Mobile Networks and Applications
https://doi.org/10.1007/s11036-019-01214-w

Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT

Hany F. Atlam [1,2] · Robert J. Walters [1] · Gary B. Wills [1] · Joshua Daniel [3]

Abstract
The Internet of Things (IoT) is becoming the future of the Internet with a large number of connected devices that are predicted to reach about 50 billion by 2020. With proliferation of IoT devices and need to increase information sharing in IoT applications, risk-based access control model has become the best candidate for both academic and commercial organizations to address access control issues. This model carries out a security risk analysis on the access request by using IoT contextual information to provide access decisions dynamically. This model solves challenges related to flexibility and scalability of the IoT system. Therefore, we propose an adaptive risk-based access control model for the IoT. This model uses real-time contextual information associated with the requesting user to calculate the security risk regarding each access request. It uses user attributes while making the access request, action severity, resource sensitivity and user risk history as inputs to analyze and calculate the risk value to determine the access decision. To detect abnormal and malicious actions, smart contracts are used to track and monitor user activities during the access session to detect and prevent potential security violations. In addition, as the risk estimation process is the essential stage to build a risk-based model, this paper provides a discussion of common risk estimation methods and then proposes the fuzzy inference system with expert judgment as to be the optimal approach to handle risk estimation process of the proposed risk-based model in the IoT system.

Keywords Security risk · Internet of Things · Adaptive access control · Context · Fuzzy logic · Expert judgment

1 Introduction

The Internet of Things (IoT) has the ability to connect and communicate billions of things simultaneously. It provides several benefits to consumers and inspires new product, services and applications. Using a collection of cheap sensors and interconnected objects, information can be collected from the surrounding environment to improve our life [1]. The IoT is considered as a universal existence that contains different types of objects that can be connected whether using wireless and wired connections. These objects have a unique addressing scheme that allow them to communicate and interact together to create novel services in various IoT applications such as smart grid, agriculture, smart cities, wearables, transportation, traffic management and others [2, 3].

The IoT notion is not new. Originally, it was first mentioned by Kevin Ashton, who is the founder of MIT auto-identification centre in 1999 [4]. Ashton has said, "*The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so*". Then the IoT has passed several stages until it formally introduced by the International Telecommunication Union (ITU) in 2005 [5]. ITU defines the IoT as: "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" [6].

Although the IoT brought unlimited benefits, it creates several challenges, especially in security. Achieving a higher

✉ Hany F. Atlam
hfa1g15@soton.ac.uk

Robert J. Walters
rjw5@soton.ac.uk

Gary B. Wills
gbw@soton.ac.uk

Joshua Daniel
joshua.daniel@bt.com

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

[2] Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

[3] Security Futures Practice, BT Research & Innovation, Ipswich, UK

Published online: 28 January 2019

level of security is a huge challenge due to the heterogeneous and distributed nature of the IoT system. In addition, applying sophisticated security algorithms could affect usability and user satisfaction. Hence, for the IoT system, the ultimate goal is to create a secure model and at the same time consider the system usability [7].

One of the critical elements to handle security challenges in the IoT is the access control model. This model is used to control the access to system resources by allowing only authorized users who have been successfully authenticated. An access control model consists of three main elements; subject, target and rules. Subjects are system users who make the access request to access system resources (targets). Rules are used to determine the access decision whether granting or denying the access [8, 9].

The major goal of the IoT system is to increase information sharing to maximize organization benefits and at the same time ensures that the highest possible security measures are applied to prevent sensitive information disclosure. However, current access control models are built using predefined rules that give the same result in different situations. This binary decision (grant/deny) cannot create a good and efficient level of security in a dynamic, heterogeneous and distrusted environment like IoT systems [10, 11].

To overcome limitations associated with current access control approaches, researchers have suggested security risk to be used as a criterion to provide the access decision. A risk analysis is carried out on the access request to measure the security risk and provide the access decision [9, 12, 13]. This mechanism is known as risk-based access control model. The main issue solved by this model is flexibility in accessing system resources. In addition, this model provides an efficient solution to many unpredicted situations which need to break the access policy because policies are imperfect and lacking such conditions. The need to increase information sharing and considering real-time conditions while making the access decision have encouraged risk-based models to grow significantly [14, 15].

The objective of this research is to develop an adaptive risk-based access control model for the IoT. This model has the capability of estimating the security risk regarding each access request using real-time and contextual information that collected while making the access request. 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 the access request to determine the access decision. In contrast to current access control models, the proposed model provides adaptive features by using smart contracts to track and monitor user's activities during access sessions to detect and prevent potential security attacks. In addition, one of the big challenges to build a risk-based model is to specify the optimal risk estimation technique to assess security risks of access control operations in the IoT system. This is because there are many issues that may arise. For example, the purpose of the risk estimation approach is to expect the probability of information disclosure in the future that corresponds to the current access. Defining such a probability is a difficult process [7, 16]. Furthermore, if the risk estimation process has based on imprecise or incomplete information about related risk attributes, this will make estimating the value of information a very difficult task. Therefore, this paper provides a review of most common risk estimation methods that are used in related risk-based models to determine the optimal approach to implement the risk estimation process for the IoT system. This is followed by proposing a risk estimation technique that combines the fuzzy logic system with expert judgment to assess security risks of access control operations in IoT systems.

The contribution of this paper can be summarized as follows:

- Proposing an adaptive and dynamic risk-based access control model that uses real-time and contextual information to determine the access decision.
- Providing a review of most common risk estimation methods that are used in related risk-based access control models with discussing advantages and limitations of each method.
- Proposing the fuzzy logic system with expert judgment as to be the optimal risk estimation approach to estimate security risks of the proposed risk-based model in the IoT system.

The remainder of this paper is structured as follows: Section 2 presents related work; Section 3 discusses access control challenges that should be taken into our accounts when building an access control model for the IoT; Section 4 discusses risk-based access control model; Section 5 presents proposed risk-based model; Section 6 provides a discussion of most common risk estimation methods that are suggested in related risk-based access control models; Section 7 presents proposed risk estimation approach, and Section 8 is the conclusion.

2 Related work

Many studies have been conducted on different access control models that use security risks to make access decisions. Jason report [17] has investigated limitations of information sharing in dynamic systems by discussing various problems of traditional access control models. The report also explained the importance of using the security risk to make access decisions and suggested three principles to build an access control

model using the risk; estimate the risk, set an acceptable risk value, and control data distribution using the acceptable risk value.

McGraw [18] has proposed a Risk-Adaptable Access Control (RAdAC) mechanism. This approach starts by determining the security risk regarding granting the access. Then the estimated risk value is compared with the access policy that defines the acceptable risk value to grant or deny the access. This is followed by confirming the system operational needs to decide if the policy and operational needs are met or not. If they are met, then the access will be granted, otherwise, the access will be denied. However, this mechanism is not considered as a risk-based model. Also, it does not reveal any information about how to evaluate risk values and operational needs quantitatively and does not use real-time features to determine access.

In addition, Zhang et al. [19] have suggested a Benefit and Risk-based Access Control (BARAC) approach. This approach uses security risk and system benefits to determine the access decision. It assigns a risk and benefit vector for each action. The access to perform a certain action is permitted only if the system benefits are higher than the risk value of the access request. The system creates an action graph to describe permitted actions and methods for users to access system resources. However, this approach uses static and predetermined action graph to determine access. Also, it is very difficult to update action state in the action graph.

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. For example, risk assessment which attracted many researchers to implement the risk estimation process. For example, Diep et al. [20] have introduced an approach 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 estimated risk value with the system acceptable risk value to determine 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. [21] have suggested three different approaches to estimate security risks of access control operations using the risk assessment. These approaches use the subject trustworthiness, the object sensitivity, and the 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 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. [8] proposed a dynamic risk-based decision approach using the risk assessment. This approach uses user previous actions to distinguish 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 and it also lacked adaptive features.

Some researchers suggested using 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. [14] have utilized the fuzzy logic approach to design a fuzzy Multi-Level Security (MLS) 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.

In addition, Bertino and Lobo [22] 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 increasing number of input parameters and fuzzy rules. Moreover, as the access model may require to provide the access to thousands of users especially in the growing IoT technology, this model might be too computationally expensive. It also does not involve contextual information to make the access decision.

In addition, Li et al. [23] have introduced a fuzzy modelling-based method for evaluating security risks of a healthcare information access. 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, this model does not explain how to evaluate risk values quantitatively. In addition, it requires a prior knowledge about various environment situations and does not involve real-time control features to make the access decision.

Some researchers suggested using game theory to measure the risk value of access operations. For example, Rajbhandari and Snekkenes [24] have proposed a risk analysis method that uses values of user benefits to estimate the risk value related to the access request using game theory. However, using only 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. [25] suggested a task-

based model to estimate the security risk using user actions through building a mathematical function. This is followed by comparing the estimated risk value with system acceptable risk value to determine access. However, this paper does not provide any information about how to evaluate risk values quantitatively. In addition, it requires a prior knowledge about outcomes of environmental situations and it lacked real-time contextual features.

In addition, Wang and Jin [26] have proposed a risk-based model which is used to control access operations of patients' medical data. This model enables exceptional access and uses statistical and mathematical methods to measure the risk value related to the access request. However, it does not tell any information about how to evaluate risk values quantitatively. It also lacked contextual information to determine access.

A risk-based model employing the concept of risk metrics has suggested by Dos Santos et al. [8]. This approach uses risk policies defined by the system administrator to identify the risk threshold value to determine access decisions which provides more flexibility. Further, this model is implemented using Python language using quantification architecture of Sharma et al. [25]. Although this approach provides greater flexibility by allowing the resource owner to define his/her own metric, it requires a security administrator to build access policies. Also, it does not use environment contextual information to build access policies.

We can conclude that current risk-based models are missing real-time contextual information, which can be extracted from the IoT environment easily, to make the access decision. Also, they focus only on making access decisions without taking into accounts providing a way to prevent potential security attacks from authorized users throughout access sessions. The novelty of our proposed risk-based model is based on using real-time contextual information of the IoT system while making the access request to determine access decisions. In addition, smart contracts are utilized to adjust user's privileges adaptively regarding their activities during access sessions.

3 Access control challenges in IoT

The IoT system has expanded to include multiple applications and services. It is a dynamic and distributed system which creates several issues that need be taken into accounts when building an access control model. These challenges involve:

1. *Interoperability:* One of the main elements of an access control model is the access policies. These policies should be created to operate with multiple users and organizations. Each organization can create its own policies, but at the same time should respect policies of other organizations [27].
2. *Dynamic Interaction*: In the IoT environment, an access model needs to consider dynamic interactions between users and access policies to incorporate various situations and changing conditions while making access decisions [27].
3. *Usability*: An access control model for the IoT with billions of users who have diverse security awareness and skills need to provide suitable interfaces to fulfil user satisfaction [28].
4. *Context awareness*: According to Cambridge dictionary, context is the situation within which something happens. Using context awareness when building an access control model can enable interactions between users and IoT devices. Therefore, it is necessary to consider real-time contextual information while determining access decisions [29].
5. *Scalability:* The IoT system has billions of devices which produce a massive quantity of data that require huge processing capabilities. Building an access model for the IoT should consider the growth of IoT devices and network size.
6. *Limited resources*: IoT devices have a small size with limited energy, memory, and processing capabilities. Therefore, an access control model for the IoT system ought to enable well-organized solutions [30].
7. *Auditability*: Providing only the access is not enough for the IoT system, an access model should be auditable. Hence, there is a need to collect and store necessary evidence of various access operations.
8. *Delegation of authority*: In some IoT situations, IoT devices need to operate on behalf of a user for a certain period. Therefore, an access model has to consider delegation of authority to enable usability and flexibility of IoT systems [29].

4 Risk-based access control model for IoT

The IoT technology has extended to reach every home in the universe. It has the ability to connect everyday objects to the Internet. Through cheap sensors, a lot of information can be collected from the surrounding environment that results in improving our life. Protecting IoT devices and their communication channels become a mandatory task to prevent sensitive information disclosure which can lead to literally lose lives [27, 31].

The access control is used to protect system resources by limiting the access only to authorized users [32, 33]. Access control models are classified into classical and dynamic approaches. Classical access control models cannot adapt to changing conditions of the IoT system. This is because they use predefined rules that give the same result in different

situations. While dynamic access control models use access rules and real-time and contextual information to determine access decisions [7, 29].

One of the dynamic ways to protect data of IoT devices and encourage information sharing is the risk-based access control model. This model uses security risk as a criterion to determine access decisions. It carries out a risk analysis to measure the risk value of the access request. Security risk is described as the possible harm that may arise from the existing operation or from some upcoming incident. Risk can be found in many aspects of our lives and used in different disciplines. According to Information Technology (IT) security perspective, a security risk is described as the harm to an operation that undesirably impacts the operations and its related information [12].

There are two different ways to build a risk-based model; adaptive and non-adaptive. Adaptive risk-models need a system monitoring operation to track and monitor the user's activities throughout access sessions. Hence, the risk estimation technique adjusts user privileges adaptively according to users' activities during access sessions. Whereas non-adaptive risk-models do not include run-time monitoring operation to detect abnormal actions but only calculate the risk value at the time of creating access sessions [34].

5 Proposed risk-based model for IoT

Although risk-based access control model is still in its first stage of approval, there is a growing need to specify formal models and standard mechanisms for it. This model has many advantages. It provides a flexible access control model that uses environmental contextual information, which is collected while making the access request, to determine the access decision. 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. Indeed, it provides an efficient solution to unexpected situations which require policy violations, as policies are imperfect [15, 29].

Security risk associated with the access request is the building block of the risk-based model. This model carries out a risk analysis to estimate the risk value related to the access request. Then, the estimated risk value is compared against risk policies to determine the access decision. Risk-based model solves several issues related to flexibility in accessing system resources [8, 35].

We propose an adaptive risk-based access control model, as shown in Fig. 1. This model collects real-time and contextual information related to the access request to determine access decisions. The proposed model has four inputs; user context, resource sensitivity, action severity and risk history. These inputs are used by the risk estimation module which is responsible for estimating the overall risk value related to the access request. This is followed by comparing the estimated risk value with risk policies to make access decisions. The decision will be either granting or denying the access. To enable abnormality detection capabilities, we propose smart contracts to track and monitor user's activities throughout access sessions to prevent malicious attacks and sensitive information disclosure.

The proposed model uses real-time features associated with user/agent to represent what is called user context. These features describe the environmental attributes that are related to the user/agent while making the access request. A security risk value is mapped to different user contexts. Location and time are the most common user contexts.

Resource/data sensitivity describes the level of importance of data that may be inappropriately attacked. Defining sensitivity levels of various types of data is a fully subjective operation that depends only on data owner to decide which is more valuable than others. To guarantee an efficient sensitivity classification, security experts should be used to categorize data. Different data have different sensitivity levels; therefore, data is assigned a sensitivity metric to differentiate various types data in the IoT system.

For each access request, the requesting user determines the action he/she wants to perform on a certain resource. Action severity is used to describes the impact of actions on system resources. Security experts can categorize different actions and assign a severity metric for each action. Hence, a risk metric will be associated with each action on a certain resource. In addition, user risk history describes user previous risk values toward various actions performed by the user. It reflects previous users' behaviour patterns to recognize good and malicious users.

One of the fundamental parts of the risk-based model is the risk estimation module. This module takes input risk factors to measure the risk value regarding each access request. The eventual purpose is to build an effective risk estimation method that uses real-time information to give an accurate risk value to control access operations in the IoT system. The estimated risk value is compared against risk policies to determine the access decision. Risk policies are built to define access boundaries and situations where access can be granted or denied. It defines a threshold value such that if the risk value of the access request is lower than the threshold risk value, the access will be granted, otherwise, the access will be denied.

The process flow of the proposed risk-based model is shown in Fig. 2. It begins when a user sends an access request to the access control manager. The requesting user should specify the resource or data to be accessed and action to be performed. The access control manager gathers contextual information related to the requesting user while creating the access request such as location

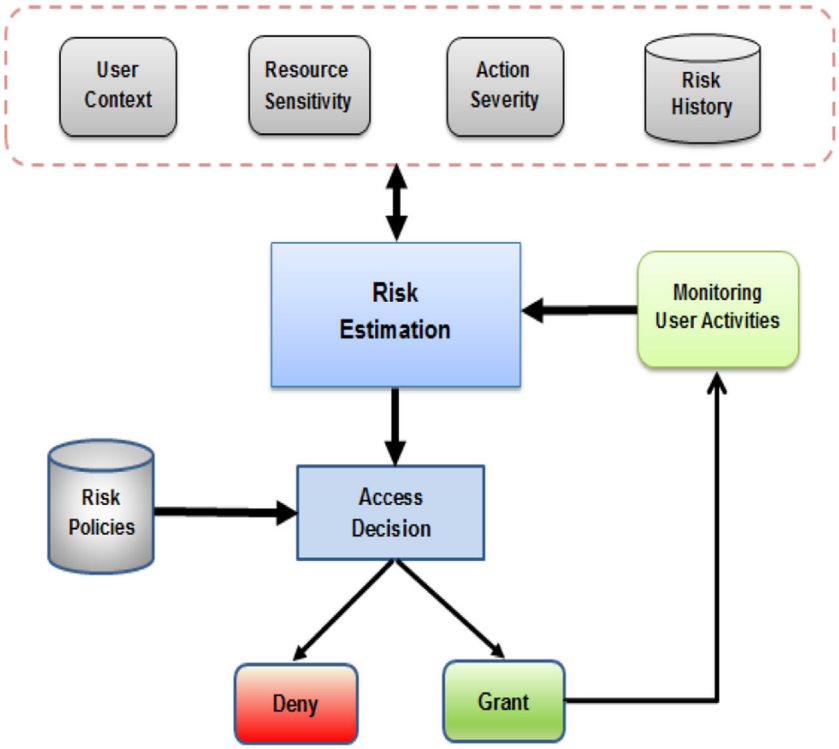

Fig. 1 Proposed risk-based model

and time with the sensitivity level of the resource to be accessed, severity of the action to be performed, as specified in the access request, and the previous risk history records of the requesting user.

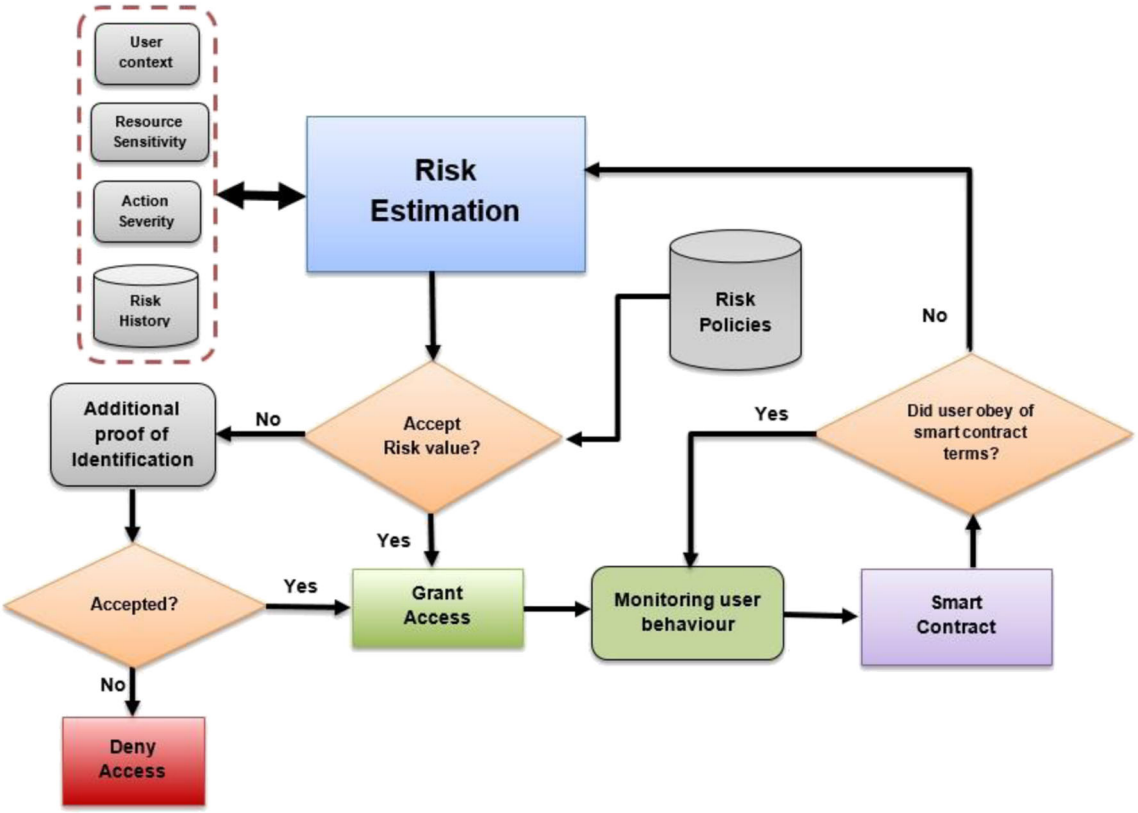

Fig. 2 The process flow of the proposed adaptive risk-based access control model

The risk estimation module uses collected information to measure the risk value associated with the requesting user. This is followed by comparing the measured risk value with risk policies to determine the access decision. If the risk value is less than the threshold risk value specified in risk policies, the access will be granted, otherwise, the access will be denied.

At this stage, we have two scenarios. The first scenario is granting the access. If the access is granted, smart contracts will be used to track and monitor user activities during the access session to detect malicious actions and make sure that the user obeys contract terms and conditions. If the smart contract does not detect any malicious activity, it will keep tracking and monitoring user behaviour throughout the access session. Whilst if a violation is discovered, the system will issue a warning and terminate the session.

The second scenario is denying the access. If the access is denied, to reduce the system false-positive rate, the user will be asked to provide additional proof of identification. If the system receives correct credentials, the access will be granted and the session will be monitored, otherwise, the access will be denied.

Classical access control approaches do not provide a way to detect malicious actions and protect system resources after granting the access. Therefore, the proposed model improves the system flexibility and adds abnormality detection capabilities by utilizing smart contracts to track and monitor user's activities during access sessions. The risk estimation module adjusts user's permission adaptively depending on their behaviour in access sessions such that if an abnormal action is discovered, user privileges will be reduced or the access session will be terminated.

Smart contracts are so powerful because of their flexibility. They can encrypt and store data securely, restrict access to data to only desired parties and then be programmed to utilize the data within a self-executing logical workflow of operations between parties. Smart contracts translate business process into a computational process to improve operational efficiency. Implementing a smart contract is done through building a software code that operates on blockchain [36]. In the proposed model, for each granted user, a smart contract will be created. Therefore, the monitoring module will compare the user behaviour during the access session with terms and conditions of the contract to detect abnormal actions throughout access sessions.

The requesting user defines the data to be accessed and action to be performed in the access request. Hence, if the access is granted, a smart contract will be created by implementing terms and conditions that guarantee that the user will have the ability to only access data and action specified in the access request. Resources/data accessed by the user are monitored to validate that the user is accessing resources that are permitted in the terms of the smart contract. Similarly, actions performed by the user during the access session are monitored to detect any violation for terms and conditions of the smart contract. If a violation is detected, the system will issue a warning message and the access session will be terminated. The process flow of applying smart contracts to monitor user activities during access sessions is shown in Fig. 3.

We believed that the proposed model provides the required flexibility for the IoT system. It provides an efficient solution for many unexpected circumstances which need policy violations by incorporating real-time and contextual features to make the access decision. Also, the use of smart contracts to monitor user activities during the access session provides a significant solution to detect security violations in time to protect system resources and prevent sensitive information disclosure.

Risk estimation module is the most significant element in risk-based models. It is responsible for estimating the risk value related to system risk factors to determine access. However, it is difficult to measure security risks without having a dataset to describes likelihood of various incidents and its impact. In addition, it is critical to consider the system flexibility when choosing the risk estimation technique. Therefore, the next section will provide a review of most common risk estimation methods that are used in related risk-based models with discussing advantages and limitations of each method to choose the optimal technique to implement the proposed risk-based model.

6 Risk estimation techniques

The security risk is one of the main features used in access control models [8]. It is the building block of risk-based access control approaches. Using security risks can increase the security to an appropriate level with ensuring flexibility and scalability of dynamic systems and increase opportunities of information sharing between different applications.

Obviously, the significant phase to implement a risk-based model is the risk estimation module. The security risk can be estimated either by qualitative or quantitative approaches [37]. Quantitative risk estimation approach is concerned with attaching specific numerical values to risks. These values are used directly to determine access decisions. Quantitative risk estimation approaches are ideal as it leads to a numeric value for the risk. However, it is difficult to perform without having a proper dataset describing risk likelihood and its impact on a specific application [38].

Qualitative risk estimation approach is used to calculate the risk early in the system. This is effective in categorising which risks should or should not be planned for and what is the appropriate action that should be taken for them. Qualitative risk analysis techniques cannot give the accurate values of the

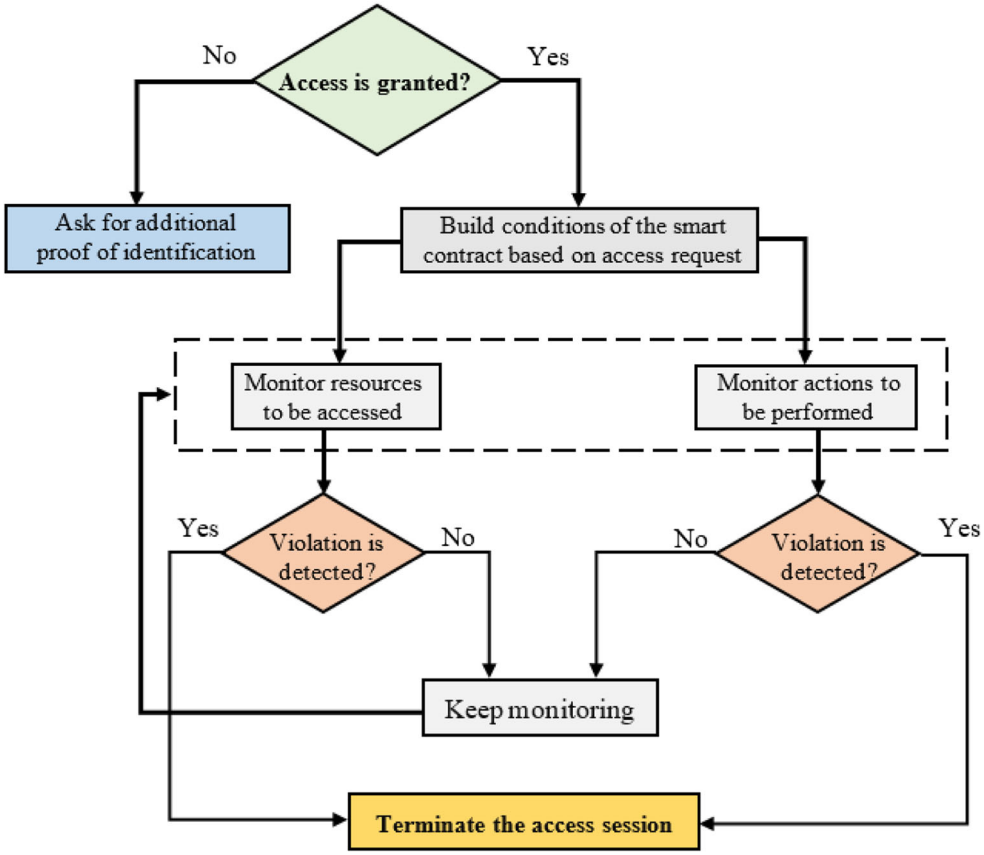

Fig. 3 Process flow of monitoring user activities using smart contracts during access session

risk. However, they are very powerful when we have little time to evaluate risks before they actually happen [37]. Table 1 presents advantages and disadvantages of quantitative and qualitative risk estimation approaches.

Since we want to obtain a numeric value for the risk to determine the access decision, we will discuss only quantitative risk estimation methods that are suggested in related risk-based models.

6.1 Fuzzy logic system

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 [39]. 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 [40].

Fuzzy logic system has many advantages. It is flexible, robust, and based on natural language which makes it easier to understand. It also tolerant to imprecise date in which it can work even when there is lack of rules. On the other hand, it faces some challenges. For instance, it needs domain experts to create accurate rules. Also, it requires more tests and simulations which take a long time especially with increasing number of rules.

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 convert crisp variables of input and output 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 a linguistic form. The IF-THEN rule is commonly used by the fuzzy logic system to represent how the input data matches the condition of a rule [39].
3. *Defuzzification* – Since the output should be a crisp variable, this phase converts the fuzzy output back to the crisp output [40].

Table 1 Advantages and disadvantages of quantitative and qualitative risk estimation methods

Approach	Quantitative methods	Qualitative methods
Advantages	• Risks are arranged by their cost	• Easier to normal people to understand it
	• Objective methods are used to evaluate and estimate risk values	• Easier to detect the risk level
	• Availability, integrity and confidentiality are used to determine the security level	• Estimation methods are easy to understand and implement
	• Best-suited measures are selected based on implementing a cost--analysis	• The risk analysis process is easier as practical value of information is not used
	• With organisation gains more experience, data accuracy will be increased	• Quantitative estimation of events probabilities and impact are not required
		• Estimated cost of the measure that should be implemented is not calculated
Disadvantages	• Calculation methods are complex	• Risk calculation and its results are subjective
	• Very difficult to implement without an automatic tool	• The subjective perspective is not enough to generate real and correct values as the reality may be defined incorrectly through only the author perspective
	• There are no standards for implementing this method	• Because of their subjectivity, the performance of risk management is difficult to follow
	• Need large time to handle the calculation process	• A cost-benefit analysis is not implemented, only a subjective approach which makes implementation of controls very difficult
	• The obtained results are introduced in the form of practical values which are hard to understand by the public without experience	• The accuracy of the estimation results is depending on the quality of risk management team

6.2 Expert judgment

When there is insufficient practical data to describe probability and impact of a certain incident, an expert judgment can be used to provide a subjective evaluation based on his/her experience through careful interviews.

Expert judgment is commonly utilized to measure uncertain parameters in a probabilistic form and to evaluates different elements of a certain model. Expert judgement can be defined as "*the expression of inferential opinions based on knowledge and experience*" [41].

Expert judgment is a powerful tool in risk analysis. It provides various solutions and decisions in several domains, such as psychology, criminal justice, financial forecasting, political science, and decision analysis. The use of expert judgement has raised many questions regarding the accuracy of the results; however, there are many circumstances where expert judgement is the only source of good information [41]. Measuring the probability of an incident in a risk analysis with the uncertainty that surrounds it is a difficult task especially for rare and extreme events. This is obviously true when trying to estimate security risks of access control operations [42].

6.3 Risk assessment

Risk assessment is used to study potential damages about a certain scenario. Risk assessment can be defined as the process of investigating possible losses using a combination of known information about the situation, and judgment about the information that is not known [43]. The risk assessment is used to identify the risk context and acceptable risk values in each situation. This can be achieved by comparing it to similar risks of similar scenarios. In addition, it aims to provide substitute solutions to reduce the risk and calculate the effectiveness of those solutions [44].

Determining the appropriate type of risk analysis depends on the available data that characterize the risk probability and its impact. An effective risk assessment has many benefits. For example, a well-established risk assessment can support a balanced basis to prevent the risk or at least reduce its impact. However, it is a subjective process that influenced by the experience and it only valid at a certain point in time [44].

6.4 Game theory

Game theory is considered as a division of applied mathematics that has been utilized in several areas like evolutionary biology, economics, artificial intelligence, political science, and information security. Game theory is used to describe multi-person decision scenarios in the form of games where each player select appropriate actions that lead to the best possible payoff while expecting reasonable actions from opponent players [45].

Game theory is the main tool for modelling and building automated decision-making operations in interactive environments. This is because it can provide consistent and mathematical platforms. The power of the game theory lies in the methodology it supports for analysing different problems of strategic choice. The process of modelling a condition as a game needs the decision-maker to interact with the players,

their strategic decisions, and observe their preferences and responses [46].

A game theory comprises of four components; the players, their strategies, payoffs and the information they have. The players are the essential part of the game, they are the decision makers within the game. While the strategy is the plan that the player uses regarding the movement of opposite player. So, it is critical for the players to select the suitable tactics. The payoff is the rewards of the players in the game. For each player, the payoff is affected by both their own actions and those of the other player [24]. In the game theory, the risk analysis is done by using user benefits rather than the probability. Moreover, game theory is recommended to be used in conditions where no practical data is available [46]. However, game theory is complex especially with more than two players. It also leads to random outcomes when using mixed strategies.

6.5 Decision tree

Decision tree is a common methodology for many operations in machine learning. It is used as a decision support instrument to provide decisions depending on a group of rules described as a tree [47]. Building a decision tree model requires dividing the data into training and validation sets. Training data are utilized to extract appropriate rules for the tree. While validating the tree and making required modifications are done using validation data.

Decision tree is represented as a flow diagram where each node, represented by a rectangle, describes the risk probability and its impact. These rectangles are connected by arrows such that each arrow leads to another box representing the percentage probability [47].

Decision tree approaches are easy to comprehend and significant for data classification. They can operate efficiently with inadequate data if experts provide all required rules. They can show all possible alternatives and traces in a single view which provide easier comparison with various alternatives. Whilst the decision tree model provides many advantages, it also has some limitations. For instance, its scalability is questionable such that when the scale of the tree increases, the obtained model will be hard to recognize and needs supplementary data to validate rules. Also, a decision tree model is based on expectations, so it may be impossible to plan for all contingencies that can arise as a result of a decision [48].

A comparison between different risk estimation approaches in terms of usability, time complexity, scalability, flexibility, subjectivity, and computing power requirements is shown in Table 2. It is clear that there is no straightforward approach that can be used without limitations. Also, a risk estimation approach without subjectivity will never exist in a risk estimation process. Scalability seems to be a problem in most approaches. Therefore, choosing the optimal risk estimation approach should depend heavily on the context.

7 Proposed risk estimation technique

There is no universal and best method for conducting a risk analysis. However, it is significant to identify strengths and weaknesses of various methods to decide the most appropriate approach regarding the context [49]. There are many questions about the way to choose the proper risk estimation method for the risk-based model. Understanding various advantages and disadvantages of previously discussed risk estimation approaches can facilitate the choice of the appropriate technique regarding the IoT context.

We propose the fuzzy logic system with expert judgment as to be the suitable risk estimation method to implement the proposed risk-based model for the IoT system, as shown in Fig. 4. Combining the fuzzy logic system with expert judgment can provide consistent and realistic risk values of various access control operations in the IoT. IoT contextual features will be collected with resource sensitivity, action severity, and risk history to evaluate the risk value related to the access request. In the absence of a dataset to represent risk probabilities and its impact, IoT domain experts will be used to provide predicted measures according to their knowledge and experience.

There are many reasons to consider the fuzzy logic system with expert judgment to conduct the risk estimation process of the proposed risk-based model. These reasons are described as follows:

- 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 the situation probability and its impact are required. Once data are available, it can be used to estimate a more precise risk value. Using the fuzzy logic system with expert judgment, there is no need for data since all required data will be provided by domain security experts.
- There are significant sources of subjective knowledge to provide the required information to estimate security risks associated with access control operations [50]. One of the most important sources is past experience. In other words, security experts in a specific context can have huge experiences about suitable rules and policies for the system. This valuable information can be converted easily into rules for the fuzzy inference system.
- There are many successful applications that used fuzzy logic systems such as decision support, management, engineering, psychology, medicine, and home appliances [51].
- The fuzzy logic system is flexible [52], so, it will be suitable for the IoT system to adapt to its changing conditions and situations.

Table 2 Benefits and limitations of risk estimation approaches

Risk estimation technique	Benefits					Limitations		
	Usable	Fast	Scalable	Dynamic	Include expert experience	Enormous resources needed	Time overhead	Subjective
Fuzzy logic system	✓			✓	✓		✓	✓
Expert judgment	✓	✓			✓			✓
Risk assessment		✓	✓		✓		✓	✓
Game theory	✓			✓		✓		✓
Decision tree		✓		✓	✓	✓	✓	✓

- Using the fuzzy logic system, the subjectivity can be reduced to an acceptable level because quantitative input data can be used so the subjectivity is moved to the process of creating rules, so it can be better controlled. Certainly, subjectivity is not completely eliminated. However, it is unlikely that a method without subjectivity will ever exist for a risk analysis [49].
- Expert judgment is a significant source of information in decision-making operations. This is because correct numerical data that describe incident frequencies and its impact do not exist in most risk-based models [41]. In some cases, quantifying the value of the risk using classical approaches is very complicated, but an expert judgment can provide a correct risk value for a specific scenario especially when appropriate experts are selected [53].
- Scalability of the fuzzy logic system is questionable and it requires significant time which can cause many issues especially it serves an access control model for the IoT which operates with thousands of thousands of users at the same time. However, artificial Neural Networks (ANNs) can be used after creating the appropriate dataset to overcome these challenges.

Although getting expert judgment can be done through group discussions, interviews provide a better way to collect valid and reliable data for the research [54]. Therefore, we intend to perform interviews with experts who have deep knowledge and expertise about the IoT security to implement the risk estimation process.

There are five stages to implement the fuzzy logic system with expert judgment to estimate security risks of the proposed risk-based model.

The first stage is Fuzzification. This stage is concerned with converting classical logic into fuzzy linguistic variables. In other words, risk factors are converted into linguistic variables that can be easily understood. We decided to use three fuzzy sets for the input risk factors. So that, Low, Moderate and High fuzzy sets will be used to represent the action severity, user context and risk history. While Not Sensitive, Sensitive and Highly Sensitive fuzzy sets will be used to represent the resource sensitivity. For the output, we have decided to use five fuzzy sets; Negligible, Low, Moderate, High, and Unacceptable High.

The second stage is setting the range of each fuzzy set. After identifying the appropriate number of fuzzy sets of each risk factor, the range of each fuzzy set should be determined. We will use IoT security experts to determine the range of fuzzy sets.

The third stage is choosing the appropriate Membership Function (MF) to represent the relationship between the input risk factors and the output risk. Fuzzy MF represents relationships between variables and how each point is mapped to a membership value between zero and 1 in the universe of discourse [55]. In practice, MFs can have different types such as

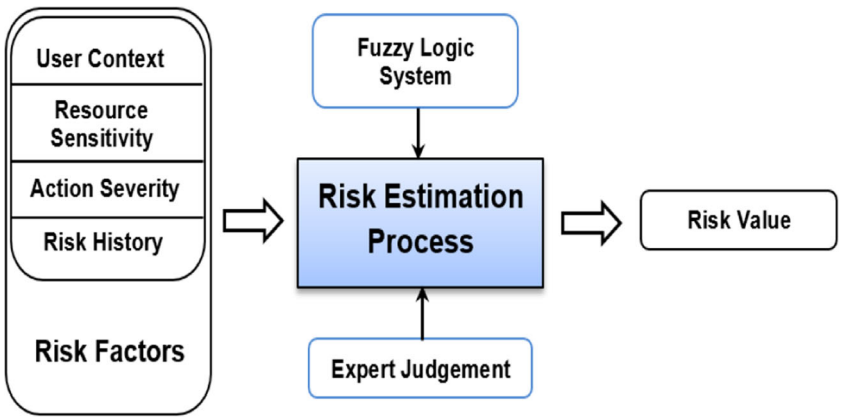

Fig. 4 Proposed risk estimation technique

trapezoidal, Gaussian, triangular, sigmoidal, and bell-shaped waveforms. Choosing the appropriate MF is based on the available dataset such that comparing results of training data with the real data and calculating error values using Mean Average Percentage Error (MAPE) can ensure choosing the appropriate MF. Due to the lack of a dataset in our research, triangular MF will be used to represent input and output fuzzy sets of the proposed risk-based model. This is because it represents expert knowledge efficiently and simplifies calculation process.

The fourth stage is fuzzy rules. After specifying risk factors and its fuzzy sets, it is necessary to define how the output risk changes regarding input risk factors [23]. Fuzzy rules act as the knowledge base of the fuzzy logic system. It is defined using a set of IF-THEN statements to describe actions or outputs that should be taken for a certain input combination [39]. The fuzzy IF-THEN rule uses linguistic variables to describe the relationship between a certain condition and an output or a conclusion. The IF part is used to represent the condition, and the THEN part is used to represent the output in a linguistic form [39].

Specifying accurate and efficient fuzzy rules require taking into account different risk factors and how they behave as a combination to produce the output risk. Therefore, IoT security experts will be used to provide appropriate fuzzy rules based on their knowledge and experience.

The final stage is defuzzification. Defuzzification is used to convert the fuzzy variable into a crisp variable [40]. There are many defuzzification methods such as mean of maximum, centre of area (centroid), modified centre of area, height method, centre of sum, and centre of maximum. We will use the centroid method as it provides the best accuracy and performance.

8 Conclusion

The IoT has attracted the attention of experts, specialists and researchers in both academia and industry. This is because it can provide unlimited capabilities that can help in our daily life activities. The IoT has the ability to connect billions of devices/objects and provide a real-world intelligent platform to collaborate and communicate with these objects through wireless or wired networks. The IoT has brought unlimited benefits, but at the same time raises several security issues. This is because current access control models with rigid and static structure and predefined rules that always give the same result in different situations cannot provide the required level of security for the IoT system. Therefore, this paper has presented an adaptive and dynamic risk-based access control model. This model uses IoT real-time and contextual information associated with the access request to determine the access decision automatically. The proposed model uses user attributes collected while making the access request, sensitivity of data to be accessed, severity of actions to be performed and user risk history as inputs to estimate the risk value regarding each access request. To add abnormality detection capabilities, smart contracts are used to track user's activities throughout the access session to detect and prevent malicious attacks from authorized users. In addition, as the essential stage to build a risk-based model is choosing the optimal risk estimation technique, we discussed most common risk estimation methods that are used in related risk-based models, then we proposed the fuzzy logic system with expert judgment as to be the optimal approach to handle risk estimation process of the proposed risk-model. In the future work, we will perform interviews with IoT security experts to determine ranges of fuzzy sets and fuzzy rules to implement the risk estimation process.

References

1. Li S, Da Xu L, Zhao S (2015) The Internet of Things: a survey. Inf Syst Front 17(2):243–259
2. Elkhodr M, Shahrestani S, Cheung H (2013) The Internet of Things: vision & challenges. IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc., p 218–222
3. Atlam HF, Walters RJ, Wills GB (2018) Fog computing and the Internet of Things: a review. Big data Cogn Comput 2(2):1–18
4. Ashton K (2009) That 'Internet of Things' thing. RFID J 4986
5. ITU (2005) The Internet of Things. Itu Internet Rep 2005:212
6. ITU (2012) Overview of the Internet of things. Ser. Y Glob. Inf. infrastructure, Internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model., p. 22
7. Habib K, Leister W (2015) Context-aware authentication for the Internet of Things. Elev Int Conf Auton Auton Syst Fined 134–139
8. Dos Santos DR, Westphall CM, Westphall CB (2014) 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, p 1–9
9. Liu JK, Au MH, Huang X, Lu R, Li J (2016) Fine-grained two-factor access control for web-based cloud computing services. IEEE Trans Inf Forensics Secur 11(3):484–497
10. Castiglione A et al (2016) Hierarchical and shared access control. IEEE Trans Inf Forensics Secur 11(4):850–865
11. Shen J, Zhou T, Chen X, Li J, Susilo W (2018) Anonymous and traceable group data sharing in cloud computing. IEEE Trans Inf Forensics Secur 13(4):912–925
12. Wang H, Zheng Z, Wu L, Li P (2017) New directly revocable attribute-based encryption scheme and its application in cloud storage environment. Clust Comput 20(3):2385–2392

13. Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y (2018) An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access X(X):1–8
14. 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 Symp. Secur. Privacy(SP'07), p 222–227
15. Shaikh RA, Adi K, Logrippo L (2012) Dynamic risk-based decision methods for access control systems. Comput Secur 31(4):447–464
16. Atlam HF, Alassafi MO, Alenezi A, Walters RJ, Wills GB (2018) XACML for building access control policies in Internet of Things. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)
17. Jason C (2004) Horizontal integration: broader access models for realizing information dominance. MITRE Corp. Tech. Rep. JSR- 04-132
18. McGraw R (2009) Risk-Adaptable Access Control (RAdAC). In: Privilege Manag. Work. NIST–National Inst. Stand. Technol. Technol. Lab
19. Zhang L, Brodsky A, Jajodia S (2006) Toward information sharing: benefit and risk access control (barac). In: the Proc. of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks. Washington, DC, USA, p 45–53
20. Diep NN, Hung LX, Zhung Y, Lee S, Lee Y, Lee H (2007) Enforcing access control using risk assessment. Fourth Eur. Conf. Univers. Multiservice Networks, p 419–424
21. Khambhammettu H, Boulares S, Adi K, Logrippo L (2013) A framework for risk assessment in access control systems. Comput Secur 39:86–103
22. Ni Q, Bertino E, Lobo J (2010) 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, p 250–260
23. Li J, Bai Y, Zaman N (2013) A fuzzy modeling approach for risk-based access control in eHealth cloud. Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013, p 17–23
24. Rajbhandari L, Snekkenes EA (2011) Using game theory to analyze risk to privacy: an initial insight. Priv. Identity Manag. Life, Springer Berlin Heidelb., p 41–51
25. Sharma M, Bai Y, Chung S, Dai L (2012) 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., p 1047–1052
26. Wang Q, Jin H (2011) Quantified risk-adaptive access control for patient privacy protection in health information systems, the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China
27. 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), p 254–260
28. Farroha B, Farroha D (2012) Challenges of 'operationalizing' dynamic system access control: Transitioning from ABAC to RAdAC. Syst. Conf. (SysCon), 2012 IEEE Int., p 1–7
29. Ouaddah A, Bouij-Pasquier I, Abou Elkalam A, Ait Ouahman A (2015) Security analysis and proposal of new access control model in the Internet of Thing. 2015 Int. Conf. Electr. Inf. Technol., p30–35
30. Li J, Zhang Y, Chen X, Xiang Y (2018) Secure attribute-based data sharing for resource-limited users in cloud computing. Comput Secur 72:1–12
31. Atlam HF, Alenezi A, Alharthi A, Walters R, Wills G (2017) 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), no. June, p 670–675
32. Li J, Huang X, Li J, Chen X, Xiang Y (2014) Securely outsourcing attribute-based encryption with checkability. IEEE Trans Parallel Distrib Syst 25(8):2201–2210
33. Hernández-Ramos J, Jara A (2013) Distributed capability-based access control for The Internet of Things. J Internet Serv Inf Secur 3:1–16
34. Wang Q, Jin H (2011) Quantified risk-adaptive access control for patient privacy protection in health information systems. Proc. 6th ACM Symp. Information, Comput. Commun. Secur. - ASIACCS '11, p 406–410
35. Li Y, Sun H, Chen Z, Ren J, Luo H (2008) Using trust and risk in access control for grid environment. Secur. Technol. 2008. SECTECH '08. Int. Conf., p 13–16
36. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J (2016) Blockchain contract: securing a blockchain applied to smart contracts. 2016 IEEE Int. Conf. Consum. Electron., p 467–468
37. Yin J, Tang C, Zhang X, McIntosh M (2006) On estimating the security risks of composite software services. In: In First Program Analysis for Security and Safety Workshop Discussion (PASSWORD 2006)
38. Ramona SE (2011) Advantages and disadvantages of quantitative and qualitative information risk approaches. Chinese Bus Rev 10(12):1106–1110
39. Bai Y, Wang D (1982) Fundamentals of fuzzy logic control – fuzzy sets, fuzzy rules and defuzzifications. Adv Fuzzy Log Technol Ind Appl 17–36
40. Kose U (2012) Fundamentals of fuzzy logic with an easy-to-use, interactive fuzzy control application. Int J Mod Eng Res 2(3):1198–1203
41. Leung K, Verga S (2007) Expert judgement in risk assessment expert judgement in risk assessment. Def. R&D Canada Cent. Oper. Res. Anal., no. December, p 321–354
42. Turisová R, Mihok J, Kádárová J (2012) Verification of the risk assessment model through an expert judgment. Kval. Inovacia Prosper. Qual Innov Prosper 37–48
43. Shapiro A, Koissi M (2015) Risk assessment applications of fuzzy logic, no. March. Casualty Actuarial Society, Canadian Institute of Actuaries
44. Stoneburner G, Goguen A, Feringa A (2002) Risk management guide for information technology systems. Nist Spec Publ Sp 30:30
45. Binmore K, Vulkan N (1999) Applying game theory to automated negotiation. Econ Res Electron Netw 1:1–9
46. Hamdi M, Abie H (2014) Game-based adaptive security in The Internet of Things for eHealth. 2014 IEEE Int Conf Commun ICC 2014, p 920–925
47. Shang K, Hossen Z (2013) Applying fuzzy logic to risk assessment and decision-making. Casualty Actuar. Soc. Can. Inst. Actuar. Soc. Actuar., p 1–59
48. Wang S, Fan C, Hsu CH, Sun Q, Yang F (2016) A vertical handoff method via self-selection decision tree for internet of vehicles. IEEE Syst J 10(3):1183–1192
49. Boc K (2012) 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". 12: 234–239
50. Alberts CJ, Dorofee A (2002) Managing information security risks: the octave approach. Addison-Wesley Longman Publishing Co., Inc., Boston
51. Zadeh LA (1975) The concept of a linguistic variable and its applications to approximate reasoning. Inf Sci (Ny) 8(4):199–249
52. Ruan D (2000) Fuzzy sets and fuzzy information granulation theory. Bejing Normal Univeristy Press, Bejing
53. Pluess D, Groso A, Meyer T (2013) Expert Judegement in risk analysis: a strategy to overcome Uncertainities. Chem Eng Trans 31:307–312
54. Bolderston A (2012) Conducting a research interview. J Med Imaging Radiat Sci 43:66–76
55. Ross TJ (2010) Fuzzy logic with engineering applications. John Wiley & Sons, Ltd