the backpropagation learning method produces large RMSE and MAE error values and small R and R^2 values. This, in turn, reflects the fact that the relationship between the predicted and observed data is less efficient and needs more training. In addition, the R^2 values were negative which implies

Table 2 Performance evaluation of the ANFIS model with the Backpropagation learning method at 20 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Backpropagation	TriMF	51.5436	51.5447	51.5337	48.2481	0.8317	−5.4804
	TrapMF	51.3364	51.3235	51.3188	48.1093	0.7262	−5.4264
	GbellMF	52.0326	52.0314	52.0209	48.6320	0.8700	−5.6035
	GaussMF	51.7004	51.6991	51.6893	48.3604	0.8710	−5.5195
	Gauss2MF	51.3429	51.3335	51.3266	48.1076	0.7379	−5.4284
	PiMF	51.3242	51.3098	51.3064	48.0995	0.7106	−5.4233
	DsigMF	51.3346	51.3242	51.3180	48.0988	0.7339	−5.4262
	PsigMF	51.3346	51.3242	51.3180	48.0988	0.7339	−5.4262

there is an inverse relationship between the predicted and observed data such that the increase in the predicted data will cause a decrease in the observed data.

The significant aspect observed from applying the backpropagation learning method at 20 epochs is that the training and testing errors decreased dramatically when increasing the number of epochs with all eight MFs. Figure 4 shows a dramatic decrease in both training and testing RMSE errors when applying TrapMF with the backpropagation learning method at 20 epochs.

After the ANFIS model was trained at 20 epochs, it was trained at 100 epochs to observe the performance when increasing the number of epochs. The reason to train the ANFIS model at 100 epochs is that the training at 20 epochs demonstrated a significant decrease in training and testing errors with the backpropagation learning method. Several experiments were carried out at 100 epochs with eight MFs to determine the best MF that produces the lowest error and the best fit with the learning process using the backpropagation training method. Training and testing errors and performance evaluation resulting from the training can be shown in Table 3.

As shown in Table 3, the results demonstrated that the ANFIS behaviour at 100 epochs was similar to the one at 20 epochs. Increasing the number of epochs to 100 demonstrated a dramatic decrease in training and testing errors for all MFs with the backpropagation learning method. The training error decreased from 51.3 at 20 epochs to reach 28.3 at 100 epochs for both DsigMF and PsigMF, which demonstrates the effect of increasing the number of epochs. Figure 5 shows training and testing errors at 100 epochs when applying the TriMF with the backpropagation learning method.

Training the ANFIS model with the backpropagation learning method showed it needs more training to achieve better results. Therefore, the ANFIS model was trained at 300 epochs to observe the performance when increasing the number of epochs to 300. Several experiments were carried out at 300 epochs with eight MFs using the backpropagation training method to determine the best MF that produces the lowest error and the best fit with the learning process. Results of training the ANFIS model at 300 epochs using the backpropagation training method can be shown in Table 4.

As shown in Table 4, increasing the number of epochs to 300 demonstrated a dramatic decrease in training and testing errors for all MFs. The training error decreased from 29.3 at

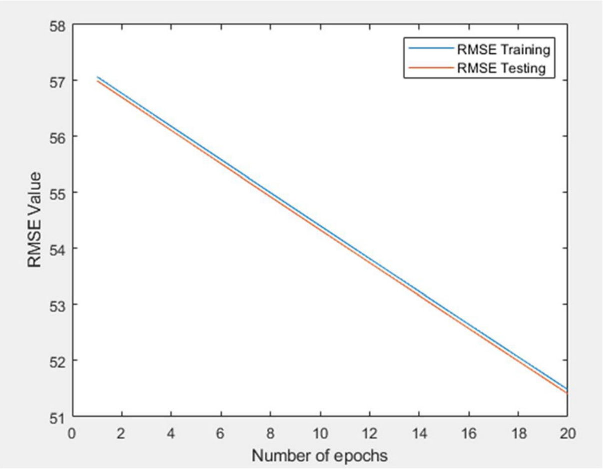


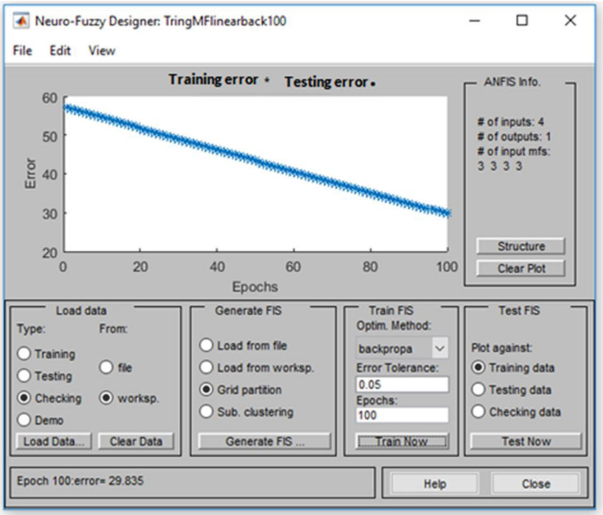
Fig. 4 RMSE of training and testing errors when applying TrapMF with backpropagation method at 20 epochs

Table 3 Performance evaluation of the ANFIS model with the Backpropagation learning method at 100 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Backpropagation	TriMF	29.5731	29.5992	29.5857	27.1901	0.8436	−1.1359
	TrapMF	29.4777	29.4701	29.4643	26.7725	0.7857	−1.1184
	GbellMF	31.3456	31.3513	31.3471	28.8931	0.8770	−1.3978
	GaussMF	30.0580	30.0639	30.0624	27.7479	0.8781	−1.2053
	Gauss2MF	29.3942	29.3970	29.3847	26.7108	0.7888	−1.1070
	PiMF	29.5411	29.5357	29.5294	26.7731	0.7794	−1.1278
	DsigMF	28.3863	28.3875	28.3793	25.5234	0.7763	−0.9653
	PsigMF	28.3862	28.3874	28.3792	25.5233	0.7763	−0.9652

100 epochs to 5.8 at 300 epochs for the Gauss2MF, which demonstrates the effect of increasing the number of epochs. Figure 6 shows training and checking errors when applying the TriMF with the backpropagation learning method at 300 epochs. It showed that the error decrease has almost stopped, which implies that there is no need for more training.

The results of training the ANFIS model using the backpropagation learning method at 20, 100, and 300 epochs have demonstrated that all MFs have shown a significant decrease in both RMSE and MAE values and a significant increase in R and R^2 values when increasing the number of epochs. For example, the RMSE value of the TriMF decreased from 51.53 to 29.59 when increasing the number of epochs from 20 to 100 and further decreased to 6.34 when increasing the number of epochs to 300. There was a negative sign of R^2 values at 20 and 100 epochs which implies there was an inverse relationship between the predicted and observed data. This negative sign disappeared when increasing the number of epochs to 300. After applying the backpropagation learning method with the different number of epochs, the results demonstrated that the Gauss2MF is the best MF as it produced the lowest RMSE (5.888) and MAE (4.577) values and the highest R (0.957) and R^2 (0.915) values.



# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Type: ○ Training ○ Testing ● Checking ○ Demo
From: ○ file ● worksp.

○ Load from file
○ Load from worksp.
● Grid partition
○ Sub. clustering

Optim. Method: backpropa
Error Tolerance: 0.05
Epochs: 100

Plot against: ● Training data ○ Testing data ○ Checking data

Epoch 100:error= 29.835

Fig. 5 Training and testing errors with TriMF and backpropagation learning method at 100 epochs

Table 4 Performance evaluation of the ANFIS model with the Backpropagation learning method at 300 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Backpropagation	TriMF	6.3084	6.3647	6.3402	5.0299	0.9497	0.9019
	TrapMF	5.9086	5.9446	5.9357	4.6255	0.9561	0.9140
	GbellMF	6.2915	6.3496	6.3289	4.9915	0.9500	0.9023
	GaussMF	6.4113	6.4639	6.4493	5.0978	0.9480	0.8985
	Gauss2MF	5.8614	5.8983	5.8884	4.5774	0.9568	0.9154
	PiMF	6.0306	6.0661	6.0598	4.7266	0.9542	0.9104
	DsigMF	9.9248	10.0127	9.9500	7.8745	0.8949	0.7584
	PsigMF	7.5377	7.5890	7.5597	6.0057	0.9317	0.8605

6.3.2 Training using hybrid learning method

The hybrid learning method is one of the common ANFIS learning methods proposed by Jang [25]. It consists of two main parts, namely forward and backward pass. In the forward pass, the parameters of the premises in the first layer should be in a steady-state. A Recursive Least Square Estimator (RLSE) method is applied to repair the consequent parameter in the fourth layer. Then, after the consequent parameters are obtained, input data are passed back to the adaptive network input, and the produced output is compared against the actual output [44]. While in the backward pass, the consequent parameters should be in a steady-state. The error occurred during the comparison between the produced output and the actual output is propagated back to the first layer. At the same time, the parameter premises in the first layer are updated using gradient descent or backpropagation learning methods. With the use of the hybrid learning method, it can ensure the convergence rate is faster because it reduces the dimensional search space in the original method of backpropagation [37].

Similarly, the ANFIS model of the proposed risk estimation technique was trained using the hybrid learning method at three different epochs numbers 20, 100, and 300 to investigate the

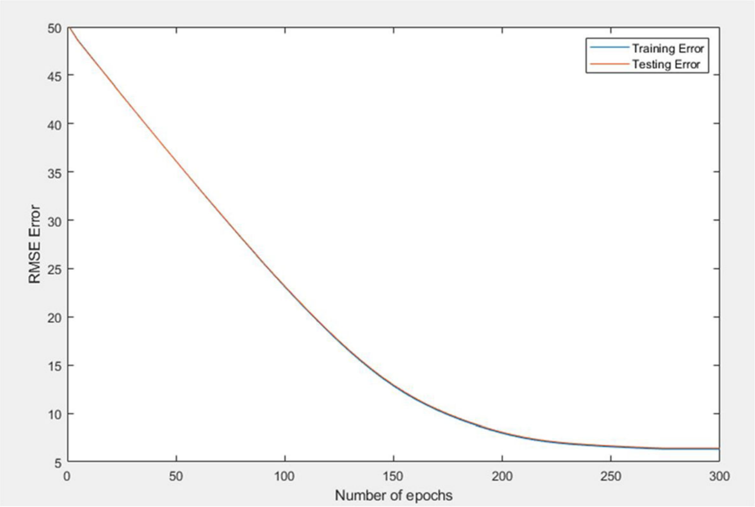


Fig. 6 Training and testing errors with TriMF and backpropagation learning method at 300 epochs

learning rate of the ANFIS model with different epochs and determine the best MF that produces the lowest error and the best fit with the learning process. Results of training the ANFIS model at 20 epochs can be shown in Table 5.

As shown in Table 5, the training and testing errors are very small for all eight MFs. The results demonstrated that four MFs including TrapMF, PiMF, DsigMF, and Gauss2MF produced the same training and testing errors during all 20 epochs, which illustrates that no error enhancement or reduction occurs with these MFs when increasing the number of epochs. Figure 7 shows training and testing errors when applying TrapMF with the hybrid learning method at 20 epochs, which illustrates that no error reduction occurs when increasing the number of epochs. While another four MFs including TriMF, GbellMF, PiMF, and GaussMF show a slight decrease in training and testing errors when increasing the number of epochs from 1 to 20. Figure 8 shows RMSE training error when applying TriMF with the hybrid learning method. It shows a slight decrease in the error when increasing the number of epochs from 1 to 20.

In the same way, the ANFIS model was trained using the hybrid learning method at 100 epochs with eight MFs. Results of training the ANFIS model at 100 epochs can be shown in Table 6. The results demonstrated that the ANFIS behaviour at 100 epochs was similar to the one at 20 epochs in which the training and testing errors showed a very slight decrease compared to error values produced at 20 epochs, as depicted in Table 6.

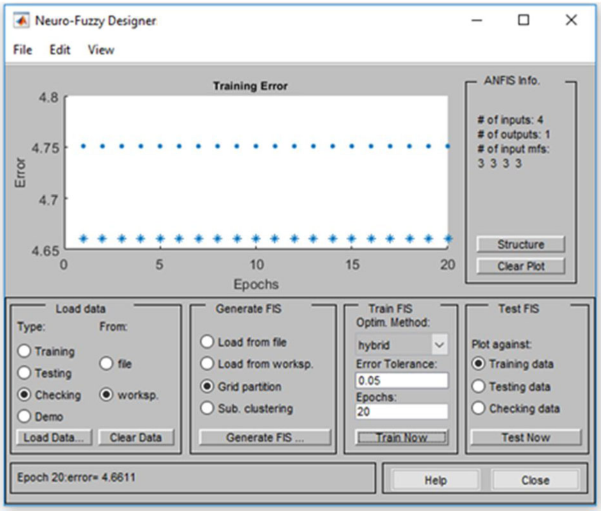
The ANFIS model of the risk estimation approach was trained using the hybrid learning method at 300 epochs with eight MFs. Results of training the ANFIS model at 300 epochs can be shown in Table 7.

The results demonstrated that the ANFIS behaviour at 300 epochs was similar to the one at 20 and 100 epochs in which the training and testing errors showed a very slight decrease compared to error values produced at 20 or 100 epochs. In other words, a group of MFs including TrapMF, Gauss2MF, DsigMF, PsigMF did not show any differences in training and checking errors as well as performance evaluation metrics when increasing the number of epochs to 300. While another group of MFs including TriMF, GbellMF, GaussMF, and PiMF have shown a very small decrease in training and testing errors when increasing the number of epochs to 300. Figure 9 shows training and testing errors when applying the GbellMF with the hybrid learning method at 300 epochs.

The results of training the ANFIS model using the hybrid learning method at 20, 100, and 300 epochs have demonstrated that a group of MFs including TrapMF, Gauss2MF, DsigMF, and PsigMF did not show any changes in RMSE and MAE values as well as R and R^2 values

Table 5 Performance evaluation of the ANFIS model with the Hybrid learning method at 20 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Hybrid	TriMF	5.3507	5.4031	5.3784	4.2339	0.9641	0.9294
	TrapMF	4.6438	4.6552	4.6647	3.5611	0.9731	0.9469
	GbellMF	5.1626	5.1762	5.2392	4.0783	0.9659	0.9330
	GaussMF	5.2102	5.2341	5.1913	4.0109	0.9666	0.9342
	Gauss2MF	4.6611	4.6706	4.6810	3.5720	0.9729	0.9465
	PiMF	4.8445	4.8525	4.8678	3.7118	0.9707	0.9422
	DsigMF	4.6974	4.7069	4.7184	3.5982	0.9725	0.9457
	PsigMF	4.6975	4.7068	4.7184	3.5984	0.9725	0.9457



# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Optim. Method: hybrid

Error Tolerance: 0.05

Epochs: 20

Epoch 20:error= 4.6611

Fig. 7 Training and testing error when applying TrapMF with the hybrid learning at 20 epochs

when increasing the number of epochs from 1 to 300. While another group of MFs including TriMF, GbellMF, GaussMF, and PiMF have shown a very slight decrease in RMSE and MAE values and a very small increase in R and R^2 values when increasing the number of epochs. For instance, the RMSE value of the TriMF decreased from 5.378 to 5.375 when increasing the number of epochs from 20 to 100 and further decreased to 5.366 when increasing the number of epochs to 300. The same behaviour continued for this group of MFs except for GaussMF which showed a different behaviour, in which the RMSE value increased from 5.191 at 20 epochs to 5.222 when increasing the number of epochs to 100, but it decreased again to reach 5.168 when increasing the number of epochs to 300. In addition, the GbellMF produced the largest amount of error decrease among other MFs in which its RMSE value decreased from 5.239 at 20 epochs to 5.013 at 300 epochs.

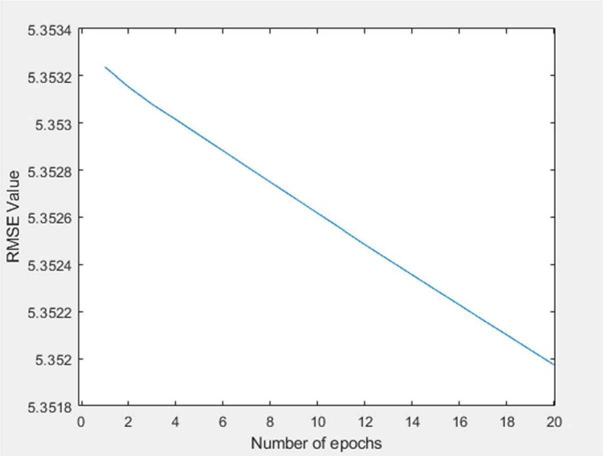


Fig. 8 RMSE training error when applying TriMF with the hybrid learning method

Table 6 Performance evaluation of the ANFIS model the hybrid learning method at 100 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Hybrid	TriMF	5.3473	5.3998	5.3748	4.2320	0.9641	0.9295
	TrapMF	4.6438	4.6552	4.6647	3.5611	0.9731	0.9469
	GbellMF	5.1084	5.1298	5.1370	3.9757	0.9673	0.9356
	GaussMF	5.1928	5.2197	5.2222	4.0634	0.9662	0.9335
	Gauss2MF	4.6611	4.6706	4.6810	3.5720	0.9729	0.9465
	PiMF	4.8392	4.8467	4.8623	3.7075	0.9707	0.9423
	DsigMF	4.6974	4.7069	4.7184	3.5982	0.9725	0.9457
	PsigMF	4.6975	4.7068	4.7184	3.5984	0.9725	0.9457

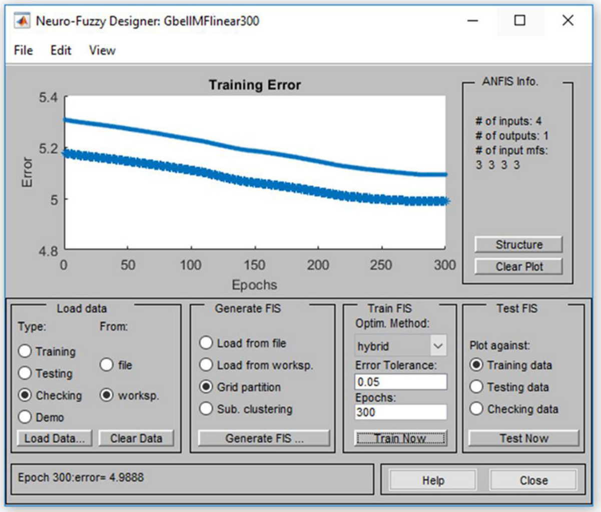
Investigating the results of training the ANFIS model using both hybrid and backpropagation learning methods demonstrates that the TrapMF with the hybrid learning method at 20 epochs is the optimal combination to implement the ANFIS model of the proposed risk estimation technique. It produced the lowest RMSE and MAE values as well as the highest R and R^2 values among all other MFs at different number of epochs. It reached the best fit with the learning process with a correlation of 0.9731, which shows that the predicted values are very close to the ideal linear line and the proposed ANFIS model is well trained.

7 Evaluation of results – Smart home

Smart home has become one of the popular IoT applications that provide new digitized services to improve our quality of life. Providing an efficient and effective access control model is one of the top priorities of a smart home. With the capability of home appliances to connect and communicate together over the Internet, protecting these devices has become an essential priority. This section discusses applying the risk-based access control model with the proposed risk estimation technique using ANFIS on various access control scenarios of the smart home.

Table 7 Performance evaluation of the ANFIS model with the hybrid learning method at 300 epochs

Learning algorithm	MF	Training Error	Testing Error	Performance Evaluation			
				RMSE	MAE	R	R^2
Hybrid	TriMF	5.3392	5.3919	5.3660	4.2282	0.9642	0.9297
	TrapMF	4.6438	4.6552	4.6647	3.5611	0.9731	0.9469
	GbellMF	4.9888	5.0047	5.0127	3.8696	0.9689	0.9387
	GaussMF	5.1389	5.1714	5.1681	4.0091	0.9669	0.9348
	Gauss2MF	4.6611	4.6706	4.6810	3.5720	0.9729	0.9465
	PiMF	4.8294	4.8357	4.8521	3.6985	0.9709	0.9426
	DsigMF	4.6974	4.7069	4.7184	3.5982	0.9725	0.9457
	PsigMF	4.6975	4.7068	4.7184	3.5984	0.9725	0.9457



ANFIS Info.
# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Load data
Type: ○ Training ○ Testing ● Checking ○ Demo
From: ○ file ● worksp.

Generate FIS
○ Load from file
○ Load from worksp.
● Grid partition
○ Sub. clustering

Train FIS
Optim. Method: hybrid
Error Tolerance: 0.05
Epochs: 300

Test FIS
Plot against:
● Training data
○ Testing data
○ Checking data

Epoch 300:error= 4.9888

Fig. 9 Training and testing errors when applying the GbellMF with the hybrid learning method at 300 epochs

7.1 Scenario description

The IoT can connect almost all environment objects over the Internet to share their data and create new applications and services. Using a software application can control smart home appliances to enable or disable them. For example, smart thermostats can be controlled remotely to control the home temperature. This allows the device's owner to control the home's temperature for more comfortable when back home. In addition, food can be cooked while you are on your way home with the capability to control the Oven or Microwave remotely to turn it on or off and control the temperature.

Our main objective is to use these digitized features securely and safely by limiting the access based on the security risk value associated with the access request. Applying the risk-based access control model to a smart home access control scenario needs specifying the four risk factors for each access request of our proposed risk-based model, as illustrated in Fig. 2.

Since there are no available real-world data that can be used, the values of risk factors were assumed based on the literature review [31, 43]. For contextual and real-time attributes (user context), time and location features were utilized. The time refers to the time of accessing a certain IoT smart home device. If the access was done in that specific time duration (for example, 9:00 AM - 5:30 PM) the risk will be high. While if the access was done outside this time, the risk will be low. The selected time interval can be set dynamically using the system owner. The location refers to the location of the requesting user while making the access request to access smart home devices. If the access was made from inside the home, then the risk will be low, while if the access was made from outside the home, the risk will be high.

The value of user context was assumed based on the literature review [31, 43], as shown in Table 8. Three risk levels were used; low, moderate and high to represent all combinations of location and time features. The risk of contextual features will be low if the device owner is accessing the device from inside the home whether within the permitted time or not, as this should be the case in real-life scenarios. Also, the risk will be moderate, if the device owner is

Table 8 The value of user context for smart home access control scenario

Permitted Time	Location (In-Home)	Context Risk level	Risk Percentage	Proposed Risk Value
Yes	Yes	Low	10%	0.1
No	Yes	Moderate	40%	0.4
Yes	No	Moderate	40%	0.4
No	No	High	70%	0.7

accessing the system within the permitted time whether inside or outside the home. While the risk will be high if the access was made outside the permitted time and from outside the home.

For the value of the resource sensitivity, since all smart home appliances are closely related to human life and can be used maliciously, all appliances/ data in this scenario were assumed to be sensitive. So, the risk of resource sensitivity is assumed to be high, and the risk value is assumed to be 0.7. The risk of action severity is assumed to be low, as most actions that are allowed remotely are basic actions such as ON, OFF, Adjust, etc. For the risk history, the same three risk levels used based on the literature (low, moderate, and high) were utilized with the same values of user context that were determined based on the literature review [31, 43].

7.2 Scenario results

The output risk value is used to assess the security risk associated with the access request and can be used to make the access decision. The risk values of this scenario were categorized into three groups, as shown in Table 9.

The system security administrator or owner can utilize these bands to grant or deny access to system resources. For example, if the output risk is low, it grants access. The system administrator or owner has the full flexibility to specify different values for risk categories and specify their output risk band to grant or deny access. After specifying values of the four risk factors of the proposed risk-based model, the output risk value for each scenario was estimated using the proposed ANFIS model, as depicted in Table 10.

Applying the proposed risk-based model to smart home access scenarios demonstrated it can provide several advantages over existing access control models. Using the contextual and real-time features involving time and location demonstrated it can provide dynamic and flexible access decisions. The proposed risk-based model provides expected functionality like existing access control models in which it allows the owners to perform all actions on various devices remotely in a secure manner.

From Table 10, the output risk was low if values of user context and risk history were low or moderate. This is logical and reflects real-life scenarios, in which if the owner is inside the home and requesting to access the device in the permitted time interval, the risk should be low. Also, since one of the main features of smart devices is the ability to access them remotely, the proposed model allows the device's owner to access various

Table 9 Access decision bands for smart home access scenarios

Output Risk Value	Risk Category
0.0–0.3	Low
0.3–0.5	Moderate
0.5–1.0	High

Table 10 Applying the proposed model to access control scenarios of a smart home

Scenario NO#	Context Features	Risk History	Risk Factors				Output Risk Value	Output Risk Category
			User Context	Resource Sensitivity	Action Severity	Risk History		
S1	Low	Low	0.1	0.7	0.1	0.1	0.2415	Low
S2	Low	Moderate	0.1	0.7	0.1	0.4	0.2834	Low
S3	Low	High	0.1	0.7	0.1	0.7	0.3746	Moderate
S4	Moderate	Low	0.4	0.7	0.1	0.1	0.2956	Low
S5	Moderate	Moderate	0.4	0.7	0.1	0.4	0.48223	Moderate
S6	Moderate	High	0.4	0.7	0.1	0.7	0.5451	High
S7	High	Low	0.7	0.7	0.1	0.1	0.5289	High
S8	High	Moderate	0.7	0.7	0.1	0.4	0.5757	High
S9	High	High	0.7	0.7	0.1	0.7	0.6504	High

devices remotely without having low-risk history. On the other hand, the output risk was high if values of user context and risk history were high. This is logical as it reflects the fact that the malicious user with a high-risk history who requested to access the device from outside the home and outside the permitted time interval should not be able to access the device.

8 Verification of results

Validating the proposed risk estimation technique to build the risk-based access control model is essential to show its effectiveness and applicability in smart homes. Hence, the authors investigated the literature review to find a related and validated risk estimation technique to compare the proposed risk estimation against, but without success. There are no available datasets or details about a risk estimation technique for access control operations that utilized real-world scenarios with risk values that can be used to compare the proposed risk estimation technique against. Therefore, the authors went to another alternative, which is the expert interview. One of the most popular ways to validate a model is through an expert review, which is a qualitative approach [16]. The use of expert interviews permits the collection of valid and reliable evidence from well-qualified experts. This can be used to validate the applicability and effectiveness of the proposed risk estimation technique in smart homes.

Several studies advocate the use of expert interviews to collect expert opinions in the absence of datasets. S. Doringer [16] indicated that expert interviews are widely used to explore a specific field of action based on the opinion of highly qualified experts. Also, Morse et al. [34] indicated that expert interviews can be used to effectively verify reliability and validity in qualitative research. Also, Cook and Skinner [14] presented face validity with expert interviews as one of the effective methods to perform credible verification, validation, and accreditation for modelling and simulation.

8.1 Interview design

The expert interview was utilized to validate the effectiveness and applicability of the proposed risk estimation technique to build a risk-based access control model in smart homes by interviewing highly qualified experts who have skills and experiences in IoT security.

The interview started by presenting the research objectives to the interviewee and making sure the interviewee understands the proposed risk-based access control model as well as the proposed risk estimation technique. The interview was designed as a semi-structured, which starts with a set of predetermined open questions that were mainly to collect experts' opinions about the applicability of the proposed risk-based access control model and risk estimation technique for smart homes. Then, the interview was followed by a set of closed-ended questions using a five-point Likert scale to validate and verify the effectiveness of the proposed ANFIS risk estimation in access control scenarios of smart homes that were previously presented in Section 7.2. The interviews were conducted online using the Zoom application and were recorded and/or taking notes manually. All interviews were conducted in the English language. Before starting the interview, each expert was asked to sign a consent form after reading the participant information sheet that included all the necessary information, terms, and conditions about the study.

8.2 Demographic information

In terms of the number of experts, according to Guest et al. [22], there is no agreed-upon number of experts for an interview in a content validity study. However, most researchers recommend a panel consisting of 3 to 15 experts. In expert sampling, participants are chosen based on their knowledge in the area of study [8, 15]. The interviews have conducted with ten IoT security experts from inside and outside the UK. The criteria used to choose experts were years of experience in security and familiarity with IoT applications. The IoT security researchers interviewed in this study were selected after investigating and reading their work and making sure that there is relevancy between their work and this study. While other experts are selected depending on their holding posts that require experience in security and IoT applications. Information on experts who have been involved in this study is shown in Table 11.

8.3 Interviews' results and findings

Ten IoT security experts from inside and outside the UK were interviewed to validate the effectiveness and applicability of the proposed risk estimation technique using the ANFIS model to build a risk-based access control model for smart homes. The interview was divided into two phases. The first phase was mainly to collect experts' opinions about the applicability

Table 11 Attributes of IoT security experts used to validate the proposed technique

Expert No	Job Description	Experience (Years)
E 1	IoT Security researcher	6–10
E 2	Senior Cybersecurity Engineer	More than 10
E 3	IoT Security researcher	6–10
E 4	IoT Security researcher	6–10
E 5	Security Administrator	6–10
E 6	IoT Security researcher	2–5
E 7	Security Administrator	2–5
E 8	IoT Security researcher	6–10
E 9	Security Administrator	More than 10
E 10	Security Administrator	6–10

of the proposed risk-based access control model and risk estimation technique using the ANFIS model for smart homes. This was conducted using four open-ended questions. The second phase of the interview was conducted using a set of closed-ended questions using a five-point Likert scale to validate and verify the effectiveness of the proposed risk estimation technique in various access control scenarios of smart homes.

The first question was about IoT security experts' feedback regarding utilizing the risk-based access control model for smart homes. The majority of experts identified that the proposed risk-based model provides more flexibility and resiliency compared to conventional and traditional access control approaches. They also illustrated that the proposed model can be the basis for more risk-based models that are built using dynamic attributes from the IoT environment. For example, Expert **E2** stated, "Your model is good considering dynamic attributes from smart devices and can be applied to various IoT applications". Expert **E5** also indicated "risk-based model is a very good idea and can be applied in various domains not only smart home, but the major issue will be how to estimate an accurate risk value". Expert **E8** also advocated the idea of utilizing security risk in access control "utilizing security risk in access control is a very good idea and can improve the security". Also, Expert **E9** illustrated that "with more contextual features from the IoT environment, the accuracy of the system will be improved".

For the second question, experts were asked about their opinion regarding using security risk values to make access decisions in IoT applications and the reliability of using security risk values in access decisions. Experts indicated that security risks can be used in access decisions as long as there is enough data to be used to measure the security risk value for each access request accurately. All experts indicated the security risk can be a reliable feature to make the access decision. They added that evaluating these security risks and providing an accurate and realistic risk value is one of the main obstacles to implement the proposed risk-based model especially when there are no available data to determine risk values quantitively for each action and resource. For example, Expert **E1** stated "security risk is a reliable feature for access decisions in IoT applications as long as there is an accurate method to evaluate it". Also, Expert **E5** indicated that "as long as risk probabilities and impact can be identified in each IoT application, the risk can be used to determine access decision". Expert **E6** also indicated that "access permissions can be adjusted based on the risk value, this can reduce malicious activities".

The third question for IoT security experts was "Is the access control scenario provided for smart homes realistic?". Experts indicated that the provided scenario is realistic and reflects the main functionality of smart homes by controlling smart appliances remotely for providing a better quality of life. The majority of experts identified location and time for contextual features as good choices and can be applied to not only smart homes but also to various IoT applications. For example, Expert **E3** stated "no problem with the scenario and using low, moderate and high with time and location features were good". Expert **E10** confirmed that "the scenario is realistic but with real data, the output can be more accurate". Also, Expert **E7** added, "the scenario is realistic but no need to focus on input values itself". While Expert **E5** indicate that "the scenario is good considering time and location only, but more dynamic features should be used as well as the objectives should be more than controlling appliances remotely". Most experts identified that the location and time as dynamic attributes are good, but they also recommended more dynamic features for the next version of the study to provide more flexibility while making the access decision.

For the fourth and last question, experts were asked about the proposed ANFIS model for risk estimation and how it is effective to provide accurate and realistic risk output values. All experts identified that the provided output in smart home access scenarios is realistic and reflects the access permission needed for each scenario. Experts added that the provided ANFIS model is a very good extension of the previous risk estimation technique "fuzzy logic system" utilized at the first stage of this research project. Expert **E4** stated, "ANFIS model is good and will improve their learning over time with more data". Expert **E6** also added, "ANFIS is robust and can provide accurate risk values for smart homes". Expert **E7** also indicated the need to apply the ANFIS model in various IoT applications not only in smart homes.

The second phase of the interview was to evaluate the reliability and applicability of the proposed ANFIS model for risk estimation in smart home access control scenarios by experts. A five-point Likert Scale (strongly agree, agree, neutral, disagree, strongly disagree) was used with each output from the provided access scenarios in Table 11. Experts were asked to rate their acceptance to the output risk value provided by the proposed ANFIS risk estimation technique for each scenario (S1 -S9). Experts were told "Please use the Likert scale to specify how confident you are for the risk output value of each scenario where 5 represents "Strongly Agree", 4 represents "Agree", 3 represents "Neutral", 2 represents "Disagree", and 1 represents "Strongly Disagree".

As the information from closed-ended questions is considered quantitative data, the experts' responses were collected and entered into SPSS software to analyse the data statistically. The One-Sample T-test was used to analyse the results. This test helps in comparing the mean of a population (μ) with a hypothesised value (μ0). The hypothesised mean (μ0) = 3, which indicates Neutral on the five-point Likert-type scales. The hypotheses for testing each risk output for each scenario are as follows:

- **H0**: If the mean rating of the scenario is > = 3, accept the null hypothesis that the output risk for the scenario is correct and realistic.
- **H1**: If the mean rating of the scenario is <3, accept the alternative hypothesis that the output of the scenario is incorrect and unrealistic.

The statistical significant level alpha is $\alpha = 0.05$. The null hypothesis (H0) is rejected if the probability (p value) of each scenario is $> \alpha = 0.05$. The output risk value for each scenario is statistically significant (correct) if the p value <0.05, otherwise, the output risk value is not statistically significant. Table 12 shows the analysis of the experts' responses.

From Table 12, IoT security experts have validated and verified all the output of the proposed ANFIS risk estimation technique and confirmed that it is correct and realistic and can be applied effectively in smart homes. The results show that all the risk output values were correct where the mean value was >3 and the p value was <0.05, so H0 is accepted and H1 is rejected.

The reliability of experts' statements was tested using Cronbach's Alpha Coefficient [13, 45]. If the reliability score is less than 0.6, it is considered poor, moderate if it is around 0.6, good if around 0.7 and excellent at 0.8 or above. Table 13 shows the Cronbach's Alpha test performed using the SPSS software. The overall reliability using Cronbach's alpha coefficient is 0.713, which shows that the results obtained from experts are reliable and internal consistency within experts was good.

Table 12 One sample T-test of expert interviews to validate the output of the proposed ANFIS risk estimation technique

Scenario NO#	Mean	Sig(2-tailed) p value	Result
S1	4.8	<0.001	Statically Significant
S2	4.4	<0.001	Statically Significant
S3	4.2	<0.001	Statically Significant
S4	3.9	<0.001	Statically Significant
S5	4.2	<0.001	Statically Significant
S6	3.6	<0.001	Statically Significant
S7	4.1	<0.001	Statically Significant
S8	4.4	<0.001	Statically Significant
S9	4.7	<0.001	Statically Significant

9 Discussion

Risk estimation is the essential element to implement a risk-based access control model. The availability of a dataset that describes the risk likelihood and impact for a specific scenario can be used to estimate the security risks efficiently and accurately. In this research, there is no available dataset that describes risk likelihood and impacts as well as there is no existing work that contains a dataset to be used to validate our proposed technique. Hence, the authors investigated and implemented the fuzzy logic system by interviewing twenty IoT security experts from inside and outside the UK and the result was published in [4]. Then, the ANFIS model was proposed in this paper to improve the accuracy and efficiency of the fuzzy logic system.

The proposed ANFIS model provides several advantages over the fuzzy logic system. The ANFIS provides a good way to tune the fuzzy logic system with different MFs to select the optimal method that results in increasing the accuracy of the output as well as adding the learning capability to the risk estimation technique to increase accuracy. Figure 10 shows the effect of the training on the shape of the MF. It shows the TrapMF of the action severity and resource sensitivity before and after 20 epochs of training using the hybrid learning method. There are significant modifications have been done to the shapes of MFs through the learning process. In addition, Fig. 11 shows the effect of the training on fuzzy rules and the output risk value in which the output risk was 60 before the training and becomes 55.2 after the training for the same input combinations.

In addition, one of the other improvements that the proposed ANFIS model added over the existing fuzzy logic systems was reducing the processing time needed for estimating the security risk value for each access request, as shown in Table 14. An access control model for the IoT system is intended to serve hundreds or thousands of users. However, the scalability of the fuzzy logic system seems to be doubtful since it requires a non-trivial time to estimate the security risks of access control operations.

Table 13 Reliability Statistics of the proposed ANFIS risk estimation technique

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
0.713	0.719	9

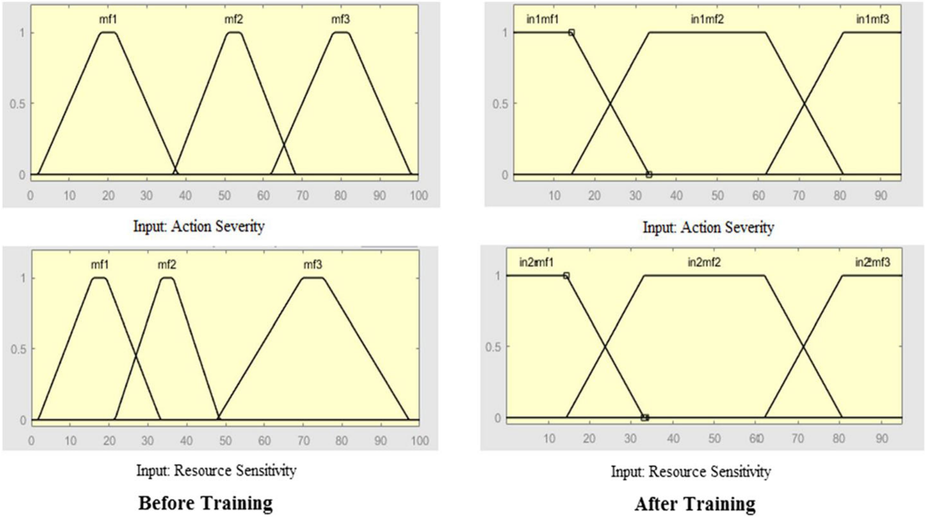
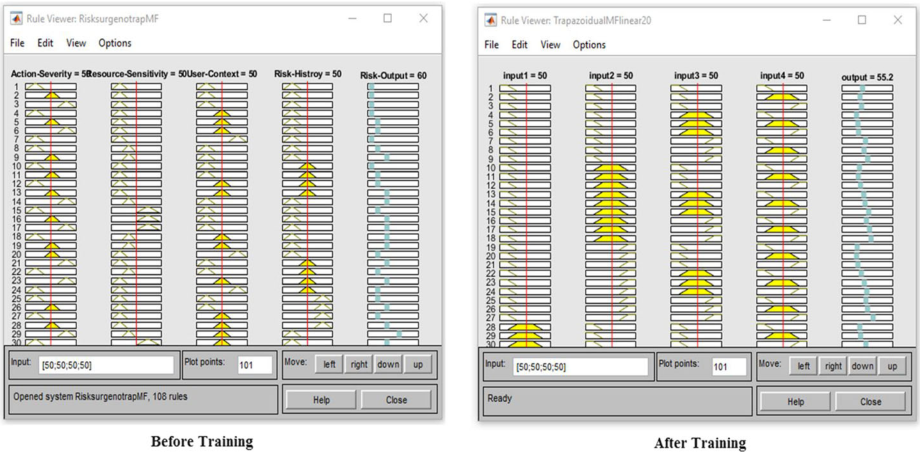


Fig. 10 Shape of fuzzy sets of the TrapMF before and after the training for input risk factors

The fuzzy logic system risk requires 57.385 seconds to estimate the security risks of 1000 access requests (0.0574 Sec per access request). This response time is efficient for a small network of devices, but with the IoT system, there are thousands of devices per network. This number of IoT devices is constantly increasing which requires taking the scalability of the risk estimation technique into account. This is where the proposed ANFIS model comes to play to reduce the processing time from 57.385 to 10.875 sec (0.01088 Sec per access request). The proposed ANFIS model provides a better efficient processing time, which can provide timeliness risk estimation techniques for not only smart homes but also for various IoT applications. Besides this, the learning capability makes the risk estimation technique able to adapt to changes and unpredicted situations in the IoT environment, which will result in more accurate and realistic risk values.


Rule Viewer: RisksurgenotrapMF

Action-Severity = 50 Resource-Sensitivity = 50 User-Context = 50 Risk-Histroy = 50 Risk-Output = 60

Input: [50;50;50;50] Plot points: 101

Opened system RisksurgenotrapMF, 108 rules

Rule Viewer: TrapazoidualMFlinear20

input1 = 50 input2 = 50 input3 = 50 input4 = 50 output = 55.2

Input: [50;50;50;50] Plot points: 101

Ready

Fig. 11 Fuzzy rules of the TrapMF before and after the training

Table 14 Processing time of the proposed ANFIS model with Mamdani FIS

Number of Access Requests	Proposed ANFIS Technique		Mamdani FIS [4]	
	Time (Sec)	Time per Request (Sec)	Time (Sec)	Time per Request (Sec)
1000	10.8750	0.01088	57.385	0.0574
10,000	81.5469	0.00815	572.125	0.0572
20,000	146.5625	0.00733	1140.4	0.05702
30,000	211.4216	0.00705	1713.6	0.05712
40,000	277.6094	0.00694	2286.4	0.05716
50,000	341.7656	0.00684	2860.5	0.05721
60,000	407.1875	0.00679	3436.2	0.05727
70,000	472.1250	0.00674	4012.4	0.05732
80,000	537.2345	0.00672	4588.8	0.05736
90,000	602.2314	0.00669	5166.9	0.05741
100,000	667.1286	0.00667	5746.23	0.05746
150,000	995.4688	0.00664	8625.32	0.0575
200,000	1325.3124	0.00663	11,506.14	0.05753
250,000	1634.8213	0.00654	14,390.1	0.05756

In terms of the limitations of our work, getting real-world data from a running IoT system can improve the efficiency and accuracy of the proposed ANFIS model. Although the proposed ANFIS model was validated and verified by ten IoT security experts who indicated that it provides accurate and realistic risk values for each access request, the availability of real-world data to compare our proposed model against will allow improving the accuracy and utilizing the proposed ANFIS model not only in smart homes but also in various IoT applications.

10 Conclusion

Traditional access control approaches provide a set of advantages, but they also have drawbacks. One of these drawbacks is that it cannot handle unpredicted situations as they are based on static and predefined policies. Dynamic access control models overcome these issues by utilizing not only access policies but also contextual and real-time attributes to make the access decision. One of the dynamic access control models is the risk-based access control model. This model uses the security risk value associated with each access request to decide whether to grant or deny access. One of the essential stages to build a risk-based access control model is to provide an accurate and realistic method to estimate the security risk value associated with each access request. Some researchers suggested the fuzzy logic system to estimate the security risk value, however, it faces issues related to scalability and cannot learn which cannot work with dynamic access control models. Therefore, this paper proposed a novel ANFIS model to estimate the security risk value associated with each access request. The proposed ANFIS model was implemented, and the results demonstrated that it provides an efficient and accurate risk estimation technique that can adapt to the changing conditions of the IoT environment. In addition, ten IoT security experts from inside and outside the UK were interviewed to validate the applicability and effectiveness of the proposed ANFIS technique in smart homes. The results of the interview illustrated that all experts confirmed that the proposed ANFIS model provides accurate and realistic results with a 0.713 in Cronbach's alpha coefficient which indicates that the results are reliable. The proposed ANFIS model provides an efficient processing time in which it reduces the processing time from 57.385 to 10.875 Sec per 1000 access requests. The proposed ANFIS model also adds the learning capability which makes the risk estimation technique able to adapt to changes and unpredicted situations in the IoT environment. The lack of real-world data to compare the proposed ANFIS model against was a limitation to this research to achieve better efficiency and accuracy. For future work, deep learning techniques will be investigated to provide more improvements in terms of accuracy and performance to provide an efficient risk estimation technique that can be used to build an effective risk-based access control model for the IoT system.

Data availability The dataset generated during and/or analysed during the current study is available from the corresponding author on reasonable request.

Declarations

Conflicts of interests/competing interests The authors declare no conflict of interest and this research has not received any external funding.

References

1. Alawad H, An M, Kaewunruen S (2020) "Utilizing an adaptive neuro-fuzzy inference system (ANFIS) for overcrowding level risk assessment in railway stations," Appl Sci (Switzerland), vol. 10, no. 15, https://doi.org/10.3390/app10155156.
2. Alayda S, Almowaysher NA, Humayun M, Jhanjhi NZ (2020) A Novel Hybrid Approach for Access Control in Cloud Computing. Int J Eng Res Technol 13(11):3404–3414. https://doi.org/10.37624/IJERT/13.11.2020.3404-3414
3. Al-Hmouz A, Shen J, Al-Hmouz R, Yan J (2012) Modeling and simulation of an adaptive neuro-fuzzy inference system (ANFIS) for Mobile learning. IEEE Trans Learn Technol 5(3):226–237. https://doi.org/10.1109/TLT.2011.36
4. Atlam HF, Wills GB (2019) An efficient security risk estimation technique for risk-based access control model for IoT. Int Things 6:1–20. https://doi.org/10.1016/J.IOT.2019.100052
5. Atlam HF, Alenezi A, Walters RJ, Wills GB (2017) An overview of risk estimation techniques in risk-based access control for the internet of things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), Porto, Portugal, April 24-26, pp 254–260. https://doi.org/10.5220/0006292602540260
6. Atlam HF, Alenezi A, Walters RJ, Wills GB, Daniel J (2017) "Developing an adaptive Risk-based access control model for the Internet of Things," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 655–661. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.103.
7. Atlam HF, Walters RJ, Wills GB, Daniel J (2018) "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," Mob Netw Appl

8. Bolderston A (2012) Conducting a research interview. J Med Imaging Radiation Sci 43:66–76. https://doi.org/10.1016/j.jmir.2011.12.002
9. Chen P, Pankaj C, Karger PA, Wagner GM, Schuett A (2007) "Fuzzy Multi – Level Security : An Experiment on Quantified Risk – Adaptive Access Control," 2007 IEEE Symposium on Security and Privacy(SP'07), pp. 22–27
10. Chen A, Xing H, She K, Duan G (2016) A dynamic risk-based access control model for cloud computing. In: 2016 IEEE international conferences on big data and cloud computing (BDCloud), social computing and networking (SocialCom), sustainable computing and communications (SustainCom) (BDCloud-SocialCom-SustainCom), Atlanta, Georgia, USA, 8-10 October, pp 579–584. https://doi.org/10.1109/BDCloud-SocialCom-SustainCom.2016.90
11. Cheng T, Wen P, Li Y (2016) "Research Status of Artificial Neural Network and Its Application Assumption in Aviation," in 2016 12th international conference on computational intelligence and security (CIS), pp. 407–410. https://doi.org/10.1109/CIS.2016.0099.
12. Choi D, Kim D, Park S (2015) "A framework for context sensitive risk-based access control in medical information systems," Comput Math Methods Med, 2015, https://doi.org/10.1155/2015/265132.
13. Connolly P (2011) Quantitative data analysis using SPSS, Open University Press
14. Cook DA, Skinner JM (2005) How to Perform Credible Verification , Validation , and Accreditation for Modeling and Simulation. J Defense Softw Eng May:20–24
15. DiCicco-Bloom B, Crabtree BF (2006) The qualitative research interview. Med Educ 40(4):314–321
16. Döringer S (2021) The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. Int J Soc Res Methodol 24(3):265–278
17. Dos Santos DR, Westphall CM, Westphall CB (2014) "A dynamic risk-based access control architecture for cloud computing," IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World pp. 1–9 https://doi.org/10.1109/NOMS.2014.6838319.
18. Dubois D, Yager RR (1992) Fuzzy set connectives as combination of belief structures. Inf Sci 66:245–275
19. Gao P, Xue L, Lu Q, Dong C (2015) Effects of alkali and alkaline earth metals on N-containing species release during rice straw pyrolysis. Energies 8(11):13021–13032. https://doi.org/10.3390/en81112355
20. Ghani MKAbd, Mohammed MA, Ibrahim MS, Mostafa S. A, Ibrahim DA (2017) "Implementing an efficient expert system for services center management by fuzzy logic controller," J Theor Appl Inf Technol, vol. 15, no. 13
21. Ghorbanzadeh O, Rostamzadeh H, Blaschke T, Gholaminia K, Aryal J (2018) A new GIS-based data mining technique using an adaptive neuro-fuzzy inference system (ANFIS) and k-fold cross-validation approach for land subsidence susceptibility mapping. Nat Hazards 94(2):497–517. https://doi.org/10.1007/s11069-018-3449-y
22. Guest G, Bunce A, Johnson L (2006) How many interviews are enough ? An experiment with data saturation and variability. Family Health Int 18(1):23–27
23. Guney K (2008) Concurrent neuro-fuzzy Systems for Resonant Frequency Computation of rectangular, circular, and triangular microstrip antennas. Prog Electromagn Res 84:253–277
24. Haykin S (2004) Neural Networks – A Comprehensive foundation. 2nd Ed., Pearson Education
25. Jang JSR (1993) ANFIS: adaptive-network-based fuzzy inference system. IEEE Trans Syst Man Cybern 23(3):665–685. https://doi.org/10.1109/21.256541
26. Jasleen K, Khan A, Abushark Y, Alam M, Khan S, Agrawal A, Kumar R, Khan R (2020) Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective. Risk Manag Healthcare Policy 13:355–371. https://doi.org/10.2147/RMHP.S233706
27. Khambhammettu H, Boulares S, Adi K, Logrippo L (2013) A framework for risk assessment in access control systems. Comput Secur 39:86–103. https://doi.org/10.1016/j.cose.2013.03.010
28. Kristjanpoller W, Michell K (2018) A stock market risk forecasting model through integration of switching regime, ANFIS and GARCH techniques. Appl Soft Comput J 67:106–116. https://doi.org/10.1016/j.asoc.2018.02.055
29. Lee S, Lee YW, Diep NN, Lee S, Lee Y, Lee H (2007) "Contextual Risk-based access control," Proceedings of the 2007 International Conference on Security & Management, p. pp 406–412
30. Li Y, Sun H, Chen Z, Ren J, Luo H (2008) "Using Trust and Risk in Access Control for Grid Environment," Int Conf Secur Technol (SECTECH '08), pp. 13–16, https://doi.org/10.1109/SecTech.2008.50.
31. Li J, Bai Y, Zaman N (2013) A fuzzy modeling approach for risk-based access control in eHealth cloud. Proceedings - 12th IEEE International Conference on Trust, Secur Privacy Comput Commun Trust Com 2013:17–23. https://doi.org/10.1109/TrustCom.2013.66
32. McGraw R (2009) Risk-adaptable access control (RAdAC): access control and the information sharing problem. Proceedings of NIST & NSA Privilege Management Workshop, pp 1–10
33. Metoui N, Bezzi M, Armando A (2016) Trust and risk-based access control for privacy preserving threat detection systems. In: Hameurlain A, Küng J, Wagner R, Dang T, Thoai N (eds) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI. Lecture Notes in Computer Science(), vol 10720. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-56266-6_1

34. Morse JM, Barrett M, Mayan M, Olson K, Spiers J (2002) Verification strategies for establishing reliability and validity in qualitative research. Int J Qual Methods 1(2):13–22
35. Mostafa SA, Mustapha A, Mohammed MA, Ahmad MS, Mahmoud MA (2018) A fuzzy logic control in adjustable autonomy of a multi-agent system for an automated elderly movement monitoring application. Int J Med Inform 112:173–184. https://doi.org/10.1016/J.IJMEDINF.2018.02.001
36. Ni Q, Bertino E, Lobo J (2010) Risk-based access control systems built on fuzzy inferences. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Ser. ASIACCS 10. Beijing China April 13 - 16, pp 250–260. https://doi.org/10.1145/1755688.1755719
37. Pramanik N, Panda RK (2009) Application of neural network and adaptive neuro-fuzzy inference systems for river flow prediction. Hydrol Sci J 54(2):247–260. https://doi.org/10.1623/hysj.54.2.247
38. Rajabi M, Sadeghizadeh H, Mola-Amini Z, Ahmadyrad N (2019) "Hybrid Adaptive Neuro-Fuzzy Inference System for Diagnosing the Liver Disorders," [Online]. Available: http://arxiv.org/abs/1910.12952
39. Rezaei K, Hosseini R, Mazinani M (2014) A fuzzy inference system for assessment of the severity of the peptic ulcers. In: Proceedings of Fourth International Conference on Soft Computing for Problem Solving, pp 263–271. https://www.airccj.org/CSCP/vol4/csit42227.pdf
40. Saduf, Wani MA (2013) Comparative study of Back propagation learning algorithms for neural networks. Int J Adv Res Comput Sci Softw Eng 3(12):1151–1156
41. Shahzadi S, Khaliq B, Rizwan M, Ahmad F (2020) Security of cloud computing using adaptive neural fuzzy inference system. *Secur Commun Netw* 2020:1–15. https://doi.org/10.1155/2020/5352108
42. Shaikh RA, Adi K, Logrippo L (2012) Dynamic risk-based decision methods for access control systems. Comput Secur 31(4):447–464. https://doi.org/10.1016/j.cose.2012.02.006
43. Sharma M, Bai Y, Chung S, Dai L (2012) "Using risk in access control for cloud-assisted ehealth," High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference, pp. 1047–1052
44. Suparta W, Alhasa KM (2016) "Adaptive Neuro-Fuzzy Interference System," in Modeling of Tropospheric Delays Using ANFIS, pp. 5–19. https://doi.org/10.1007/978-3-319-28437-8_2.
45. Taber KS (2018) The use of Cronbach's alpha when developing and reporting research instruments in science education. Res Sci Educ 48(6):1273–1296. https://doi.org/10.1007/s11165-016-9602-2
46. Tiwari S, Babbar R, Kaur G (2018) Performance evaluation of two ANFIS models for predicting water quality index of river Satluj (India). Adv Civil Eng 2018:1–10. https://doi.org/10.1155/2018/8971079
47. Vieira J, Dias FM, Mota A (2004) Neuro-fuzzy systems: a survey. In: Proceeding of 5th WSEAS NNA International Conference on Neural Networks and Applications, Udine, Italy, March 25 - 27, pp 1–6
48. Wang YM, Elhag TMS (2008) An adaptive neuro-fuzzy inference system for bridge risk assessment. Expert Syst Appl 34(4):3099–3106. https://doi.org/10.1016/j.eswa.2007.06.026
49. Wang Q, Jin H (n.d.) Quantified risk-adaptive access control for patient privacy protection in health information systems. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), Hong Kong, China, March 22-24, pp 406–410. https://doi.org/10.1145/1966913.1966969
50. Wu Y, Zhang B, Lu J, Du K-L (2011) Fuzzy logic and neuro-fuzzy systems: a systematic introduction. Int J Artif Intel Exp Syst 2(2):47–80
51. Xu Q (2013) A novel machine learning strategy based on two-dimensional numerical models in financial engineering. Math Problems Eng 2013:1–6. https://doi.org/10.1155/2013/659809
52. Xu Q, Wu J, Chen Q (2014) "A novel mobile personalized recommended method based on money flow model for stock exchange," Math Problems Eng, 2014, https://doi.org/10.1155/2014/353910.
53. Xu Q, Wang Z, Wang F, Gong Y (Oct. 2019) Multi-feature fusion CNNs for Drosophila embryo of interest detection. Physica A: Stat Mech Appl 531:121808. https://doi.org/10.1016/J.PHYSA.2019.121808
54. Xu Q, Wang F, Gong Y, Wang Z, Zeng K, Li Q, Luo X (2019) A novel edge-oriented framework for saliency detection enhancement. Image Vis Comput 87:1–12. https://doi.org/10.1016/J.IMAVIS.2019.04.002
55. Xu Q, Huang G, Yu M, Guo Y (Feb. 2020) Fall prediction based on key points of human bones. Physica A: Stat Mech Appl 540:123205
56. Yao F, Yerima SY, Kang B, Sezer S (2017) Continuous implicit authentication for mobile devices based on adaptive neuro-fuzzy inference system In: 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), London, UK, June 10 -20, pp 1–7. https://doi.org/10.1109/CyberSecPODS.2017.8074846
57. Zanchettin C, Mimku L, Ludermir TB (2010) Design of Experiments in neuro-fuzzy systems. Int J Comput Intell Appl 09(02):137–152. https://doi.org/10.1142/S1469026810002823

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.