I. J. Computer Network and Information Security, **2018, 1, 26-35**
Published Online January 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.01.04

Validation of an Adaptive Risk-based Access Control Model for the Internet of Things

Hany F. Atlam*[1, 2], Ahmed Alenezi[1], Raid Khalid Hussein[1], Gary B. Wills[1]
[1]Electronics and Computer Science Dept., University of Southampton, Southampton, UK
[2]Computer Science and Engineering Dept., Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt
E-mail: {hfa1g15, aa4e15, rkh2n14, gbw}@soton.ac.uk

Received: 20 June 2017; Accepted: 07 November 2017; Published: 08 January 2018

***Abstract*—**The Internet of Things (IoT) has spread into multiple dimensions that incorporate different physical and virtual things. These things are connected together using different communication technologies to provide unlimited services. These services help not only to improve the quality of our daily lives, but also to provide a communication platform for increasing object collaboration and information sharing. Like all new technologies, the IoT has many security challenges that stand as a barrier to the successful implementation of IoT applications. These challenges are more complicated due to the dynamic and heterogeneous nature of IoT systems. However, authentication and access control models can be used to address the security issue in the IoT. To increase information sharing and availability, the IoT requires a dynamic access control model that takes not only access policies but also real-time contextual information into account when making access decisions. One of the dynamic features is the security risk. This paper proposes an Adaptive Risk-Based Access Control (AdRBAC) model for the IoT and discusses its validation using expert reviews. The proposed AdRBAC model conducts a risk analysis to estimate the security risk value associated with each access request when making an access decision. This model has four inputs/risk factors: user context, resource sensitivity, action severity and risk history. These risk factors are used to estimate a risk value associated with the access request to make the access decision. To provide the adaptive features, smart contracts will be used to monitor the user behaviour during access sessions to detect any malicious actions from the granted users. To validate and refine the proposed model, twenty IoT security experts from inside and outside the UK were interviewed. The experts have suggested valuable information that will help to specify the appropriate risk factors and risk estimation technique for implantation of the AdRBAC model.

***Index Terms*—**Security, Internet of Things, Risk, access control, Adaptive, Context, Validation.

I. INTRODUCTION

The IoT has become able to provide a real-world intelligent platform to increase the collaboration of distributed smart objects through different communication technologies. It extends the interaction between humans and applications through objects, which can be users or applications [1]. The IoT has the potential to add a new dimension by enabling communications with and among smart objects, thus leading to the vision of ‘‘anytime, anywhere, anything” communications [2], [3].

The concept of the IoT was first mentioned by Kevin Ashton in 1999 [4]. He has said, “The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so”. Later, the International Telecommunication Union (ITU) IoT formally presented the IoT in 2005 [5]. The ITU defines it 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].

Security is one of the most difficult of the challenges that need to be addressed in the IoT. This challenge is more complicated due to the dynamic and heterogeneous nature of IoT systems [6], [7]. Authentication and access control models are the essential elements to address the security issue in the IoT. They can prevent unauthorised users from gaining access to system resources, prevent authorised users from accessing resources in an unauthorised manner and allow authorised users to access resources in an authorised manner [8], [9].

The main purpose of access control is to reject unauthorised users and limit operations of authorised users using a certain resource. In addition, it tries to prevent activity that could cause a security breach [8]. A powerful access control model should fulfil security requirements of confidentiality, integrity, and availability [11], [12].

There are two categories of access control models; traditional and dynamic approaches. Traditional access control approaches are static in nature as they depend on predefined policies that always give the same outcome regardless of the situation. They are context insensitive. Furthermore, they require a rigid authentication infrastructure [11], [12]. So they cannot provide for distributed and dynamic environments as IoT systems [15], [16]. On the other hand, dynamic access control approaches are more appropriate to the IoT. This is because they are characterised by using not only access policies but also environment features that are estimated in real-time to determine access decisions. These dynamic features can include trust, risk, context, history and operational need [15].

The risk-based access control model is one of the dynamic models that uses the security risk associated with the access request to make the access decision. This paper proposes an Adaptive Risk-Based Access Control (AdRBAC) model for the IoT. This model uses real-time user contextual features, resource sensitivity, action severity and risk history as inputs to estimate the security risk value of each access request to make the access decision. In current risk-based access control models, there is no way to detect malicious actions from granted users during the access session. While the proposed model will monitor the user behaviour during the access session to detect any abnormal or malicious actions. To prove the research concept, Twenty IoT security domain experts have validated and refined the proposed model.

The rest of the paper is organized as follows: related models will be discussed in Section II; IoT security challenges will be presented in Section III; Section IV will discuss the access control in the IoT; risk-based access control model will be presented in Section V; Section VI will present access control requirement that needed to implement an access control model for the IoT; Section VII presents the proposed model; Section VIII discusses the validation of the proposed model; Section IX provides a discussion; and Section X is the conclusion.

II. RELATED WORK

A number of studies have used the security risk for dynamic access control models. The JASON report [18] has proposed three main components for a risk-based access control model: estimating the risk value associated with the access request, identifying acceptance levels of the risk, and controlling information sharing based on the estimated risk value and access control policies.

McGraw [19] has proposed a Risk Adaptable Access Control (RAdAC) model. This model estimates the security risk and operational needs to make the access decision. It estimates the risk associated with the access request and then compares it with the access control policy and operational needs to make the final access decision. However, this model does not provide details about how to estimate risk and operational needs quantitatively. Also, it lacked adaptive features. In addition, Kandala et al. [20] have provided an approach that identifies different risk components of the RAdAC model using attribute-based access control approach.

A dynamic and flexible risk-based access control model has been proposed by Diep et al. [14]. This model uses the risk assessment to estimate the risk value associated with the access request depending on outcomes of actions in terms of availability, confidentiality, and integrity. However, this model does not provide how to evaluate the risk value for each state of the environment and for each outcome of action and lacks risk adaptive features.

Khambhammettu et al. [21] have proposed a framework based on estimating object sensitivity, subject trustworthiness, and the difference between the object sensitivity and the subject trustworthiness using a risk assessment. However, this framework does not provide how to estimate the risk value for each situation of the environment. Besides, it requires a system administrator to give a reasonable value for each input feature in the early state of the risk assessment process and lacked risk adaptive features as well.

A task-based access control model has been proposed by Sharma et al. [22] to estimate the risk value associated with the access request using functions based on the actions a user wants to perform. The risk value is computed in terms of different actions and corresponding outcomes. The outcomes and the risk probability are determined along with the level of data sensitivity. The users' previous behaviour patterns are then used to estimate the overall risk value. The estimated risk value is compared with the risk threshold to determine the access decision. However, this model does not use real-time features in the risk estimation process and lacks risk adaptive features.

A contextual risk-based access control model has been proposed by Lee et al. [15]. This model gathers all useful information from the environment and evaluates them from the security perspective. Risk assessment with Multifactor Evaluation Process (MFEP) is applied to estimate the associated risk value. The risk value is based on outcomes of actions in term of availability, confidentiality, and integrity. This model is evaluated to manage the access control in a hospital. However, this model ignored the users' past behaviour and also lacks risk adaptive features.

A risk-based access control model has been proposed by Dos Santos et al. [8]. This model employs the notion of quantifying risk metrics and aggregating them. It is based on the idea of risk policies, which allow service providers and resource owners to define their own metrics, allowing greater flexibility to the access control system. However, this model requires a system administrator to ensure the minimum security is achieved. In addition, it does not use real-time features in the risk estimation process and lacks risk adaptive features as well.

In summary, current risk-based access control models concentrate only on providing access decisions without providing any way to prevent any abnormal and unusual data access from authorised users, unlike the proposed model which is based on providing the access decision and then monitoring user behaviour during the access session to detect any abnormal actions. The novelty of the proposed model is based on providing the adaptive features and using real-time access features to make the access decision, which provides more flexibility in accessing system resources and incorporate unconditional situations. To the best of the researcher knowledge, the proposed model will be the first to use smart contracts to monitor the user access behaviour during access sessions. The proposed AdRBAC model has been validated and refined using Twenty IoT security experts that will ensure it will be implemented correctly.

III. IoT Security Challenges

Although benefits of the IoT are countless, like all new technologies, it introduces many security challenges that include malicious actors manipulating the flow of information or tampering with IoT devices themselves. There are variety of IoT security challenges that need to be addressed. These challenges include:

- **User Privacy**: Privacy is one of the most sensitive issues in the IoT system. This is because IoT devices collect various sensitive personal information like financial accounts, user habits, geo-locations, physical condition and many others that can affect the user privacy that should be protected [1].
- **Large Scale**: Many IoT devices are designed to be deployed at a massive scale that is beyond traditional Internet-connected devices. Therefore, the potential quantity of interconnected links between these devices in a dynamic manner is unprecedented. Existing tools and strategies associated with the IoT security need new consideration [23].
- **Identity Management**: Due to the large number of IoT devices, which are in billions, an efficient and lightweight identity management scheme is needed. Because of the distributed nature of the IoT, this issue is more complicated [24].
- **End-to-End Security**: Establishing an efficient security technique between IoT devices and Internet users is an important issue. Standard cryptographic solutions are not sufficient, so future research should focus on developing an efficient end-to-end security measure [25].
- **Attack Resistant Security Solution**: Due to the diversity of IoT devices and users, the attack resistant security measures should be implemented. All devices in IoT have low computation resources and low memory; hence, they are defenceless. Possible external attacks like Denial of Service attack, flood attack and other attacks on devices have to be considered. A mitigation plan to address these attacks is another big issue [24].
- **Authentication and Access Control**: Authentication is identity evidence between communicating parties. Since there are billions of IoT devices, authentication and access control are important to create a secure communication channel between different devices and services [9].
- **Physical Security**: Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Physical access to IoT devices may be achieved easily by attackers. Anti-tamper tools and other design innovations will need to be considered to increase the physical security of IoT devices [23].
- **Device Usability**: IoT devices might have no clear way to alert the owner when a security breach arises making it difficult for a user to know that a security breach has occurred. A security breach might last for a long time before being observed and corrected. Similarly, the user might not be aware that a sensor exists in his/her surroundings, potentially allowing a security breach to persist for long periods without detection [23].

In this paper, the access control issue will be addressed. Building a dynamic access control model for the IoT is one of the important things that are needed to establish a secure communication channel not only between IoT devices and users but also between IoT objects and each other.

IV. Access Control in the IoT

The main functions of the access control are to grant access rights only to authorised users and to prevent authorised users from accessing system resources in an unauthorised manner [8]. A powerful access control model should also fulfil security demands of confidentiality, integrity, and availability [11].

IoT devices send and receive a variety of information about the owner's behaviour. Therefore, it is important to protect not only the communication process between IoT devices but also authentication and access control of IoT devices itself [25], [27]. The access control process works with many layers of the IoT. It works with different data whether in storage, in motion, or at the IoT device itself. Therefore, access control is a big issue in the IoT that needs addressing.

There are many access control models, which can be divided into two categories; traditional and dynamic. Traditional access control (also called classical access control) models are static in nature as they depend on predefined policies that always give the same outcome regardless of the situation. They are context insensitive. Furthermore, they require a rigid authentication infrastructure [13], [14]. There are three main traditional access control models; Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-based Access Control (RBAC).

DAC model is designed for multi-user databases and systems with few previously known users. All system resources are under full control from the user. DAC grants access depending on the user identity and authorization are defined through open policies. The owner of the resource can grant the access to any user. DAC mainly deals with the inheritance of permissions, user-based authorization, auditing of system events and administrative privileges [28].

MAC model is concerned with confidentiality and integrity of information and is mainly used in military and government applications. In MAC, the security policy is controlled by a security policy administrator and the user does not have the capability to override it [28].

RBAC model consists of three elements: users (subjects requesting access), roles (collection of permissions) and operations (actions on target resource). Access permissions are related to roles and the appropriate role is granted to the user. A single user can be associated with one or more roles, and a single role can include one or more user. RBAC classifies users based on their roles [29].

Dynamic access control models are characterised by the use of not only the access policies but also dynamic contextual features which are estimated in real-time at the time of making the access request [30]. Features that can be taken into account in dynamic access control models can include risk, need, benefit, trust and context. The dynamic nature of the access control is implemented in these models because access decisions vary according to contextual information and features that are evaluated at the time of the access request [31], [32].

The AdRBAC model is proposed to provide more flexibility in accessing system resources. The security risk value associated with the access request will be used as the main criterion for making access decisions.

V. Risk-based Access Control Model

The risk is generally defined as the potential damage that can occur from an incident and is usually represented by the probability of occurrence of an undesired incident multiplied by its impact. Risk metrics are used to quantify assets, threats and vulnerabilities of a certain system. Furthermore, the risk is different from uncertainty, since the risk can be measured and managed [8]. Risk-based access control models permit or deny access requests dynamically based on the estimated risk of each access request [33]. AdRBAC performs a risk analysis on each user access request to make the access decision. This analysis can be qualitative or quantitative, automatically attributing a numeric value to risk [8]. Mathematically, the most common formula to represent the risk in quantitative terms is:

$$QuantifiedRisk = Likelihood * impact \quad (1)$$

Where likelihood represents the probability of an incident to happen while impact represents the estimation of the value of the damage regarding that incident [33].

The fundamental distinction between adaptive and non-adaptive access control models is that the adaptive model requires a system monitoring process to adaptively adjusts user permissions based on the users' activities during the access session [13]. If a malicious action is detected, the access session will be terminated or the user permissions will be reduced.

Before discussing the proposed AdRBAC model and its validation by security domain experts, the requirements that should be taken into consideration when designing an access control model for the IoT will be presented to discuss how the proposed model considers these requirements.

VI. Access Control Requirements in the IoT

Due to the distributed and dynamic nature of the IoT, there are many requirements to implement an access control model for the IoT. According to [34], [35] requirements include;

1. **Interoperability with multiple users**: Access control policies should be designed to support multiple organisations. For instance, each organisation creates its own policies and respects other collaborating organisation's policies.
2. **Dynamic interaction**: Access control policies should be predictable and specified in a dynamic and continuous way by considering context changing during the access control process.
3. **Context awareness**: The context is considered one of the core features in the IoT since it enables intelligent interactions between users and devices. Using the context will permit access decisions determined dynamically based on surrounding environment features.
4. **Usability**: The access control model should be easily administrated, expressed and modified. It also should provide easy to use interfaces for both consumers and devices.
5. **Limited resources**: The resources associated with IoT devices such as energy, memory, and processing power are limited due to devices lightweight. Therefore, the access control model designed for the loT should support efficient solutions.
6. **Scalability**: The IoT connects billions of devices. The access control model should be extensible in size, structure, and number of devices without affecting the system performance.
7. **Delegation of authority**: In many IoT scenarios, many devices are operating on behalf of a user and other scenarios where a device may operate on a third party's behalf for a specific period. The access control model should implement delegation of authority to provide more usability and flexibility for the IoT system.
8. **Auditability**: All access control models need to be auditable. Hence, collection and storage of evidence are necessary for context awareness. This becomes a challenge when utilising a distributed approach.

VII. Proposed Model

Dynamic access control approaches use real-time environment features to make the access decision. One of these features is the security risk associated with the access request, which is the building block of the risk-based access control model. This model performs a risk analysis to make the access decision.

The proposed AdRBAC model has four inputs as shown in Fig.1, user/agent context, resource sensitivity, action severity and risk history. These inputs/risk factors are used to estimate the security risk associated with each access request. The estimated risk value is then compared against the risk policies to make the access decision. To provide the adaptive features, the user behaviour will be monitored to detect any abnormal actions from granted users during the access session. This model will provide an appropriate security level while ensuring flexibility and scalability to the IoT system.

In addition, the proposed model can work well in applications where unexpected situations often require the violation of security policies. This may occur because policies are incomplete or incoherent, sometimes even conflicting. The most usual examples of such needs are in medical and military applications, where the need to take actions may save lives and system immobility may cause serious harm [8].

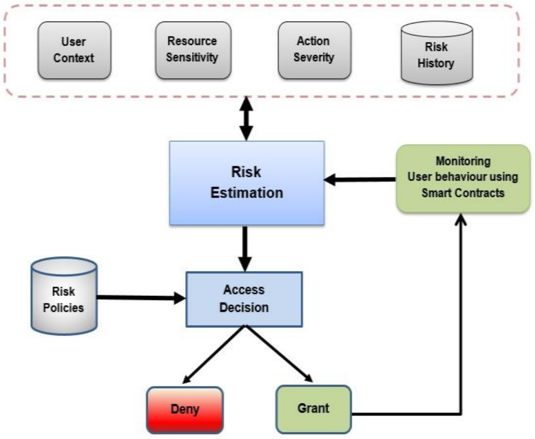

Fig.1. The Proposed Adaptive Risk-based Access Control Model.

As shown in Fig.1, the user/agent context represents the environmental features that are embedded with the user/agent at the time of making the access request. With the IoT, there are many sensors that can be used to collect variety of context features during making the access request. These contexts are used to determine the security risk value associated with the user requesting the access to the system. Location and time are the most common user contexts [36]. The agent is used to express on the diversity of applications in IoT systems. An agent represents any system entity that has the ability to make an access request [37]. For the rest of the paper, the user will be used to represent either user or agent.

Resource sensitivity represents how valuable the resource/data is to the owner. Data has different sensitivity levels based on who should have access to it and how much damage would be done if it were disclosed. A risk metric is assigned to each resource in the IoT system depending on how valuable the resource data is to the owner. For instance, the higher the data sensitivity, the higher the risk metric associated with the resource [34].

Action severity represents the consequences of a certain action on a particular resource in terms of security requirements of confidentiality, integrity, and availability. Different operations have different impacts and so have different risk values. For instance, the risk of a “view” operation is lower than the risk of a “delete” operation [38], [39].

The risk history is used to represent the user previous risk values on a certain resource. This is because the risk history reflects previous users’ behaviour patterns. Moreover, it is used to identify good and bad authorised users and predict the user future behaviour [34].

Risk estimation module is the essential part of the risk-based access control model. It is responsible for taking the input features and quantify the risk value associated with the access request. Determining the security risk associated with each access request is a complex task, which requires the consideration of a variety of factors [21]. However, the ultimate goal is to develop an efficient risk estimation process.

The access decision determines whether the access is granted or denied according to the risk policies. Risk policies or access control policies are mainly used by the risk estimation module to make the access decisions. These policies are created by the resource owner to identify terms and conditions of granting or denying the access. The overall risk value is compared against risk policies to determine the access decision.

The proposed model is trying to improve the security levels of access control by monitoring the user behaviour during the access session. In current risk-based access control models, if the decision is to grant access to the user, then there is no way to prevent any abnormal and unusual data access from authorised users during access sessions. So, a monitoring module is needed to adaptively adjust risk values based on the user behaviour during the access session. Preventing malicious actions during the access session is the primary goal of the monitoring module so that the target of the proposed model is to increase information sharing and availability but at the same time prevent any malicious attack to guarantee the integrity and confidentiality of the data.

Applying smart contracts to accomplish the monitoring process is a big challenge especially as it will be the first use of smart contracts in this context. Smart contracts are treated as software code that runs on a blockchain [40]. It can force a functional implementation of particular demands and can confirm that certain conditions or terms were met or not [41], [42]. Hence, the monitored user behaviour information will be compared with the smart contract to ensure that the user acts according to the terms of the smart contract so as to prevent any potential security breach during the access sessions.

The proposed AdRBAC model tries to achieve the requirements that are needed to implement an access control model for the IoT system that are stated in section VI. How the proposed model addresses these requirements is outlined in Table 1.

Table 1. Considering Access Control Requirements through the Proposed Model

Requirements of access control	Proposed AdRBAC Model
Interoperability with multiple users	To support interoperability, the risk policies will be designed using real-time contextual features that change dynamically. Therefore, risk policies will be more flexible and will have the ability to work with multiple organisations and users.
Dynamic interaction	The proposed model provides a dynamic and flexible access control model for IoT applications. It uses real-time contextual features to make the access decision. Therefore, the access decision is dynamically changes based on collected environment features.
Context awareness	The proposed model uses real-time contextual features collected from IoT environment to make the access decision. Therefore, the proposed model is a risk aware model that takes context awareness of surrounding environment to make the access decision.
Usability	The implementation of the proposed model should consider building usable interfaces that can easily be administrated and modified.
Limited resources	The proposed model will employ the centralised and contextual access control architecture where IoT devices participate in access decisions. The access control logic will be implemented at a central server with all required resource capabilities. IoT contextual features will be sent to the central entity to help to make access decisions. Therefore, the resource limitations will not be a problem.
Scalability	The proposed model is for IoT devices, which are in billions, therefore, the design of risk estimation module and risk policies should take into consideration the increasing number of IoT devices.
Delegation of authority	The proposed model provides more flexibility by using real-time contextual features to build risk policies. Therefore, it can consider delegation of authorities, especially in unexpected situations.
Auditability	The proposed model involves a monitoring module to record and monitor all activities performed by the granted user during the access session.

VIII. Validation of Proposed Model

Validating the proposed AdRBAC model is essential to ensure any implementation will be appropriate. One of the most popular ways to validate a model is through an expert review, which is a qualitative approach [43]. The use of the expert interviews permits the collection of valid and reliable data that are relevant to the research to refine it in the light of the opinions of well-qualified experts.

A. Interview Design

The expert review is used to gain an understanding of underlying reasons, opinions and motivations in the research area. It does not use statistical procedures or other means of quantification [44].

The proposed model was validated through expert interviews. The purpose of the interview was to get more information about the model from highly experienced persons who have skills and experiences in IoT security. The interview was semi-structured, which starts with a set of predetermined open questions with other questions emerging from the dialogue during the interview, by either the interviewer or interviewee [45].

The interview questions were pilot-tested by seven security research fellows in the University of Southampton. Based on this pre-test, it was decided to give an open question to ask how reasonable the methodology followed by the researcher.

To interact directly with the interviewees and provide further questions based on the interviewees' answerers, face-to-face interviews were used [16]. The interviews were conducted on the campus of the University of Southampton in expert's office. Other interviews were conducted online using video conferencing on Skype [46] and were recorded by an audio recorder or taking notes manually. All interviews were conducted in the English language.

B. Ethics Approval

Before starting the interview, each expert was asked to sign a consent form after reading the participant information sheet that included all the necessary information, terms and conditions about the study. The University of Southampton Ethics Committee granted approval for this study under their reference number 25091.

C. Demographic Information

In terms of the number of experts, according to Guest et al. [47], there is no agreed-upon number of experts for an interview in a content validity study. However, most researchers recommend a panel consisting of 3 to 15 experts. In expert sampling, participants are chosen based on their knowledge in the area of study [48].

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 a relevancy between their work and this study. While other experts are selected depending on their holding posts that require experience in security and IoT applications. Information on experts who have involved in this study are shown in Table 2. Most experts had extensive experience in security and IoT applications and 2- 5 years of experience.

Table 2. Attributes of IoT security Experts Who Validate the Proposed Model

Expert No	Job Description	Experience (Years)
E 1	IoT Security researcher	6 – 10
E 2	Senior Cybersecurity Engineer/Architect	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/Architect	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

D. *Results and Findings*

The need for access control models that provide more flexibility than traditional approaches has been pointed out repeatedly in recent years especially after the appearance of IoT. The risk-based access control model provides a dynamic way to make the access decision. It uses the risk associated with the access request as a criterion to determine the access decision.

The AdRBAC model has been refined and validated using IoT security domain experts through interviews. The purpose of the expert interviews was to validate the model and the strategy proposed by the researcher to implement it. Before interview questions were asked, each expert was given a brief background about the aim of the research. After the research had been outlined, six open-ended questions were asked to the experts.

The first question was about their feedback about the model in general. Most experts have interested in the model from the first moment I explained it to them. They confirmed that it will be valuable to industry and advised trying to contact interested companies to get more support to complete the research.

With regards the next question, experts were asked to validate the four risk factors that will be used to estimate the security risk associated with the access request in IoT applications. The majority of experts agreed that the proposed risk factors are appropriate to different IoT applications, especially the user context that allows the access control system to use the real-time contextual information to make the access decision. In addition, they added that the proposed risk factors could be used with different IoT applications without any problems. However, they 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 specific IoT application besides the proposed four risk factors. We believe that one of the powerful points of the 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.

In the subsequent question, experts were asked about the ranking of risk factors in terms of importance to determine the final access decision. Most experts decided that all risk factors used in the proposed model are important. However, they considered the resource sensitivity and the risk history are the most effective risk factors, then the action severity and the user context. On the other hand, some experts suggested that the ranking of risk factors should be regarding a specific application. In other words, the ranking of risk factors may need to be changed according to the application domain. For instance, for sensitive applications, the resource sensitivity and action severity would be more important.

After that, experts were asked about appropriate risk estimation techniques to be used to implement the model and estimate the value of the security risk associated with each access request. The majority of experts decided that identifying the appropriate risk estimation approach is the essential and difficult stage to implement the model. This is because risk estimation tries to predict the future in terms of probability of occurrence of a certain incident and its impact. They added that estimating the risk without having dataset describing different probabilities and the impact of different access control scenarios would make estimating the risk more difficult. Experts suggested reviewing different risk estimation techniques that were used in existing risk-based access control models. The researcher has reviewed different risk estimation approaches in this paper [49].

In addition, many experts suggested using fuzzy logic approach. However, they advised trying to reduce the subjectivity associated with the fuzzy logic system. 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 ANN to get high performance, but this only applies when there is an available dataset.

For the next question, the experts were asked about the effectiveness of adding the adaptive features into the model such that after granting the access, the access session will be monitored. Most of the experts were interested in it and recommended it be implemented, together with a mitigation plan to mitigate against different attacks and malicious actions during the access session. In addition, they have added that the response time to detect and prevent the attack or malicious action should be considered. On the other hand, some experts felt that although monitoring the user access session is important, it violates the user privacy especially the owner of the IoT device. Therefore, they advised dividing the grant band into two bands, one without monitoring for the users who have very low security risk values and one with monitoring for the users who have security risk values less than the threshold risk value.

Finally, the experts were asked about the appropriate standard access control model that can be used to implement AdRBAC model. Most experts advised using eXtensible Access Control Markup Language (XACML) model to implement the proposed model and build access control policies. XACML an open standard designed to represent security policies and access rights of web services. It is a common standard in access control models between multiple vendors [50]. Moreover, XACML is an XML-based language, which is used to create flexible access control policies to describe requirements to access a certain resource [51].

IX. Discussion

The IoT security experts reviewed the proposed AdRBAC model. The majority of experts have felt that the proposed model is interesting and will be a good starting point to increase the information sharing and availability in IoT application by considering security risks associated with the access request and at the same time increases the level of security in IoT applications.

Twenty IoT security experts have validated and refined the proposed model through confirming the methodology followed by the researcher and suggesting new information related to risk estimation techniques and risk factors. As advised by experts, a fuzzy logic approach will be used to estimate the security risk associated with access requests. The fuzzy logic will provide a flexible framework. Regarding risk factors, we believe that the proposed four risk factors are appropriate as they can be adjusted to different IoT application easily without the need to add or remove other factors. In addition, we believed that XACML is the appropriate access control standard, as advised by experts, to be used to implement the proposed model.

X. Conclusion

Due to the dynamic nature of the IoT, traditional access control approaches cannot satisfy security requirements, as they are static and context insensitive. Therefore, this research has sought to develop a dynamic and adaptive access control model that can adapt to IoT changing conditions. Risk-based access control is one of the dynamic models that uses real-time contextual features to estimate the security risk associated with the access request to make the access decision. The AdRBAC model for the IoT has been proposed. This model has four inputs; user contextual features, resource sensitivity, action severity and risk history. This model provides not only the flexibility in accessing system resources but also the ability to handle exceptional access requests when a user must be granted the access to perform a critical action that can save lives as in medical and military applications. Twenty IoT security experts were interviewed to validate the proposed model and get more information about the proposed model form highly experienced persons. Most experts were interested and confirmed that the model will be valuable to the industry. They advised using the fuzzy logic to conduct the risk estimation process especially in the absence of the appropriate datasets. Moreover, they have recommended working on a specific IoT application and specify related risk factors. In addition, they have advised implementing a mitigation plan to be used to detect and prevent malicious actions during monitoring the access session and finally they have suggested that XACML is an appropriate access control standard to be used to implement the proposed model. In future work, the fuzzy logic approach will be used to implement the risk estimation process of the proposed model.

Acknowledgment

We acknowledge Egyptian cultural affairs and mission sector and Menoufia University for their scholarship to Hany Atlam that allows the research to be undertaken.

References

[1] M. Elkhodr, S. Shahrestani, and H. Cheung, “The Internet of Things: Vision & challenges,” *IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc.*, pp. 218–222, 2013.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] J. Kaur and K. Kaur, “Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 4, pp. 57–70, 2017.

[4] K. Ashton, “That ‘Internet of Things’ Thing,” *RFiD J.*, p. 4986, 2009.

[5] ITU, “The Internet of Things,” *Itu Internet Rep. 2005*, p. 212, 2005.

[6] ITU, “Overview of the Internet of things,” *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model.*, p. 22, 2012.

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

[8] 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.

[9] 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.

[10] 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.

[11] V. Suhendra, "A Survey on Access Control Deployment," *Commun. Comput. Inf. Sci.*, pp. 11–20, 2011.

[12] D. Kumar, A. Sharma, and S. Singh, "Entity Based Distinctive Secure Storage and Control Enhancement in Cloud," *Int. J. Inf. Eng. Electron. Bus.*, vol. 9, no. 1, pp. 10–19, 2017.

[13] K. Z. Bijon, R. Krishnan, and R. Sandhu, "A framework for risk-aware role based access control," *2013 IEEE Conf. Commun. Netw. Secur.*, pp. 462–469, 2013.

[14] 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.

[15] 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.

[16] A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and G. B. Wills, "The Impact of Cloud Forensic Readiness on Security," in *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, 2017, pp. 511–517.

[17] 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.

[18] C. Jason, "HORIZONTAL INTEGRATION: Broader Access Models for Realizing Information Dominance," *MITRE Corp. Tech. Rep. JSR- 04-132*, 2004.

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

[20] S. Kandala, R. Sandhu, and V. Bhamidipati, "An Attribute Based Framework for Risk-Adaptive Access Control Models," *Proc. 6th Int. Conf. Availability, Reliab. Secur.*, pp. 236–241, 2011.

[21] 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.

[22] 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.

[23] C. World, "The Internet of Things : An Overview," *Internet Soc.*, no. October, 2015.

[24] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[25] M. S. A. Carlo, "An Overview of Privacy and Security Issues in the Internet of Things," *McKinsey Q.*, vol. 2, p. 6, 2013.

[26] Y. Lee, "Technology Trends of Access Control in IoT and Requirements Analysis," *IEEE, Inf. Commun. Technol. Converg. (ICTC), 2015 Int. Conf.*, pp. 1031–1033, 2015.

[27] M. O. Onyesolu and A. C. Okpala, "Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM)," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. October, pp. 50–56, 2017.

[28] C. Langaliya and R. Aluvalu, "Enhancing Cloud Security through Access Control Models : A Survey," *Int. J. Comput. Appl.*, vol. 112, no. 7, pp. 8–12, 2015.

[29] D. F. Ferraiolo, J. a Cugini, and D. R. Kuhn, "Role-Based Access Control: Features and Motivations," *Proc. 11th Annu. Comput. Secur. Appl. Conf.*, pp. 241–248, 1995.

[30] Q. Wang and H. Jin, "Quantified risk-adaptive access control for patient privacy protection in health information systems," *Proc. 6th ACM Symp. Information, Comput. Commun. Secur. - ASIACCS '11*, pp. 406–410, 2011.

[31] Y. Li, H. Sun, Z. Chen, J. Ren, and H. Luo, "Using Trust and Risk in Access Control for Grid Environment," *Secur. Technol. 2008. SECTECH '08. Int. Conf.*, pp. 13–16, 2008.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] E. L. O. Feitosa, "Security Information Architecture for Automation and Control Networks," in *VIII Brazilian Symposium on Information Security and Computational Systems*, 2014, no. March 2017.

[38] 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.

[39] H. F. Atlam, G. Attiya, and N. El-Fishawy, "Comparative Study on CBIR based on Color Feature," *Int. J. Comput. Appl.*, vol. 78, no. 16, pp. 975–8887, 2013.

[40] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, 2016.

[41] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," *2016 IEEE Int. Conf. Consum. Electron.*, pp. 467–468, 2016.

[42] H. F. Atlam, G. Attiya, and N. El-Fishawy, "Integration of Color and Texture Features in CBIR System," *Int. J. Comput. Appl.*, vol. 164, no. 3, pp. 23–29, 2017.

[43] 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.

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

[45] B. DiCicco-Bloom and B. F. Crabtree, "The qualitative

research interview," *Med. Educ.*, vol. 40, no. 4, pp. 314–321, 2006.

[46] V. Lo Iacono, P. Symonds, and D. H. K. Brown, "Skype as a tool for qualitative research interviews," *Sociol. Res. Online*, vol. 21, no. 2, pp. 50–57, 2016.

[47] 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.

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

[49] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "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)*, 2017, pp. 254–260.

[50] T. J. N. Liang Chen, Luca Gasparini, "XACML and risk-aware access control," in *Proc. ICEIS*, 2013, pp. 66–75.

[51] C. M. Westphall and G. R. Schmitt, "A Risk Calculus Extension to the XACML Language," *Brazilian Symp. Inf. Syst.*, pp. 321–328, 2016.

Authors' Profiles

Hany F. Atlam has born in Menoufia, Egypt in 1988. He has completed his bachelor of engineering and computer science from Faculty of Electronic Engineering, Menoufia University, Egypt in 2011, then completed his Master degree in computer science from the same university in 2014. He joined the University of Southampton as a Ph.D. student since January 2016. Hany's now is a lecturer in Faculty of Electronic Engineering, Menoufia University, Egypt and a Ph.D. candidate at the University of Southampton, UK.

He has many experiences in networking as he holds international Cisco certifications and Cisco Instructor certifications. Hany is a member of Institute for Systems and Technologies of Information, Control and Communication (INSTICC), and Institute of Electrical and Electronics Engineers (IEEE).

Hany's research areas include IoT security and privacy, Cloud computing security, Blockchain, Big data, digital forensics, computer networking and image processing.

Ahmed Alenezi a lecturer at Northern Border University, Saudi Arabia and a Ph.D. candidate at the University of Southampton, UK. Ahmed is interested in multidisciplinary research topics that related to computer science. His research interests include Parallel Computing, Digital forensics, Cloud Forensics, Cloud Security, Internet of Things Forensics and Internet of Things Security.

Raid Khalid Hussein is a Ph.D. candidate. at the University of Southampton, UK. His research interests include cloud Virtualization and security, IOT security and Cloud Forensic.

Gary B. Wills is an Associate Professor in Computer Science at the University of Southampton. He graduated from the University of Southampton with an Honours degree in Electromechanical Engineering, and then a PhD in Industrial Hypermedia system. He is a Chartered Engineer, a member of the Institute of Engineering Technology and a Principal Fellow of the Higher Educational Academy. He is also a visiting associate professor at the Uniiversity of Cape Town and a research professor at RLabs.

Gary's research projects focus on Secure System Engineering and applications for industry, medicine and education.

How to cite this paper: Hany F. Atlam, Ahmed Alenezi, Raid Khalid Hussein, Gary B. Wills,"Validation of an Adaptive Risk-based Access Control Model for the Internet of Things", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.1, pp.26-35, 2018.DOI: 10.5815/ijcnis.2018.01.04