# An Efficient Security Risk Estimation Technique for Risk-based Access Control Model for IoT

Hany F. Atlam*[1, 2], Gary B. Wills[1]
[1]Electronic and Computer Science Department, University of Southampton, Southampton, United Kingdom
[2]Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt
{hfa1g15, gbw}@soton.ac.uk

**Abstract** - The need to increase information sharing in the Internet of Things (IoT) applications made the risk-based access control model to be the best candidate for both academic and commercial organizations. Risk-based access control model carries out a security risk analysis on the access request by using IoT contextual information to provide access decisions dynamically. Unlike current static access control approaches that are based on predefined policies and give the same result in different situations, this model provides the required flexibility to access system resources and works well in unexpected conditions and situations of the IoT system. One of the main issues to implement this model is to determine the appropriate risk estimation technique that is able to generate accurate and realistic risk values for each access request to determine the access decision. Therefore, this paper proposes a risk estimation technique which integrates the fuzzy inference system with expert judgment to assess security risks of access control operations in the IoT system. Twenty IoT security experts from inside and outside the UK were interviewed to validate the proposed risk estimation technique and build the fuzzy inference rules accurately. The proposed risk estimation approach was implemented and simulated using access control scenarios of the network router. In comparison with the existing fuzzy techniques, the proposed technique has demonstrated it produces precise and realistic values in evaluating security risks of access control operations in the IoT context.

**Keywords**: Security risk, Risk estimation, Internet of Things, Risk-based access control model, Fuzzy logic system.

## 1. Introduction

Nowadays, the Internet of Things (IoT) attracts the attention of specialists and researchers in both academia and industry. This is because it can provide unlimited capabilities that can help us in our daily life activities and enhance the quality of our life [1]. The IoT has the ability to

link billions of devices and provide a real-world intelligent platform to collaborate and communicate with these devices through wireless or wired networks [2].

There are enormous benefits for the IoT system, however, it introduces several challenges especially in security and privacy. These issues are difficult to be handled since the IoT is a dynamic and heterogeneous system in nature [3, 4]. One of the main aspects to handle security issues in the IoT is the access control model. This model not only limits access to authorised users but also prevents authorised users from accessing system resources in an unauthorised way [5, 6].

There are two categories of access control approaches; traditional and dynamic. Traditional access control approaches use static and predefined policies to provide the access decision. These policies always give the same result in different situations. Hence, this rigid method cannot provide a reliable solution for IoT systems, which are characterized by changing conditions while determining access decisions [7, 8]. On the other hand, dynamic access control approaches use access policies and real-time information to determine whether granting or denying access. These features involve context, trust, history events, risk, and operational need [9].

Risk-based access control model uses the security risk as a criterion to decide access decisions. It performs a risk analysis to estimate the security risk value related to each access request. The estimated risk value is then compared against access policies to determine the access decision. This model solves the issue regarding the flexibility in accessing system resources. In addition, it provides an efficient solution to many unpredicted situations which need policy violations as policies are incomplete. The need to proliferate information sharing in the IoT system has encouraged risk-based models to grow significantly [10, 11].

Obviously, estimating the security risk related to each access request is the critical phase to implement a risk-based model for the IoT. However, estimating the risk is not an easy task. There are several factors that need to be considered like user's trustworthiness, data sensitivity, users and objects access history, type of access being requested and the location from which access is being requested [12]. Moreover, the understanding and estimation of the security risk are changing based on the application context or culture of organisations.

Specifying the optimal risk estimation technique to assess security risks of access control operations in IoT systems is not an easy task, there are many issues that may arise. For example, the core drive of the risk estimation process is to expect the future likelihood of information disclosure that is corresponded to the current access. Identifying this likelihood in the absence of data is a difficult task [3]. Furthermore, if the risk estimation process has based on imprecise

or incomplete data about related risk factors, this will make defining the value of information very difficult [13]. In addition, the IoT system requires a flexible and scalable risk estimation technique that can adapt to growing numbers and changing conditions during making access decisions.

This paper proposes a risk estimation technique which is based on integrating the fuzzy logic system with expert judgment to assess security risks of access control operations in the IoT system. The proposed risk estimation approach has been validated by Twenty IoT security experts from inside and outside the UK. Also, IoT security experts were used to create fuzzy rules of the fuzzy model. The proposed technique has implemented and simulated with access control scenarios of the network router. Simulation results have proved that the proposed risk estimation technique can produce precise, correct and realistic results in evaluating security risks of access control operations. Also, the proposed technique has compared against existing risk estimation techniques which utilized the fuzzy logic system in implementing their risk-based models.

This paper provides a novel approach to assess security risks of access control operations in the IoT system by integrating knowledge and expertise of IoT security experts with the fuzzy inference system to make the access decision for each access request. In comparison with existing risk estimation techniques, as far as the authors aware, there is no published work used real-time and contextual features with security risks to make the access decision in IoT applications. Our proposed approach utilizes real-time and contextual attributes associated with the user/agent at the time of making the access request to estimate the risk value associated with the requesting user to determine the access decision. In addition, in contrast to existing fuzzy risk estimation techniques which do not provide a comprehensive discussion about how the security risk is estimated quantitively and how their fuzzy rules were built, our proposed technique provides a detailed discussion of how different parameters of the fuzzy logic system are defined and how the security risk is estimated. Also, our proposed technique adds more robustness, validity and accuracy than existing fuzzy risk estimation techniques by defining different parameters of the fuzzy logic system using knowledge and expertise of twenty IoT security.

The contribution of this paper can be summarized as follows:

- Proposing the fuzzy logic system with expert judgment to be the appropriate risk estimation approach to implement the risk-based model for the IoT system.
- Validating the proposed risk estimation approach and creating fuzzy inference rules

by interviewing Twenty IoT security experts.

- Implementing the proposed risk estimation approach using MATLAB fuzzy logic toolbox.
- Providing simulation results of the proposed risk estimation technique by using access control scenarios of the network router.
- Comparing the proposed risk estimation approach with existing fuzzy-based techniques.

The remainder of this paper is structured as follows; Section 2 examines related risk-based models, Section 3 introduces risk-based model and its main elements; Section 4 presents the proposed risk estimation technique; Section 5 discusses the research methodology; Section 6 discusses the results and findings of experts' interviews; Section 7 introduces the implementation of the proposed risk estimation approach; Section 8 discusses simulation results; and finally, Section 9 is the discussion and conclusion.

# 2. Related Work

The essential element to implement a risk-based model is to identify the appropriate risk estimation technique for evaluating risk values to determine access decisions. Many studies have proposed various approaches to evaluate the risk. Risk assessment attracted many researchers to implement the risk estimation process. For instance, Diep et al. [11] have introduced a method that uses the risk assessment to assess security risks of access control operations using outcomes of actions to measure the risk value regarding each access request. This is followed by comparing the estimated risk with the system acceptable risk value to decide access decisions. However, the paper does not explain how to measure risk values quantitatively. Also, this approach cannot provide the flexibility needed in the IoT system and does not use contextual information to determine access.

In addition, Khambhammettu et al. [14] have suggested three different approaches to estimate security risks of access control operations using the risk assessment. These approaches use the subject trustworthiness, object sensitivity, and difference between them to estimate the risk value. However, this model does not explain any information about how to evaluate risk values in different situations quantitatively. Further, a security system administrator is needed to associate a sensible numeric value for each input combination at the beginning of the risk assessment, and it does not involve real-time and contextual information to determine access.

Also, Shaikh et al. [9] proposed a dynamic risk-based decision approach using the risk

assessment. This approach uses user previous actions to distinguish between good and malicious users. After transaction completion, it assigns reward and penalty points to users to determine access decisions. However, building a risk-based model using reward and penalty points are not enough to determine precise access decisions efficiently.

Some researchers suggested the fuzzy inference system to measure the risk especially with the lack of appropriate data to characterize risk probability and its impact. For example, Chen et al. [7] have utilized the fuzzy logic approach to design a fuzzy multi-level security model to provide access decisions. This model measures the risk related to the access request using the difference between object and subject security levels. So, if the difference was large, the risk value will be high. The resultant output risk is represented as a binary number where 0 permits the access and 1 denies the access. However, the paper does not explain how to estimate the risk quantitively. Also, it does not provide any information about fuzzy rules and how they built it. In addition, their model lacked dynamic and real-time features to determine access.

In addition, Ni et al. [13] have presented a fuzzy inference approach to evaluate security risks of access operations. This approach uses subject and object security levels to measure the risk value. However, the proposed approach faces many challenges regarding the scalability as it requires a long time to estimate the security risk value especially with the increasing number of input parameters and fuzzy rules. Moreover, as the access model may require providing access to thousands of users especially in the growing IoT technology, this model might be too computationally expensive. Also, the paper does not provide any information about fuzzy rules and how they built it. In addition, the proposed approach does not involve contextual information to make the access decision.

Li et al. [15] 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. These values are then converted into fuzzy values to specify the proper access management in a cloud environment. However, the paper does 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.

In the same way, Arias-Cabarcos et al [16] have presented a risk estimation approach to support dynamic identity federations in the Cloud computing environment. Their method is based on proposing a group of risk metrics and uses the fuzzy inference system to estimate the risk. However, there is a difficulty to predefine risk metric for various situations of the environment. It also, lacked real-time features while making the access decision.

Some researchers suggested using game theory to measure the risk value of access operations. For example, Rajbhandari and Snekkenes [17] have proposed a risk analysis method that uses values of user benefits to evaluating the risk value related to the access request using game theory. However, using only the user's benefits to make access decisions are not enough to build a scalable and flexible approach for the IoT. In addition, it does not use contextual information to determine access.

Other researchers have suggested mathematical functions to formulate an algorithm to measure security risks of access operations. For example, Sharma et al. [18] suggested a task-based model to estimate the security risk using user actions by building a mathematical function. This is followed by matching the estimated risk value with system acceptable risk values to determine access. However, the paper does not provide information about how to evaluate the quantitative values of the risk. In addition, it requires prior knowledge about outcomes of environmental situations and it lacked real-time contextual features.

# 3. Risk-based Access Control

Access control is used to limit the permissions of users who have been authenticated successfully. It controls access to ensure that only authorised users granted the proper permissions to maintain confidentiality and integrity for the system resources [11].

The risk is defined as the possible damage that may arise from the existing operation or from some upcoming incident [19]. The risk can be found in many aspects of our lives and used in various disciplines. The security risk in the access control context can be defined as, the likelihood of information leakage and resulted in damage that may occur from access to the system [4].

Risk-based access control model uses the security risk to permit or deny access requests. Although this risk model is still in its first stage of approval, there is an increasing demand to specify essential models and procedures for it [7]. A risk-based model has many advantages. For instance, it provides more flexibility in accessing system resources by using real-time and contextual information collected while making the access request to decide whether granting or denying access. In addition, it takes into consideration the exceptional access requests that are necessary for medical and military applications in which providing the access can save lives [4, 19]. Indeed, it provides an efficient solution to unexpected situations which require policy violations, as policies are incomplete.

There are a variety of methods to build a risk-based model. These methods have some common characteristics. Figure 1 shows the main elements and process flow of a risk-based

model. The user attempts to access system resources by sending an access request to the access control manager. The access request is then processed, and the risk estimation module uses available information about risk features to measure the risk value related to the access request. This is followed by comparing the estimated risk value against risk policies which are specified by the security system administrators. If the estimated risk value is lower than the threshold value defined in risk policies, the access is granted, and the obligation will be applied, otherwise, the access will be denied [20, 21].

There are different ways to evaluate security risks. However, the purpose of the risk estimation process is to define a method to arrange risks according to their priorities and assign a numeric value to the risk to provide the access decision in accordance with a specific context [22]. There are two categories of risk estimation techniques; qualitative and quantitative. Quantitative risk estimation approaches are concerned with attaching specific numerical values to risks, while qualitative risk estimation approaches estimate the risk early in the system in linguistic forms such as low, moderate and high [23].

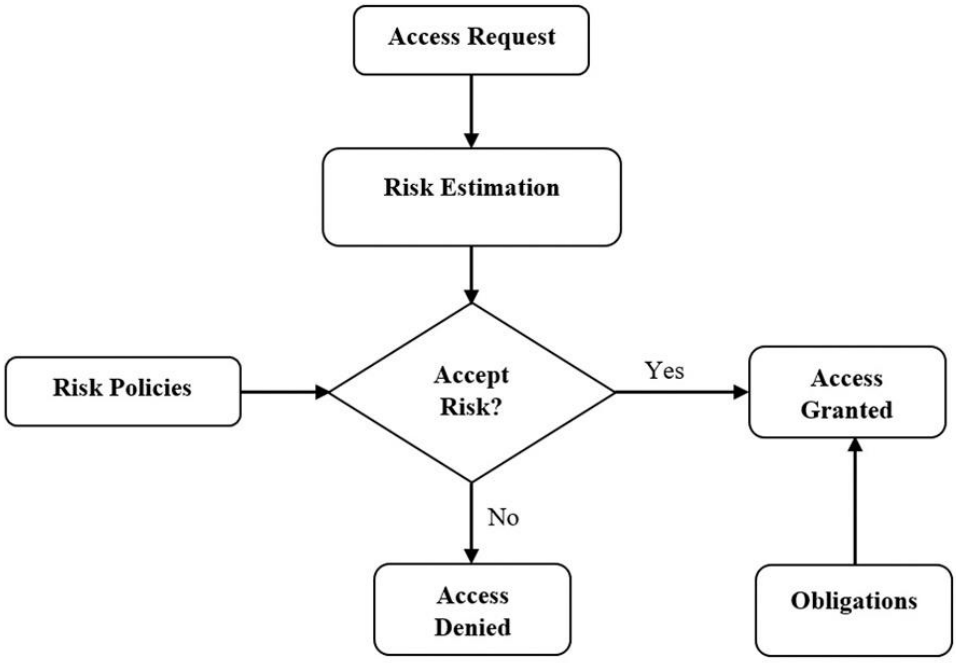


**Figure 1**. Flow process of a risk-based model

# 4. Proposed Risk Estimation Technique

The IoT system connects billions of heterogeneous devices in a dynamic way, therefore, existing access approaches, which are based on static policies and produce the same result in different situations, cannot provide the required security level for various IoT applications. While dynamic access approaches use policies and real-time features to determine the access

decision. One of the dynamic features is the security risk which is the building block of based access control model.

We proposed a Risk-Based Access Control model for the IoT. This model uses user attributes related to the surrounding environment such as time and location, sensitivity of data to be accessed by the user, severity of actions that will be performed by the user and user risk history as inputs for the risk estimation algorithm to measure the risk value related to each access request to determine the access decision, as shown in Figure 2. In addition, the proposed model provides an efficient solution for many unexpected circumstances which need policy violations by incorporating real-time information to determine the access [24, 25].

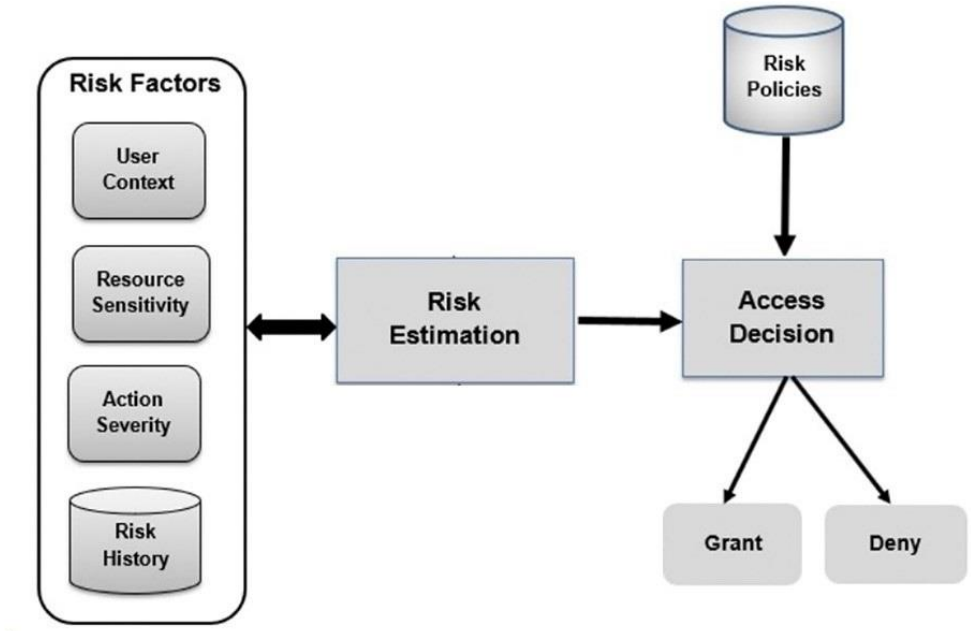


**Figure 2**. Proposed risk-based model

Risk estimation module is the essential part of the risk-based model. It is responsible for evaluating security risks of access control operations in various situations of the IoT environment. It uses input risk factors to measure the risk value regarding each access request. Estimating the security risk is a complex operation which needs considering several factors [14]. Therefore, the target of this paper is to present an appropriate and efficient risk estimation technique to implement the proposed risk-based model.

There is no universal and best method for conducting a risk analysis. However, it is critical to specify the strengths and weaknesses of various approaches to decide the most appropriate regarding a specific context [26, 27]. We propose the fuzzy logic system with expert judgment as to be the suitable risk estimation technique for implementing the proposed risk-based model for the IoT, as shown in Figure 3. Integrating the fuzzy inference system with expert judgment

can provide consistent and realistic risk values. The fuzzy logic system simplifies complex risk management systems which need a suitable quantitative probability model by using either available datasets or expert judgment to assess security risks in a consistent way. In the absence of a dataset to represent risk likelihoods and its impact of various risk factors in various situations of the environment, IoT security domain experts can be used to provide predicted measures according to their knowledge and expertise.


**Figure 3**. Proposed Risk Estimation Technique

There are many reasons to consider the fuzzy logic system with expert judgment for the risk estimation process. Firstly, there are significant sources of subjective knowledge to provide all required information to evaluate security risks regarding access control operations [26]. One of the main sources is past experience. Security administrators generally have some security skills regarding different risk factors and suitable rules and policies regarding each context. This type of subjective knowledge can be converted easily into rules for a fuzzy inference system. Secondly, one of the major problems in any research especially in security is the lack of data. To correctly estimate the risk associated with a specific situation, the data describing situation probability and its impact are required. Once data are available, they can be used to estimate a more precise risk value. Using the fuzzy logic system with expert judgment, there is no need for dataset since the required data will be provided by domain security experts. Expert judgment is a significant source of information in risk-based decision-making operations. This is because correct numerical data describing incident frequencies and its impact do not exist in most risk models [27]. In some cases, quantifying the value of the risk using classical approaches is very complicated, but with expert judgment, an accurate value for a certain situation can be defined especially when appropriate experts are selected [28]. Thirdly, the fuzzy logic system is flexible [29], so, it will be suitable for the IoT system to adapt to its

changing conditions and situations. Fourthly, although expert judgement adds more subjectivity to the risk estimation process, with the fuzzy logic system, the subjectivity can be reduced to an acceptable level, since subjectivity is moved to the process of creating rules which can be better controlled. Certainly, subjectivity is not completely eliminated. However, it is unlikely that a method with no subjectivity will ever exist for a risk analysis [30]. Finally, there are many successful applications that used the fuzzy logic system such as decision support, engineering, psychology, medicine, and home appliances [32, 33].

# 5. Research Methodology

Typically, there are two research methodologies to conduct research; qualitative and quantitative. Quantitative research methodology depends on measuring and analysing data to determine the relationships between one set of data with another to explain a certain phenomenon. The measurement of these variables might produce quantifiable conclusions. Thus, it places emphasis on methodology, procedure and statistical measures of validity [33]. Qualitative research methodology is only concerned with identifying the meaning and understanding of a phenomenon. It is not concerned with the quantification of the phenomenon but providing an understanding of the phenomenon through observation [33–35].

For our research, pure quantitative models require accurate numerical information about the system structure and its initial state that is represented quantitatively, when such data is unavailable, quantitative models face many constraints that restrict the successful implementation of this model. In other words, the main target of the risk estimation technique in the context of access control in the IoT system is to provide a quantitative and numeric value for the risk. This value is then used to determine the access decision whether granting or denying the access. However, the lack of the appropriate dataset to describe risk probabilities and impacts for a set of specified incidents stands as a barrier to having a quantitative method to achieve the research goal. To overcome this problem and provides the suitable risk estimation technique, different risk estimation techniques were reviewed, and we have selected the fuzzy logic system to implement the risk estimation process of the risk-based access control model.

The fuzzy logic system extends the quantitative analysis to include other elements from the qualitative analysis. The effectiveness of this approach appears in situations where elements of the quantitative assessment are available not in numerical forms but in linguistic expressions. In other words, the fuzzy logic system is capable of converting linguistic expressions describing risk factors into quantified values to be used to provide the access decision.

The fuzzy logic system has several variables including the number of linguistic expressions for each input and output, defining the appropriate membership function, building the accurate fuzzy rules and defining the best defuzzification method. These variables need to be defined accurately to get a precise output. Defining these variables can be done by using either trial and error method or through domain experts. However, the trial and error method requires a predetermined dataset of a group of incidents with their risk probabilities and impacts to determine these variables which are not available in our research. Therefore, we decided to use the knowledge and expertise of IoT security experts to define fuzzy parameters and build the proposed fuzzy technique to estimate security risks of access control operations in the IoT system. The expert interview is one of the popular methods of qualitative analysis. It provides a powerful tool to gain an understanding of underlying reasons, opinions and motivations of the research. It does not use statistical measures or other means of quantification [36].

In terms of the number of experts who are required to interview in a research study. According to Guest et al. [37], 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 [38]. For our research, the interviews have conducted with twenty IoT security experts from inside and outside the UK. The criteria used to choose experts was 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 works and making sure that there is relevancy between their work and this study. While other experts are selected depending on their holding positions that require experience in security and IoT applications. In addition, experts are selected after making sure they have the required knowledge about the fuzzy logic system. Although we believed that such knowledge will not affect building the fuzzy rules, as it is human reasoning using English expressions which are easier to understand. However, specifying other fuzzy variables such as the number of fuzzy sets for each input, range of each fuzzy set, membership function and defuzzification method, require extensive knowledge about the fuzzy logic system to specify the precise and accurate fuzzy variables. In addition, most experts had large experiences in security and IoT applications. The attributes of IoT security experts who have involved in this study can be shown in Table 1.

The expert interview was carried out in two phases in which the first phase has utilized to validate the proposed risk estimation technique and define the required parameters to build the fuzzy logic system. The second phase has utilized to build fuzzy inference rules. The first phase was designed as a semi-structured, which starts with a set of predefined open questions with other questions emerging from the dialogue during the interview, by either the interviewer or

interviewee [39]. While the second phase of the interview was designed as a structured containing a set of closed questions to build fuzzy rules of the proposed risk estimation technique. The interview questions were pilot-tested by seven security research fellows at the University of Southampton. 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 of the study. The University of Southampton Ethics Committee granted approval for this study under their reference number 25091.

**Table 1.** 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 | More than 10 |
| E 4 | IoT Security researcher | 6 – 10 |
| E 5 | Security Administrator | 2 – 5 |
| E 6 | IoT Security researcher | 2 – 5 |
| E 7 | Risk analysis professors | 2 – 5 |
| E 8 | IoT Security researcher | 2 – 5 |
| E 9 | Security Administrator | 2 – 5 |
| E 10 | Senior Cybersecurity Engineer | 2 – 5 |
| E 11 | Security Specialist | 6 – 10 |
| E 12 | Security Administrator | 6 – 10 |
| E 13 | Security Specialist | 6 – 10 |
| E 14 | IoT Security researcher | 2 – 5 |
| E 15 | Security Specialist | 2 – 5 |
| E 16 | Security Administrator | 2 – 5 |
| E 17 | IoT Security researcher | 2 – 5 |
| E 18 | Security Administrator | 6 – 10 |
| E 19 | Security Administrator | 6 – 10 |
| E 20 | IoT Security researcher | 2 – 5 |

# 6. Results and Findings of Interviews

Validating the proposed risk estimation approach is essential to ensure its accuracy and acceptance. One of the most popular ways to validate a proposed technique is an expert review [40]. The use of the expert interviews allows collecting valid and reliable data that is related to the research to refine it in the light of opinions of well-qualified experts. The interview was divided into two phases. The first phase was to validate the proposed risk-model and proposed risk estimation technique using IoT security experts. Before asking the interview questions, each expert was given a brief background about the aim of the research, then nine open-ended questions were asked to the experts.

The first question was about their feedback about the proposed risk-based access control model in general. Most experts have interested in the model from the first moment I explained it to them. They have confirmed that it will be valuable to industry and advised trying to contact with interested companies to get more support to complete the research. Majority of experts decided that identifying the appropriate risk estimation approach is the essential and difficult stage to implement the proposed model.

For the second question, experts were asked about proposed risk factors in the proposed model and their suggestion if they are appropriate to different IoT applications. Experts have suggested that the appropriate risk factors depend on the application domain. In other words, they suggested starting to work with one specific IoT application and try to identify different risk factors that are associated with this IoT application besides the proposed four risk factors. We believe that one of the powerful points of the proposed model is that it can be adjusted to different IoT application easily using the four risk factors. Therefore, we prefer to work only with these risk factors at this stage of the research.

The third question was about their opinion regarding which is more appropriate for making access decisions qualitative or quantitative risk estimation techniques. Some experts have suggested that there is no right or wrong answer for it, it depends on the application where the proposed technique will be applied for. While other experts have suggested that the quantitative will be more appropriate for access control operations as it requires a specific value for the risk to use it to make the access decision whether granting or denying the access.

Regarding the fourth question, experts were asked about their feedback about the proposed risk estimation technique. Most experts have interested in it and they have confirmed that it will be a challenge to provide accurate and precise risk estimation especially for rare incidents that are not predicted while implementing the current approach.

In the fifth question, experts were asked about the issues they saw in the proposed technique that need to be addressed. Majority of experts have said that the subjectivity is the most difficult issue in the proposed approach. They have advised trying to reduce the subjectivity associated with the proposed approach by increasing the number of interviewed experts and choose different experts with different skills to get the required information that builds an accurate model. Most experts considered the fuzzy logic approach is the appropriate technique especially when there is no available data to estimate the risk. In addition, some experts suggested using one of the machine learning techniques to estimate security risks in the model. They advised to choose one specific IoT application and find the related dataset and use the artificial neural network to get high performance, but this only applies when there is available

data.

Finally, experts were asked four questions to define various parameters required to build the fuzzy model of the proposed risk estimation technique. They were asked to provide information regarding the number of fuzzy sets for each risk factor, the appropriate range of each fuzzy set, the appropriate membership function to represent the relation between input risk factors and output risk, and the appropriate defuzzification method.

Specifying the number of fuzzy sets and range of each fuzzy set may not require extensive knowledge about the fuzzy logic system but deciding the appropriate membership function and defuzzification method need to have such knowledge. Even with this knowledge, deciding the appropriate membership function and defuzzification method without having a dataset will be difficult. The best way to specify the appropriate membership function and defuzzification method are through trial and error method. However, applying the trial and error method requires having a dataset of correct and precise output of a set of input combinations or incidents describing the risk probabilities and impacts, so we can, for example, compare the defuzzified output of each defuzzification method with the desired output, so we can determine the best defuzzification method for the proposed risk estimation technique. We took this issue into our considerations while building interview questions. The researcher has told experts that most related studies regarding the fuzzy logic system have suggested using either Triangular MF or Trapezoidal MF when there is no available dataset and experts are asked to decide the appropriate MF either by choosing one from what suggested by the researcher or by suggesting another one using their experience in such context. The same scenario was for selecting the appropriate defuzzification method. The researcher has told experts that most related studies regarding fuzzy logic system have suggested using centroid or mean of maximum method and the experts are asked to decide the appropriate defuzzification method either by choosing one from what suggested by the researcher or by suggesting another one defuzzification method using their experience in such situations. Experts' responses to define various fuzzy parameters are summarized in Table 2.

**Table 2.** Experts responses regarding fuzzy parameters required to implement the proposed risk estimation technique

| Expert No | Experts Responses | | | |
|---|---|---|---|---|
| | Number of fuzzy sets | Range of each fuzzy set | Membership function | Defuzzification method |
| E1 | Three fuzzy sets; low, medium, and high. | Low range 0.0 – 0.3, medium range 0.2 – 0.8, and high range 0.6 -1.0 | Trapezoidal MF | Centroid method. |
| E2 | Three fuzzy sets; low, moderate, and high | Low range 0.0 – 0.2, moderate can be 0.15 – 0.7, and high can be 0.6 -1.0 | Triangular MF | Centroid method |
| E3 | Three fuzzy sets; low, moderate, and high. | Low range 0.0 – 0.35, moderate range 0.2 – 0.75, and high range 0.6 - 1.0 | Triangular MF | Centroid method |
| E4 | Three fuzzy sets; low, moderate, and high | Low range 0.0 – 0.25, moderate range 0.2 – 0.65, and high range 0.6 - 1.0 | Sigmoid MF | Centroid method |
| E5 | Four fuzzy sets; very low, low, moderate, and high | Very low range 0.0 – 0.15, Low range 0.1 – 0.35, moderate range 0.2 – 0.7, high range 0.6 – 0.1 | Triangular MF | Do not know |
| E6 | Three fuzzy sets; low, moderate, and high | Low range 0.0 – 0.3, moderate range 0.2 – 0.6, and high range 0.5 -1.0 | Do not know | Do not know |
| E7 | Five fuzzy sets; negligible, low, moderate, high, and unacceptable high | Negligible range 0.0 – 0.15, Low range 0.1 – 0.3, moderate range 0.2 – 0.5, high range 0.4 – 0.8, and unacceptable range 0.7 -1.0 | Triangular MF | Centroid method |
| E8 | Two fuzzy sets; low and high | Low range 0.0 – 0.5, and high range 0.4 – 1.0 | Trapezoidal MF | Mean of Maximum |
| E9 | Four fuzzy sets; low, moderate, high, and unacceptable high | Low range 0.0 – 0.2, moderate range 0.15 – 0.5, high range 0.4 -0.8, and unacceptable high range 0.7 -1.0 | Triangular MF | Centroid method |
| E10 | Three fuzzy sets; low, medium, and high. | Low range 0.0 – 0.25, medium range 0.2 – 0.75, and high range 0.6 -1.0 | Trapezoidal MF | Centroid method |
| E11 | Three fuzzy sets; low, moderate, and high. | Low range 0.0 – 0.3, moderate range 0.2 – 0.75, and high range 0.6 -1.0 | Triangular MF | Centroid method |
| E12 | Four fuzzy sets; negligible, low, moderate, and high | Negligible range 0.0 – 0.15, Low range 0.1 – 0.3, moderate range 0.2 – 0.7, and high range 0.6 – 0.1 | Trapezoidal MF | Bisector method |
| E13 | Four fuzzy sets; low, moderate, high, and unacceptable high | Low range 0.0 – 0.3, moderate range 0.2 – 0.5, high range 0.4 -0.8, and unacceptable high range 0.7 -1.0 | Triangular MF | Centroid method |
| E14 | Three fuzzy sets; low, moderate, and high | Low range 0.0 – 0.3, moderate range 0.2 – 0.7, and high range 0.6 -1.0 | Triangular MF | Centroid method |
| E15 | Four fuzzy sets; low, moderate, high, and unacceptable high | Low range 0.0 – 0.3, moderate range 0.2 – 0.4, high range 0.35 -0.7, and unacceptable high range 0.6 -1.0 | Trapezoidal MF | Centroid method |
| E16 | Three fuzzy sets; low, medium, and high. | Low range 0.0 – 0.25, medium range 0.2 – 0.75, and high range 0.6 -1.0 | Trapezoidal MF | Centroid method |
| E17 | Three fuzzy sets; low, moderate, and high. | Low range 0.0 – 0.35, moderate range 0.3 – 0.75, and high range 0.6 - 1.0 | Triangular MF | Centroid method |
| E18 | Three fuzzy sets; low, moderate, and high. | Low range 0.0 – 0.25, medium range 0.2 – 0.65, and high range 0.6 -1.0 | Triangular MF | Centroid method |
| E19 | Three fuzzy sets; low, | Low range 0.0 – 0.3, moderate range | Triangular MF | Centroid method |

| | | | | |
|---|---|---|---|---|
| | moderate, and high. | 0.2 – 0.75, and high range 0.6 -1.0 | | |
| E20 | Three fuzzy sets; low, moderate, and high. | Low range 0.0 – 0.25, medium range 0.2 – 0.7, and high range 0.6 -1.0 | Trapezoidal MF | Centroid method |

Experts have provided useful information regarding parameters needed to implement the proposed risk estimation technique. It is unsurprised that most experts' responses were different. Regarding the appropriate number of fuzzy sets for the proposed risk factors (user context, action severity, resource sensitivity, and risk history), most of the experts have decided that three fuzzy sets will be enough to represent different states of each risk factor, those experts represent about 65% of all experts. While Five experts have decided that four fuzzy sets are the appropriate number of fuzzy sets for all proposed risk factors, whereas one expert has decided to represent risk factors with two fuzzy set and another expert has decided to use five fuzzy sets. The Distribution of experts' responses to decide the number of fuzzy sets can be shown in Table 3.

**Table 3**. Distribution of experts' responses to decide the number of fuzzy sets

| Number of fuzzy sets | Number of experts | Percentage % |
|---|---|---|
| Two fuzzy sets | 1 | 5% |
| Three fuzzy sets | 13 | 65% |
| Four fuzzy sets | 5 | 25% |
| Five fuzzy sets | 1 | 5% |

Based on the experts' responses, we decided to use three fuzzy sets to represent each risk factor. The user context, action severity, and risk history are represented by "Low", "Moderate" and "High" fuzzy sets. The resource sensitivity is represented by "Not Sensitive", "Sensitive" and "Highly Sensitive" fuzzy sets. While the output risk is represented by using five fuzzy sets; "Negligible", "Low", "Moderate", "High" and "Unacceptable High".

Based on the suggestions provided by the researcher to specify the appropriate membership function to represent the relation between input risk factors and output risk, about 58% of experts have validated triangular MF as to be the most appropriate when there is no dataset to describes the relationship between input and output, while about 37% of experts have validated that trapezoidal MF should be used to represent the shape of input-output data. On the other hand, Expert #4 suggested using sigmoid MF as the appropriate membership function, while Expert #6 preferred not to answer this question. Similarly, based on suggestions provided by the researcher to specify the appropriate defuzzification method, the majority of experts have validated the centroid method to be the appropriate defuzzification method. Only Expert #8 has validated using the mean of maximum as the appropriate defuzzification method, while Expert #12 has suggested using the Bisector method to be the appropriate defuzzification method. Two

experts (Expert #5 and Expert #6) preferred not to answer this question. Distribution of experts' responses to decide the appropriate membership function and defuzzification method is shown in Table 4.

**Table 4**. Distribution of experts' responses to decide appropriate membership function and defuzzification method

| Membership function | Number of experts | Percentage | Defuzzification method | Number of experts | Percentage |
|---|---|---|---|---|---|
| Trapezoidal MF | 7 | 35% | Centroid | 16 | 80% |
| Triangular MF | 11 | 55% | Bisector | 1 | 5% |
| Sigmoid MF | 1 | 5% | MOM | 1 | 5% |
| No Response | 1 | 5% | No Response | 2 | 10% |

For the range of each fuzzy set, there were different suggestions from experts. After analyzing these suggestions, we decided to use ranges indicated in Table 5, which represent various fuzzy sets of each risk factor with its notations with the output risk.

**Table 5.** Input and output linguistic variables and their range

| Linguistic Expression | Notation | Range |
|---|---|---|
| Risk factor: User Context (UC) | | |
| Low | L | 0.0 – 0.4 |
| Moderate | M | 0.3 – 0.7 |
| High | H | 0.6 –1.0 |
| Input variable: Resource Sensitivity (RS) | | |
| Not Sensitive | NS | 0.0 – 0.35 |
| Sensitive | S | 0.2 – 0.5 |
| Highly Sensitive | HS | 0.45 – 1.0 |
| Input variable: Action Severity (AS) | | |
| Low | L | 0.0 – 0.4 |
| Moderate | M | 0.35 – 0.7 |
| High | H | 0.6 – 1.0 |
| Input variable: Risk History (RH) | | |
| Low | L | 0.0 – 0.4 |
| Moderate | M | 0.3 – 0.7 |
| High | H | 0.6 – 1.0 |
| Output variable: Risk | | |
| Negligible | N | 0.0 – 0.3 |
| Low | L | 0.1 – 0.4 |
| Moderate | M | 0.2 – 0.6 |
| High | H | 0.4 – 0.8 |
| Unacceptable High | UH | 0.7 – 1.0 |

The second phase of the interview was to build fuzzy rules. The fuzzy rules are the knowledge base used by the fuzzy model to produce the output where incorrect fuzzy rules can lead to incorrect output. One of the problems associated with fuzzy logic models is the lack of appropriate data to create appropriate and correct fuzzy rules. If a dataset is available, fuzzy rules can be built dynamically and efficiently. In this research, there is no dataset so there is no

way to ensure appropriate fuzzy rules were created. Therefore, IoT security experts were interviewed to build the fuzzy rules after validating the proposed technique and determining the number of fuzzy sets for risk factors of the proposed risk-model.

Since the proposed model has four risk factors, each will be represented using three fuzzy sets, the total number of fuzzy rules will be 3*3*3*3=81 rules. Various combinations of the fuzzy rules were built and twenty IoT security experts were asked to categorize each rule combination with one of the outputs fuzzy sets (Negligible, Low, Moderate, High and Unacceptable High), and their responses are recorded and analysed.

The mean function was used to determine the final decision regarding the output of each rule. The mean also called the average, is the most common function used to measure the spread of values in statistics. The mean function was used to ensure that all responses of experts will be considered [41].

To use expert's responses in SPSS software, expert's responses have given ratings in which Negligible =1, Low=2, Moderate=3, High=4, and Unacceptable High=5. Therefore, the output of each fuzzy rule mapped to one of these five categories. An assumption was made in which any mean value lower than 0.5 will be mapped to the lower category and any mean value higher than or equal to 0.5 will be mapped to the higher category. For instance, if the mean value is 1.25, the fuzzy rule output will be mapped to 1 (Negligible), while if the mean value is 1.6, the fuzzy rule output will be mapped to 2 (Low). Table 6 represents combinations of fuzzy rules inputs, number of experts' responses for each rule and rule output after taking the mean of all experts' responses and mapped it to the category of the output risk linguistic expressions according to the previous assumption.

**Table 6.** Building fuzzy rules through IoT security experts

| Rule No | Rule Inputs | | | | Experts Responses regarding each rule | | | | | Mean | Mapped Category | Rule Output |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | RS | UC | RH | N | L | M | H | UH | | | |
| **1** | L | NS | L | L | 20 | 0 | 0 | 0 | 0 | 1 | 1 | **N** |
| **2** | M | NS | L | L | 15 | 5 | 0 | 0 | 0 | 1.25 | 1 | **N** |
| **3** | H | NS | L | L | 6 | 5 | 9 | 0 | 0 | 2.15 | 2 | **L** |
| **4** | L | S | L | L | 11 | 6 | 1 | 2 | 0 | 1.70 | 2 | **L** |
| **5** | M | S | L | L | 1 | 5 | 12 | 5 | 0 | 2.75 | 3 | **M** |
| **6** | H | S | L | L | 0 | 5 | 10 | 5 | 0 | 3 | 3 | **M** |
| **7** | L | HS | L | L | 1 | 11 | 6 | 2 | 0 | 2.45 | 2 | **L** |
| **8** | M | HS | L | L | 0 | 4 | 13 | 2 | 1 | 3 | 3 | **M** |
| **9** | H | HS | L | L | 0 | 5 | 6 | 8 | 1 | 3.25 | 3 | **M** |
| **10** | L | NS | M | L | 18 | 2 | 0 | 0 | 0 | 1.10 | 1 | **N** |
| **11** | M | NS | M | L | 11 | 3 | 6 | 0 | 0 | 1.75 | 2 | **L** |
| **12** | H | NS | M | L | 7 | 1 | 12 | 0 | 0 | 2.25 | 2 | **L** |
| **13** | L | S | M | L | 1 | 9 | 9 | 1 | 0 | 2.5 | 3 | **M** |
| **14** | M | S | M | L | 0 | 7 | 11 | 2 | 0 | 2.75 | 3 | **M** |
| **15** | H | S | M | L | 0 | 0 | 6 | 14 | 0 | 3.7 | 4 | **H** |
| **16** | L | HS | M | L | 0 | 0 | 14 | 6 | 0 | 3.3 | 3 | **M** |

| Rule No | Rule Inputs | | | | Experts Responses regarding each rule | | | | | Mean | Mapped Category | Rule Output |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | RS | UC | RH | N | L | M | H | UH | | | |
| **17** | M | HS | M | L | 0 | 0 | 6 | 13 | 1 | 3.75 | 4 | **H** |
| **18** | H | HS | M | L | 0 | 0 | 6 | 12 | 2 | 3.8 | 4 | **H** |
| **19** | L | NS | H | L | 17 | 1 | 2 | 0 | 0 | 1.25 | 1 | **N** |
| **20** | M | NS | H | L | 1 | 13 | 4 | 2 | 0 | 2.35 | 2 | **L** |
| **21** | H | NS | H | L | 0 | 0 | 15 | 5 | 0 | 3.25 | 3 | **M** |
| **22** | L | S | H | L | 0 | 0 | 19 | 1 | 0 | 3.05 | 3 | **M** |
| **23** | M | S | H | L | 0 | 0 | 12 | 8 | 0 | 3.4 | 3 | **M** |
| **24** | H | S | H | L | 0 | 0 | 0 | 20 | 0 | 4 | 4 | **H** |
| **25** | L | HS | H | L | 0 | 0 | 7 | 13 | 0 | 3.65 | 4 | **H** |
| **26** | M | HS | H | L | 0 | 0 | 0 | 4 | 16 | 4.8 | 5 | **UH** |
| **27** | H | HS | H | L | 0 | 0 | 0 | 6 | 14 | 4.7 | 5 | **UH** |
| **28** | L | NS | L | M | 15 | 3 | 1 | 1 | 0 | 1.4 | 1 | **N** |
| **29** | M | NS | L | M | 7 | 8 | 5 | 0 | 0 | 1.9 | 2 | **L** |
| **30** | H | NS | L | M | 0 | 11 | 6 | 3 | 0 | 2.6 | 3 | **M** |
| **31** | L | S | L | M | 1 | 13 | 5 | 1 | 0 | 2.3 | 2 | **L** |
| **32** | M | S | L | M | 0 | 0 | 18 | 2 | 0 | 3.1 | 3 | **M** |
| **33** | H | S | L | M | 0 | 0 | 8 | 11 | 1 | 3.65 | 4 | **H** |
| **34** | L | HS | L | M | 0 | 1 | 13 | 6 | 0 | 3.25 | 3 | **M** |
| **35** | M | HS | L | M | 0 | 0 | 4 | 16 | 0 | 3.8 | 4 | **H** |
| **36** | H | HS | L | M | 0 | 0 | 0 | 15 | 5 | 4.25 | 4 | **H** |
| **37** | L | NS | M | M | 12 | 5 | 2 | 1 | 0 | 1.6 | 2 | **L** |
| **38** | M | NS | M | M | 2 | 9 | 6 | 3 | 0 | 2.5 | 3 | **M** |
| **39** | H | NS | M | M | 0 | 10 | 5 | 5 | 0 | 2.75 | 3 | **M** |
| **40** | L | S | M | M | 0 | 2 | 18 | 0 | 0 | 2.9 | 3 | **M** |
| **41** | M | S | M | M | 0 | 0 | 15 | 5 | 0 | 3.25 | 3 | **M** |
| **42** | H | S | M | M | 0 | 0 | 2 | 18 | 0 | 3.9 | 4 | **H** |
| **43** | L | HS | M | M | 0 | 0 | 1 | 19 | 0 | 3.95 | 4 | **H** |
| **44** | M | HS | M | M | 0 | 0 | 0 | 19 | 1 | 4.05 | 4 | **H** |
| **45** | H | HS | M | M | 0 | 0 | 0 | 8 | 12 | 4.6 | 5 | **UH** |
| **46** | L | NS | H | M | 1 | 16 | 0 | 3 | 0 | 2.25 | 2 | **L** |
| **47** | M | NS | H | M | 0 | 0 | 16 | 4 | 0 | 3.2 | 3 | **M** |
| **48** | H | NS | H | M | 0 | 0 | 10 | 10 | 0 | 3.5 | 4 | **H** |
| **49** | L | S | H | M | 0 | 0 | 6 | 13 | 1 | 3.75 | 4 | **H** |
| **50** | M | S | H | M | 0 | 0 | 0 | 20 | 0 | 4 | 4 | **H** |
| **51** | H | S | H | M | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **52** | L | HS | H | M | 0 | 0 | 1 | 15 | 4 | 4.15 | 4 | **H** |
| **53** | M | HS | H | M | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **54** | H | HS | H | M | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **55** | L | NS | L | H | 1 | 17 | 1 | 1 | 0 | 2.1 | 2 | **L** |
| **56** | M | NS | L | H | 0 | 8 | 10 | 2 | 0 | 2.7 | 3 | **M** |
| **57** | H | NS | L | H | 0 | 1 | 10 | 9 | 0 | 3.4 | 3 | **M** |
| **58** | L | S | L | H | 0 | 2 | 15 | 3 | 0 | 3.05 | 3 | **M** |
| **59** | M | S | L | H | 0 | 0 | 8 | 12 | 0 | 3.6 | 4 | **H** |
| **60** | H | S | L | H | 0 | 0 | 1 | 4 | 15 | 4.7 | 5 | **UH** |
| **61** | L | HS | L | H | 0 | 0 | 3 | 9 | 8 | 4.25 | 4 | **H** |
| **62** | M | HS | L | H | 0 | 0 | 0 | 5 | 15 | 4.75 | 5 | **UH** |
| **63** | H | HS | L | H | 0 | 0 | 0 | 2 | 18 | 4.9 | 5 | **UH** |
| **64** | L | NS | M | H | 0 | 17 | 1 | 2 | 0 | 2.25 | 2 | **L** |
| **65** | M | NS | M | H | 0 | 7 | 11 | 2 | 0 | 2.75 | 3 | **M** |
| **66** | H | NS | M | H | 0 | 1 | 11 | 6 | 2 | 3.45 | 3 | **M** |
| **67** | L | S | M | H | 0 | 0 | 4 | 16 | 0 | 3.8 | 4 | **H** |
| **68** | M | S | M | H | 0 | 0 | 1 | 19 | 0 | 3.95 | 4 | **H** |
| **69** | H | S | M | H | 0 | 0 | 0 | 2 | 18 | 4.9 | 5 | **UH** |
| **70** | L | HS | M | H | 0 | 0 | 0 | 5 | 15 | 4.75 | 5 | **UH** |
| **71** | M | HS | M | H | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **72** | H | HS | M | H | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **73** | L | NS | H | H | 0 | 1 | 18 | 1 | 0 | 3 | 3 | **M** |
| **74** | M | NS | H | H | 0 | 0 | 2 | 10 | 8 | 4.3 | 4 | **H** |
| **75** | H | NS | H | H | 0 | 0 | 1 | 12 | 7 | 4.3 | 4 | **H** |

| Rule No | Rule Inputs | | | | Experts Responses regarding each rule | | | | | Mean | Mapped Category | Rule Output |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AS | RS | UC | RH | N | L | M | H | UH | | | |
| **76** | L | S | H | H | 0 | 0 | 1 | 9 | 10 | 4.45 | 4 | **H** |
| **77** | M | S | H | H | 0 | 0 | 0 | 2 | 18 | 4.9 | 5 | **UH** |
| **78** | H | S | H | H | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **79** | L | HS | H | H | 0 | 0 | 0 | 3 | 17 | 4.85 | 5 | **UH** |
| **80** | M | HS | H | H | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |
| **81** | H | HS | H | H | 0 | 0 | 0 | 0 | 20 | 5 | 5 | **UH** |

# 7. Implementation of Proposed Technique

A fuzzy logic system is a computational approach which imitates how people think. It describes the world in imprecise terms such as if the temperature is hot, it responds with precise action. Computers can work only on precise evaluations, while the human brain can provide reasoning with uncertainties and judgments [42]. The fuzzy logic system is considered as a try to combine both techniques. Indeed, the fuzzy logic system is a precise problem-solving approach that has the ability to work with numerical data and linguistic knowledge simultaneously. It simplifies the management of complex systems without the need for its mathematical description [43].

The computation process using the fuzzy logic system consists of three main phases:

1. *Fuzzification* – The majority of variables are crisp or classical variables. Fuzzification process is used to change input and output crisp variables into fuzzy variables to process it and produce the desired output.
2. *Fuzzy Inference Process* – Describing relationships between different inputs and output to drive the fuzzy output is done through building IF-THEN fuzzy rules. The fuzzy IF-THEN rule uses linguistic variables to describe the relationship between a certain condition and an output. The IF part is mainly used to represent the condition, and the THEN part is used to provide the output in linguistic description. The IF-THEN rule is commonly employed by the fuzzy logic system to represent how the input data matches the condition of a rule [42].
3. *Defuzzification* – Since the output should be a crisp variable, this phase converts the fuzzy output back to the crisp output [43].

The proposed risk estimation approach is implemented using MATLAB fuzzy logic toolbox. MATLAB provides an efficient framework and easy-to-use graphical user interfaces that can generate surfaces and plots to analyse the system's performance [15]. Mamdani Fuzzy Inference System (FIS) was adopted to implement the risk estimation process. This is because it is intuitive, has widespread acceptance and is well suited to human inputs. Figure 4 shows the implementation of the proposed fuzzy model.

There are five steps to implement a Mamdani FIS; The first step is used to convert the input and output variables of the system into linguistic expressions (fuzzy sets). As confirmed by the IoT security experts, three fuzzy sets were used to represent each risk factor and five fuzzy sets were used to represent the output risk, as indicated in Table 5.

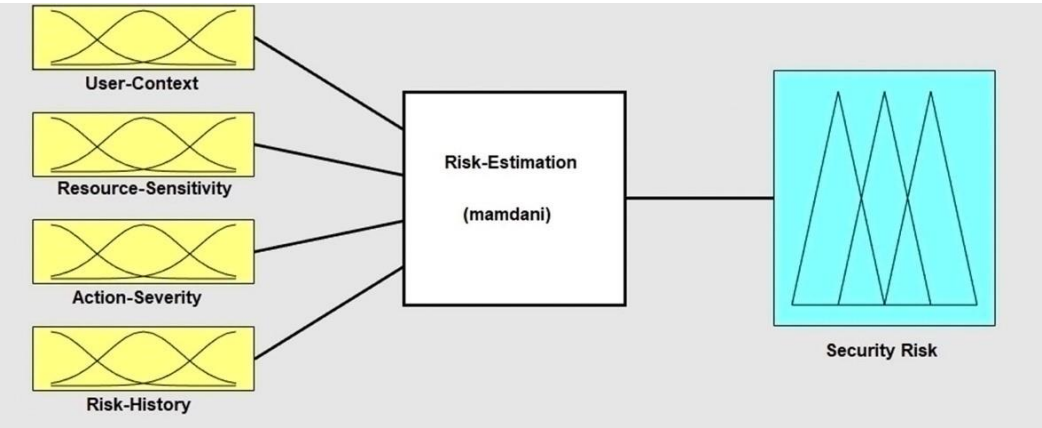


**Figure 4**. Implementation of Risk estimation in MATLAB fuzzy logic toolbox

The second step is to specify the MF that represent the relationship between input risk factors and output risk. Based on IoT security experts' suggestion, triangular MF is appropriate as it provides a proper representation of the expert knowledge and facilitates the calculation process [15]. Figure 5-8 shows the representation of the triangular MF four input risk factors, while Figure 9 shows the representation of the triangular MF of the output risk.

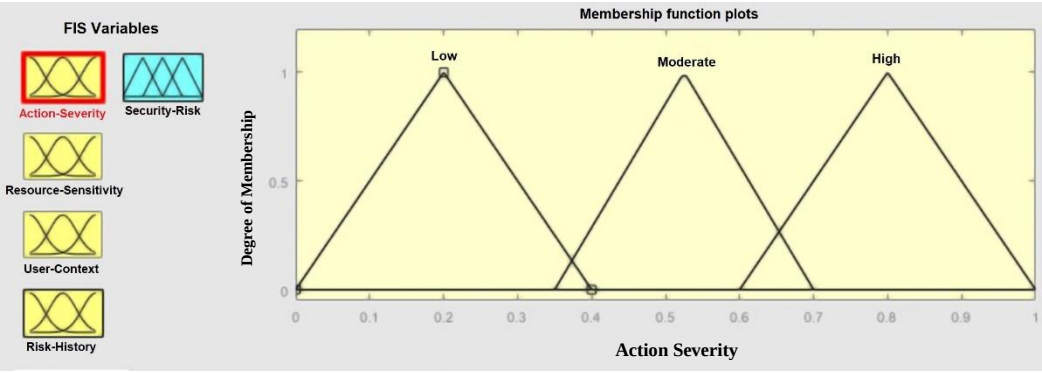


**Figure 5.** Triangular MF of the action severity

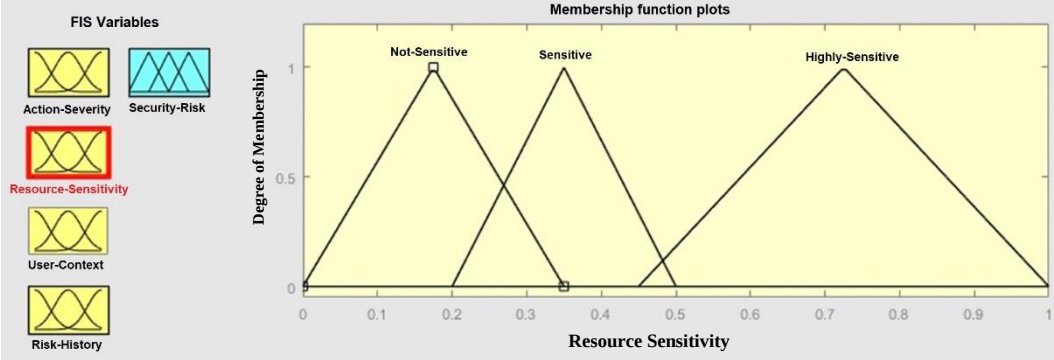


**Figure 6.** Triangular MF of the resource sensitivity

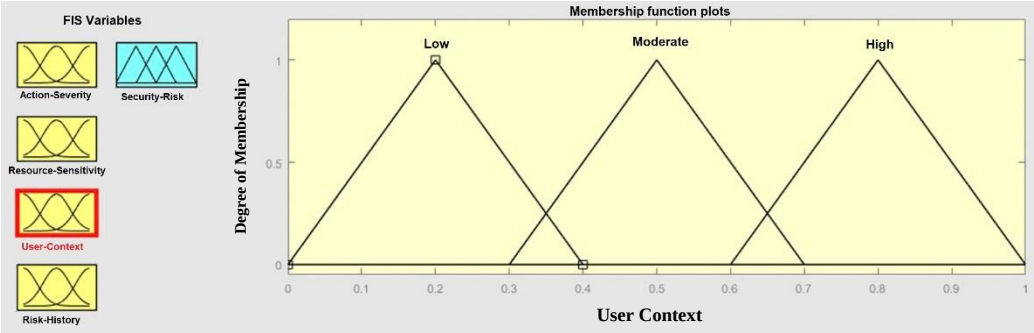


**Figure 7**. Triangular MF of the user context

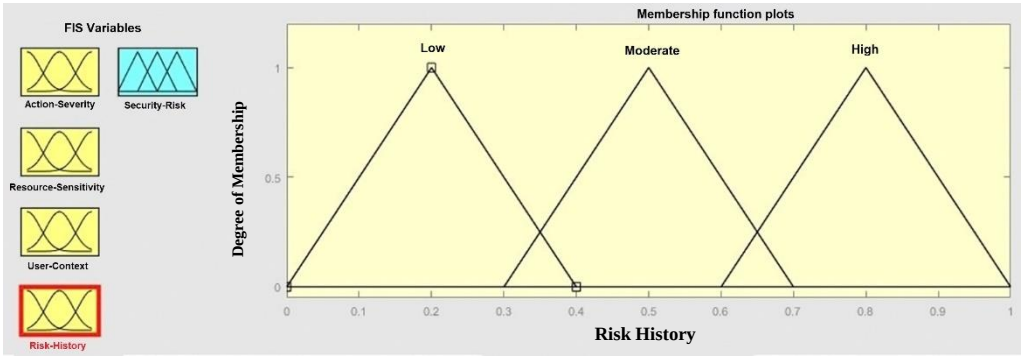


**Figure 8.** Triangular MF of the risk history

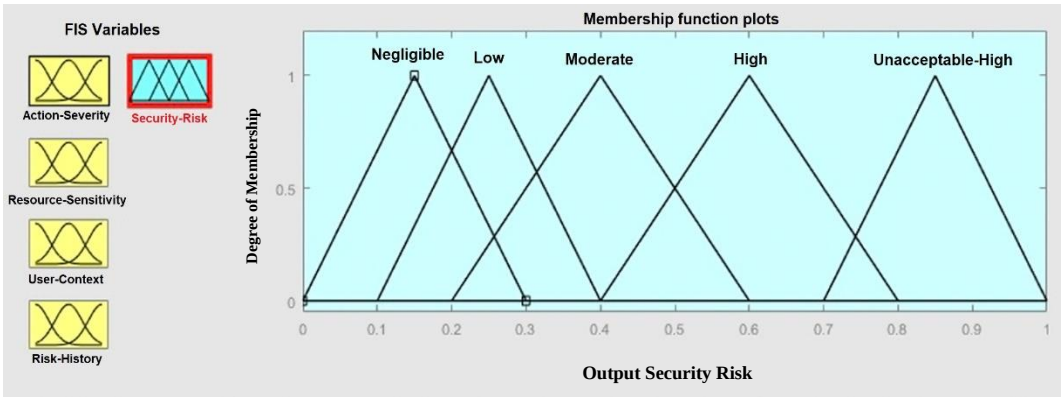


**Figure 9.** Triangular MF of the output risk

The third step is fuzzy rules, which are the knowledge base that is used by the fuzzy model to generate the output. In this research, there is no dataset so there is no way to ensure

appropriate fuzzy rules were created. Therefore, Twenty IoT security experts were used to create fuzzy rules of the proposed risk estimation technique. after that, MATLAB rule editor was used to construct fuzzy rules statements automatically. All the rules had the same weight and the connection type was logical AND.

The fourth step is the rule aggregation which combines outputs of all fuzzy rules. In other words, MFs of all fuzzy rules are gathered into a single fuzzy set via rule aggregation [15]. The max (maximum) aggregation operator will be used to combine output rules into one fuzzy set. The final step is the defuzzification. The output risk of the proposed fuzzy model must be back to be a crisp value. As confirmed by IoT security experts, the centroid method was selected to defuzzifize the output.

# 8. Simulation Results

To test the proposed risk estimation approach, access control scenarios of the network router will be simulated to show different access decisions in various situations based on the risk value related to each access request. All experiments and measurement were coded using MATLAB on Intel(R) Core (TM) i7-2600, 3.40 GHz CPU with 16 GB RAM running Windows 10.

The network router is an electronic device designed to connect at least two networks and forward packets among them according to the information existed in the packet header and routing table. The router is a fundamental element to the operation of the Internet and other complex networks [40, 41].

To provide access control scenarios of the network router, four parameters need to be specified:

1) Router access methods: specify various methods to access the router.
2) Router data to be accessed: a user will access the router only to perform certain operations on certain data. Therefore, different router data and operations should be specified.
3) Values of four risk factors of the proposed risk model: to calculate the risk value related to each access request, the value of user context, resource sensitivity, action severity and user risk history should be specified.
4) Router acceptable risk values: after estimating the risk value of the requesting user, the access decision should be decided to either grant or deny the access.

Before starting experiments, we will specify these four parameters. Firstly, there are two methods to access the network router via console and telnet connection. The router console connection is used to connect end devices, such as PC to the router to manage its configurations using a rollover cable connection. While telnet connection is used to configure the router remotely through a router virtual terminal.

Secondly, we categories data that can be accessed through the router as follows:

- Non-Volatile Random-Access Memory (NVRAM) data: is used to store start-up configuration files of the router.
- Dynamic Host Configuration Protocol (DHCP) data: allocates IP address information to various devices in the network dynamically.
- Flash Data: is used to store the router internetworking operating system.
- Configuration passwords: are router passwords that are required to enter different router configuration modes to add or edit any configuration commands.
- Routing table data: is used by the router to determine the best path to forward packets to its destination. Without routing table, all router packets will be discarded.

The router data were classified in terms of actions severity and data sensitivity levels, as shown in Table 7. The data sensitivity level is depending on the action to be performed. For instance, “View” operation is not sensitive while “Delete” operation is sensitive on the same NVRAM data.

**Table 7.** Data sensitivity with different actions regarding router data

| Router Data | Action | Sensitivity |
|---|---|---|
| NVRAM data | View | Not Sensitive |
| | Delete | Sensitive |
| | Modify | Sensitive |
| DHCP data | View | Not Sensitive |
| | Modify | Sensitive |
| | Create | Sensitive |
| Flash Data | Delete | Not Sensitive |
| Configuration passwords | View | Sensitive |
| | Modify | Sensitive |
| Routing table | View | Not Sensitive |
| | Delete | Sensitive |

Thirdly, to formulate access control scenarios of the router, the values of the four risk factors of the proposed risk-based model need to be specified. Therefore, we will use Sharma et al. [18] formula to calculate the risk value regarding action severity and data sensitivity. The risk

value is calculated in terms of various actions, risk probability, and cost regarding data availability, integrity, and confidentiality. The formula is represented as:

$$\text{Risk} = (C \times P) + (I \times P) + (A \times P) \quad (1)$$

Where C, I and A represents confidentiality, integrity, and availability respectively. While P represents the probability. Also, Sharma et al. [18] have suggested some actions and corresponding values of CIA, as shown in Table 8. Therefore, values of action severity and resource sensitivity of the proposed approach can be estimated from this table. For instance, if a user needs to carry out a "view" operation on sensitive data and the probability was assumed 0.5. Therefore, only confidentiality will be affected, and the risk score will be 0.5.

**Table 8.** Risk values associated with action and data sensitivity [18]

| Action | Sensitivity | C | I | A |
|---|---|---|---|---|
| Create | Sensitive/Not-Sensitive | 0 | 1 | 1 |
| View | Sensitive | 1 | 0 | 0 |
| View | Not-Sensitive | 0 | 0 | 1 |
| Modify | Sensitive/Not-Sensitive | 0 | 1 | 1 |
| Delete | Sensitive/Not-Sensitive | 0 | 1 | 1 |

Finally, after estimating the risk value of the requesting user, the access decision should be determined. We assumed that the risk threshold value will be 0.5 such that if the output risk value is lower than or equal to 0.5, the access will be granted, otherwise the access will be denied. The risk threshold value can be changed easily according to the system owner to increase system flexibility.

Next section provides simulation results of console and telnet connection of the network router.

## 8.1 Scenario 1

Suppose a user wants to manage router configurations through the console connection. The router was initially configured but the user wants to access the router to perform other operations. Since the user has the ability to reach the physical location of the router and attach the rollover cable to connect the router to his/her end device, so he/she will be considered as a trusted user with low-risk history and low user context. Therefore, the risk history and user context will be assumed to be 0.35.

The values of resource sensitivity and action severity were calculated using Sharma et al. in [18] formula with assuming the risk probability to be 0.4. Table 9 shows different access control scenarios of the router through the console connection. The proposed risk estimation approach has used values of risk factors to measure the risk value related to each access control

scenario. For instance, when the user context was 0.35, the sensitivity of data to be accessed by the requesting user was 0.4, the severity of action to be performed was 0.4 and risk history of requesting user was 0.35, the risk estimation approach computes the risk of the access request which was 0.4. Since the risk threshold is less than 0.5 or equal, the access was granted.

As shown in Table 9, when values of resource sensitivity and action severity were 0.4, the output risk values were below the risk threshold value which has resulted in granting the access to the requesting user. While when values of resource sensitivity and action severity were 0.8 or 0.9, the value of output risk was higher than the risk threshold value, so the access has been denied.

**Table 9.** Access control scenarios of console connection using proposed risk estimation approach

| **Router Data** | **Action** | **Risk Factors** | | | | **Output Risk Value** | **Access Decision** |
|---|---|---|---|---|---|---|---|
| | | User Context | Resource Sensitivity | Action Severity | Risk History | | |
| NVRAM data | View | 0.35 | 0.4 | 0.4 | 0.35 | 0.40 | Access granted |
| | Delete | 0.35 | 0.9 | 0.9 | 0.35 | 0.60 | Access denied |
| | Modify | 0.35 | 0.8 | 0.8 | 0.35 | 0.60 | Access denied |
| DHCP data | View | 0.35 | 0.4 | 0.4 | 0.35 | 0.40 | Access granted |
| | Modify | 0.35 | 0.8 | 0.8 | 0.35 | 0.60 | Access denied |
| | Create | 0.35 | 0.8 | 0.8 | 0.35 | 0.60 | Access denied |
| Flash Data | Delete | 0.35 | 0.8 | 0.8 | 0.35 | 0.60 | Access denied |
| Configuration passwords | View | 0.35 | 0.4 | 0.4 | 0.35 | 0.40 | Access granted |
| | Modify | 0.35 | 0.9 | 0.9 | 0.35 | 0.60 | Access denied |
| Routing table | View | 0.35 | 0.4 | 0.4 | 0.35 | 0.40 | Access granted |
| | Delete | 0.35 | 0.8 | 0.8 | 0.35 | 0.60 | Access denied |

## 8.2 Scenario 2

Consider a user wants to manage router configurations remotely. The router was initially configured but the user wants to access the router to perform other operations. Since the user is trying to access the router from a remote location, the user context will be high, so we assumed it to be 0.75. Also, the user risk history is assumed to be unknown because the router owner can access the router remotely and the malicious user as well. Therefore, we assumed that risk history has two values 0.35 and 0.75.

The access to the router via telnet connection will be the same as console connection in terms of values of actions severity and data sensitivity on the router data. Also, the risk probability assumed to be 0.4. Table 10 shows access control scenarios of telnet connection using the proposed risk estimation approach. Most access requests were denied. This is because values of user context and risk history were assumed to be high. Further, when the risk history was

low; 0.35, the access was also denied since values of user context, action severity and resource sensitivity were high, which lead to a high-risk value in the output.

On the other hand, access is granted only when risk history, action severity, and resource sensitivity values were low. In other words, the access has been granted only when the value of risk history was 0.35 and values of both action severity and resource sensitivity were 0.4.

**Table 10.** Access control scenarios of telnet connection using the proposed risk estimation approach

| **Router Data** | **Action** | **Risk Factors** | | | | **Output Risk Value** | **Access Decision** |
|---|---|---|---|---|---|---|---|
| | | User Context | Resource Sensitivity | Action Severity | Risk History | | |
| NVRAM data | View | 0.75 | 0.4 | 0.4 | 0.35 | 0.50 | Access granted |
| | View | 0.75 | 0.4 | 0.4 | 0.75 | 0.85 | Access denied |
| | Delete | 0.75 | 0.9 | 0.9 | 0.35 | 0.85 | Access denied |
| | Delete | 0.75 | 0.9 | 0.9 | 0.75 | 0.85 | Access denied |
| | Modify | 0.75 | 0.8 | 0.8 | 0.35 | 0.85 | Access denied |
| | Modify | 0.75 | 0.8 | 0.8 | 0.75 | 0.85 | Access denied |
| DHCP data | View | 0.75 | 0.4 | 0.4 | 0.35 | 0.50 | Access granted |
| | View | 0.75 | 0.4 | 0.4 | 0.75 | 0.85 | Access denied |
| | Modify | 0.75 | 0.8 | 0.8 | 0.35 | 0.85 | Access denied |
| | Modify | 0.75 | 0.8 | 0.8 | 0.75 | 0.85 | Access denied |
| | Create | 0.75 | 0.8 | 0.8 | 0.75 | 0.85 | Access denied |
| | Create | 0.75 | 0.8 | 0.8 | 0.35 | 0.85 | Access denied |
| Flash Data | Delete | 0.75 | 0.8 | 0.8 | 0.35 | 0.85 | Access denied |
| | Delete | 0.75 | 0.8 | 0.8 | 0.75 | 0.85 | Access denied |
| Configuration passwords | View | 0.75 | 0.4 | 0.4 | 0.35 | 0.50 | Access granted |
| | View | 0.75 | 0.4 | 0.4 | 0.75 | 0.85 | Access denied |
| | Modify | 0.75 | 0.9 | 0.9 | 0.75 | 0.85 | Access denied |
| | Modify | 0.75 | 0.9 | 0.9 | 0.35 | 0.85 | Access denied |
| Routing table | View | 0.75 | 0.4 | 0.4 | 0.35 | 0.50 | Access granted |
| | View | 0.75 | 0.4 | 0.4 | 0.75 | 0.85 | Access denied |
| | Delete | 0.75 | 0.8 | 0.8 | 0.75 | 0.85 | Access denied |
| | Delete | 0.75 | 0.8 | 0.8 | 0.35 | 0.85 | Access denied |

# 9. Discussion and Conclusion

Current access control models based on static and predetermined policies cannot satisfy the flexibility needed in various IoT applications. While risk-based access control model provides a dynamic approach by using not only policies but also real-time and contextual information to make the access decision. This model aims to increase information sharing of IoT applications by estimating the risk value associated with each access request and compare it

with a threshold risk value to make the access decision. One of the main objectives of this research is to build a dynamic access control model for the IoT that can use real-time and contextual features collected from the IoT environment while making the access request to make the access decision. These features are used as a risk factor with other three risk factors (resource sensitivity, action severity, and risk history) to estimate the overall risk value associated with each access request to determine the access decision. These contextual features depend on the IoT application. For instance, in a healthcare context, location and time can be used to provide a risk metric for contextual features associated with a doctor, or any actor in the healthcare application, while requesting to access patient information to either write a prescription or order examinations.

Reviewing existing and related risk-based access control models demonstrated that no previous research has employed the contextual and real-time features collected from the IoT environment while making the access request as a risk factor to estimate the risk associated with the access request. Table 11 provides a summary of risk factors used by different related risk-based access control models discussed with the proposed risk-based access control model.

**Table 11**. Risk factors used to build risk-based access control model

| Risk Model | Subject clearance | Object clearance | Resource Sensitivity | Action Severity | Risk History | Contextual Features |
|---|---|---|---|---|---|---|
| Chen et al. [7] | ✓ | ✓ | | | | |
| Li, Bai and Zaman [15] | | | ✓ | ✓ | ✓ | |
| Ni, Bertino and Lobo [13] | ✓ | ✓ | | | | |
| Khambhammettu et al. [14] | | | ✓ | | | |
| Shaikh, Adi and Logrippo [9] | | | | | ✓ | |
| Rajbhandari and Snekkenes [17] | ✓ | | | ✓ | | |
| Sharma et al. [18] | | | ✓ | ✓ | ✓ | |
| Diep et al. [11] | | | | ✓ | | |
| Arias-Cabarcos et al. [16] | | | | ✓ | | |
| Proposed Model | | | ✓ | ✓ | ✓ | ✓ |

The fuzzy logic system supported with expert knowledge was selected to implement the risk estimation module of the proposed risk-model, after reviewing different risk estimation techniques used in the context of access control in the literature. The proposed technique solved the issue of unavailability of a dataset by interviewing twenty IoT security experts from inside and outside the UK to validate the proposed technique and define correct fuzzy parameters to implement the fuzzy model. The fuzzy logic system has converted experts' qualitative

expressions into numeric values that can be used to make the access decision for an access request. The proposed fuzzy model has implemented and proved it can provide realistic and accurate results for estimating security risks access control operations in different situations. It also has proved that it can provide a scalable and flexible risk-based access control model.

The proposed fuzzy technique was compared against previous fuzzy models used to estimate security risks of access control operations, as shown in Table 12. As compared with existing fuzzy models, our proposed technique provides a dynamic and context-aware model by using real-time and contextual features associated with user/agent at the time of making the access request as a risk factor besides resource sensitivity, action severity and risk history to estimate the risk values associated with each access request to decide the access decision. Fuzzy rules are the brain of the fuzzy logic system which needs to be built accurately to output a precise risk value for each access request. Although fuzzy rules are built on expert knowledge, there is no evidence or any details about using security experts to build fuzzy rules in related fuzzy models in risk-based access control models discussed in the literature. Also, their work did not provide any details about how to identify the fuzzy variables. Moreover, in situations of defining fuzzy rules by experts, the number of experts ranges between 5-8 due to the complexity to reach a large number of experts, but in this research, we used Twenty IoT security experts from inside and outside the UK to build fuzzy rules and identify other fuzzy variables. This number of experts adds more robustness and accuracy to the research.

**Table 12.** Comparison between the proposed technique with existing fuzzy-based models to estimate security risks of access control operations.

| Items | Chen et al. [7] | Ni et al. [13] | Li et al. [15] | Proposed Technique |
|---|---|---|---|---|
| Risk factors | Difference between subject security level and object security level | Object security level and subject security level | Data sensitivity, action severity, and user risk history | Contextual features of user/agent, resource sensitivity, action severity and risk history |
| Context-awareness | Not Context-aware | Not Context-aware | Not Context-aware | Context-aware |
| Fuzzy rules | Fuzzy rules are built by authors | Fuzzy rules are built by authors | Fuzzy rules are built by authors | Twenty IoT security experts were interviewed to build fuzzy rules |
| Subjectivity | High subjectivity as technique variables are proposed by authors | High subjectivity as technique variables are proposed by authors | High subjectivity as technique variables are proposed by authors | The parameters of the fuzzy logic system and fuzzy rules are built using knowledge of twenty IoT security experts. |
| Validation | No proof of validation is presented | No proof of validation is presented | No proof of validation is presented | The proposed technique has validated using Twenty IoT security experts |
| Unpredicted situations | Not supported as it based on static policies | Not supported as it based on static policies | Not supported as it based on static policies | Flexible in unpredicted situations as it uses real-time features with policies determine the access decision |

| | | | | |
|---|---|---|---|---|
| Technique evaluation | No scenarios are provided to evaluate the technique | No scenarios are provided to evaluate the technique | No scenarios are provided to evaluate the technique | Access control scenarios of a network router are provided to evaluate the proposed technique |

One of the major issues of the fuzzy logic system is subjectivity. Since previous fuzzy-based techniques discussed in the literature build their fuzzy model by their authors, this increases the subjectivity of these models. To reduce the subjectivity in our proposed technique, twenty IoT security experts were interviewed to build fuzzy rules and define fuzzy parameters for the proposed fuzzy technique. Indeed, the subjectivity was not completely eliminated, but we reduce it as we interviewed a quite big number of experts. However, it is unlikely that a method with no subjectivity will ever exist for risk analysis. In addition, although the main target of the risk estimation process is to provide a numeric value for the risk, existing fuzzy-based techniques did not provide a comprehensive discussion about how the risk is estimated quantitively.

In addition, the proposed technique provides a flexible approach that can adapt to changing conditions during making access decisions since it uses real-time information as one of the risk factors to make the access decision. Using only static and rigid policies cannot provide the required flexibility in unpredicted situations especially in healthcare and military in which providing access to required information can literally save thousands of lives. Also, the previous fuzzy-based techniques did not provide proof about how their techniques can be applied to different access control scenarios, while our proposed technique has been validated by presenting different access control scenarios of the network router, as one of IoT devices. The proposed technique has proved that it can generate realistic and accurate results for estimating security risks access control operations in different situations.

Although the fuzzy rules are static, once created cannot be updated, the proposed model provides a dynamic way to provide access decisions and can adapt to unexpected situations of the IoT environment by incorporating updates to user contextual attributes, such as time, location, date, or user description, the access decisions can reflect up-to-the-moment security need. For the proposed fuzzy models, fuzzy rules represent the knowledge base that is used to assess different situations of risk factors including user contextual and real-time attributes to provide the access decision for each access request. Access control scenarios of the network router can provide a good demonstration to this point. For example, when the user asked to perform “Delete” action on the NVRAM data since the risk metric of contextual features associated with the user was 0.35, the output risk value became 0.6. While when the user asked to perform the same action on the same data but with high risk metric for contextual features,

which assumed to be 0.75, the output risk value became 0.85. Therefore, with static fuzzy rules which specified by security experts, the overall output risk value has changed with changing user contextual features.

The efficiency of the proposed fuzzy model is one of the important aspects to demonstrate the applicability of the proposed model in real-world IoT applications. The efficiency of the proposed risk estimation techniques has evaluated with the different number of access requests in term of processing time. We generate different sets of access requests. The set size was in the range [1000, 250000], and the processing time and time per request for each set were calculated, as shown in Table 13. We used the same hardware and software specification used in the simulation of router access control scenarios to provide processing time with different number of access requests. The processing time for each access request was about 0.03 second, which indicates that the proposed fuzzy model can provide a fast and scalable way to provide access decisions.

**Table 13**. Processing time and time per request with different number of access requests

| Number of access requests | Time (Sec) | Time per request (Sec) |
|---|---|---|
| 1000 | 30.49 | 0.0305 |
| 10000 | 306.67 | 0.0307 |
| 20000 | 578.45 | 0.0285 |
| 30000 | 870.15 | 0.0290 |
| 40000 | 1155.12 | 0.0292 |
| 50000 | 1480.41 | 0.0296 |
| 60000 | 1812.14 | 0.0302 |
| 70000 | 2144.23 | 0.0306 |
| 80000 | 2486.32 | 0.0311 |
| 90000 | 2823.32 | 0.0314 |
| 100000 | 3170.21 | 0.0317 |
| 150000 | 4815.214 | 0.0321 |
| 200000 | 6500.174 | 0.0325 |
| 250000 | 8275.236 | 0.0331 |

In the future, in contrast to existing access control models that cannot detect malicious actions during access sessions, we are going use smart contracts to monitor user activities to detect and prevent malicious activity during access sessions. The use of smart contracts to monitor and track users' activities throughout the access session will provide a significant solution to detect security violations in time to protect system resources and prevent sensitive information disclosure.

This paper presented a risk estimation technique to assess security risks of access control operations in IoT applications. The proposed technique uses the fuzzy logic system supported by experts' knowledge and expertise to implement the risk-based model. Twenty IoT security

experts from inside and outside the UK were interviewed to validate the proposed risk estimation approach, build fuzzy rule and define other variables of the proposed fuzzy model. Then, the proposed technique has implemented using MATLAB and tested with various access control scenarios of the network router. Simulation results have demonstrated that it can produce precise and realistic results in evaluating security risks of access control operations.

**Conflict of Interest**: No

# References


[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[2] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "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)*, 2017, no. June, pp. 655–661.

[2] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of Things : State-of-the-art , Challenges , Applications , and Open Issues," *Int. J. Intell. Comput. Res.*, vol. 9, no. 3, pp. 928–938, 2018.

[3] K. Habib and W. Leister, "Context-Aware Authentication for the Internet of Things," *Elev. Int. Conf. Auton. Auton. Syst. fined*, pp. 134–139, 2015.

[4] D. R. Dos Santos, C. M. Westphall, and C. B. Westphall, "A dynamic risk-based access control architecture for cloud computing," *IEEE/IFIP NOMS 2014 - IEEE/IFIP Netw. Oper. Manag. Symp. Manag. a Softw. Defin. World*, pp. 1–9, 2014.

[5] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the Internet of things," *Proc. - 32nd IEEE Int. Conf. Distrib. Comput. Syst. Work. ICDCSW 2012*, pp. 588–592, 2012.

[6] N. Ye, Y. Zhu, R. C. Wang, R. Malekian, and Q. M. Lin, "An efficient authentication and access control scheme for perception layer of internet of things," *Appl. Math. Inf. Sci.*, vol. 8, no. 4, pp. 1617–1624, 2014.

[7] P. Chen, C. Pankaj, P. A. Karger, G. M. Wagner, and A. Schuett, "Fuzzy Multi – Level Security : An Experiment on Quantified Risk – Adaptive Access Control," *2007 IEEE Symp. Secur. Privacy(SP'07)*, pp. 222–227, 2007.

[8] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog Computing and the Internet of Things: A Review," *big data Cogn. Comput.*, vol. 2, no. 2, pp. 1–18, 2018.

[9] R. A. Shaikh, K. Adi, and L. Logrippo, "Dynamic risk-based decision methods for access control systems," *Comput. Secur.*, vol. 31, no. 4, pp. 447–464, 2012.

[10] D. Ricardo dos Santos, C. M. Westphall, and C. B. Westphall, "Risk-based Dynamic Access Control for a Highly Scalable Cloud Federation," *Proc. Seventh Int. Conf. Emerg. Secur. Information, Syst. Technol. (SECUREWARE 2013)*, pp. 8–13, 2013.

[11] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y. Lee, and H. Lee, "Enforcing Access Control Using Risk Assessment," *Fourth Eur. Conf. Univers. Multiservice Networks*, pp. 419–424, 2007.

[12] R. McGraw, "Risk-Adaptable Access Control ( RAdAC )," *inPrivilege Manag. Work. NIST–National Inst. Stand. Technol. Technol. Lab.*, 2009.

[13] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access control systems built on fuzzy inferences," *Proc. 5th ACM Symp. Information, Comput. Commun. Secur. ser. ASIACCS 10. New York, NY, USA ACM*, pp. 250–260, 2010.

[14] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo, "A framework for risk assessment in access control systems," *Comput. Secur.*, vol. 39, pp. 86–103, 2013.

[15] J. Li, Y. Bai, and N. Zaman, "A fuzzy modeling approach for risk-based access control in eHealth cloud," *Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013*, pp. 17–23, 2013.

[16] P. Arias-Cabarcos, F. A. Rez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, "A metric-based approach to assess risk for 'On cloud' federated identity management," *J. Netw. Syst. Manag.*, vol. 20, no. 4, pp. 513–533, 2012.

[17] L. Rajbhandari and E. A. Snekkenes, "Using game theory to analyze risk to privacy: An initial insight," *Priv. Identity Manag. Life, Springer Berlin Heidelb.*, pp. 41–51, 2011.

[18] M. Sharma, Y. Bai, S. Chung, and L. Dai, "Using risk in access control for cloud-assisted ehealth," *High Perform. Comput. Commun. 2012 IEEE 9th Int. Conf. Embed. Softw. Syst. (HPCC-ICESS), 2012 IEEE 14th Int. Conf.*, pp. 1047–1052, 2012.

[19] S. Elky, "An Introduction to Information System Risk Management," 2006.

[20] H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, "Integration of cloud computing with internet of things: challenges and open issues," 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)*, 2017, no. June, pp. 670–675.

[21] S. Lee, Y. W. Lee, N. N. Diep, S. Lee, Y. Lee, and H. Lee, "Contextual Risk-based access control," *Proc. 2007 Int. Conf. Secur. Manag.*, p. pp 406–412, 2007.

[22] G. P. Kulk, R. J. Peters, and C. Verhoef, "Quantifying IT estimation risks," *Sci. Comput. Program.*, vol. 74, no. 11–12, pp. 900–933, 2009.

[23] J. Yin, C. Tang, X. Zhang, and M. McIntosh, "On estimating the security risks of composite software services," in *In First Program Analysis for Security and Safety Workshop Discussion (PASSWORD 2006)*, 2006.

[24] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," *I.J. Comput. Netw. Inf. Secur.*, no. January, pp. 26–35, 2018.

[26] C. J. Alberts and A. Dorofee., *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., Boston,MA, USA, 2002.

[27] D. Kahneman, P. Slovic, and A. Tversky, "Judgment under uncertainty: heuristics and biases," *Science (80-. ).*, vol. 185, no. 4157, pp. 1124–1131, 1974.

[28] D. Pluess, A. Groso, and T. Meyer, "Expert Judegement in Risk Analysis: A Strategy to Overcome Uncertainities," *Chem. Eng. Trans.*, vol. 31, pp. 307–312, 2013.

[29] Da Ruan, *Fuzzy Sets And Fuzzy Information Granulation Theory*. Bejing: Bejing Normal Univeristy Press, 2000.

[30] K. Boc, "Fuzzy approach to risk analysis and its advantages against the qualitative approach," in *Proceedings of the 12th International Conference "Reliability and Statistics in Transportation and Communication*, 2012, no. 12, pp. 234–239.

[31] L. A. Zadeh, "The concept of a linguistic variable and its applications to approximate reasoning," *Inf. Sci. (Ny).*, vol. 8, no. 4, pp. 199–249, 1975.

[32] H.-J. Zimmermann, "Practical Applications of Fuzzy Technologies," in *The Handbooks of Fuzzy Sets*, Springer Berlin Heidelberg, 2000.

[33] T. Eldabi *et al.*, "Quantitative and qualitative decision-making methods in simulation modelling," *Manag. Decis.*, vol. 40, no. 1, pp. 64–73, 2002.

[34] D. Berleant and B. J. Kuipers, "Qualitative and quantitative simulation: bridging the gap," *Artif. Intell.*, vol. 95, pp. 215–255, 1997.

[35] W. Pang and G. M. Coghill, "Qualitative , semi-quantitative , and quantitative simulation of the osmoregulation system in yeast," *BioSystems*, vol. 131, pp. 40–50, 2015.

[36] A. Strauss and J. Corbin, "Basics of Qualitative Research," in *Basics of. Qualitatice Research 2nd edition.*, 1990, pp. 3–14.

[37] G. Guest, A. Bunce, and L. Johnson, "How Many Interviews Are Enough ? An Experiment with Data Saturation and Variability," *Fam. Heal. Int.*, vol. 18, no. 1, pp. 23–27, 2006.

[38] A. Bhattacherjee, "Social Science Research: principles, methods, and practices," 2012.

[39] B. DiCicco-Bloom and B. F. Crabtree, "The qualitative research interview," *Med. Educ.*, vol. 40, no. 4, pp. 314–321, 2006.

[40] R. K. Hussein, A. Alenezi, H. F. Atlam, M. Q. Mohammed, R. J. Walters, and G. B. Wills, "Toward

Confirming a Framework for Securing the Virtual Machine Image in Cloud Computing," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 4, pp. 44–50, 2017.

[41] A. Phinyomark, S. Thongpanja, and H. Hu, "The Usefulness of Mean and Median Frequencies in Electromyography Analysis," in *A Perspective on Current Applications and Future Challenges*, no. December 2014, Dr. Ganesh R. Naik (Ed.), InTech, 2012, pp. 196–218.

[42] Y. Bai and D. Wang, "Fundamentals of Fuzzy Logic Control – Fuzzy Sets , Fuzzy Rules and Defuzzifications," *Adv. Fuzzy Log. Technol. Ind. Appl.*, pp. 17–36, 1982.

[43] U. Kose, "Fundamentals of Fuzzy Logic with an Easy-to-use , Interactive Fuzzy Control Application," *Int. J. Mod. Eng. Res.*, vol. 2, no. 3, pp. 1198–1203, 2012.

[44] A. Shuzhao and W. Zhaohui, "Based on the Part of Routing Information Congestion Modeling Research with the Large-Scale Network," *Int. J. Futur. Gener. Commun. Netw.*, vol. 7, no. 2, pp. 173–182, 2014.

[45] J. Kim *et al.*, "A Traffic Aware Routing Protocol for Congestion Avoidance in Content-Centric Network," *Int. J. Multimed. Ubiquitous Eng.*, vol. 9, no. 9, pp. 69–80, 2014.