Adaptive risk-aware access control model for Internet of Things

Annanda Thavymony RATH
Precise, Faculty of Computer Science
University of Namur, Belgium
Email: rath.thavymony@unamur.be

Jean-Noël Colin
Precise, Faculty of Computer Science
University of Namur, Belgium
Email: jean-noel.colin@unamur.be

***Abstract*—IoT technology allows people to connect to and control devices remotely anywhere and anytime. However, serious concerns are raised over access control of sensitive IoT devices (e.g. portable health device) and personal information pertaining to them. The static access control model used in conventional system, which does not take into account the profile and behaviour of the agent requesting access to the system to determine the risk associated with the request, does not fit well to be used in some scenarios of some IoT application domains (e.g. smart healthcare). In this paper, we propose an adaptive risk-aware access control and the integration of this concept into the existing access control models, such as attribute-based and privacy-aware role-based access control. The proposed model is designed to address both security and privacy concerns for data sharing in IoT system. A prototype of the access control system implemented in XACML based on the proposed model is also presented in this paper.**

***Keywords*-adaptive; risk-aware; access control; IoT;**

I. Introduction

IoT offers the capability to connect the physical world (represented by physical objects) to the virtual world (represented by the Internet). Although cross-linking of devices offers new possibilities to influence and to exchange, this can also lead to potential risks concerning information security and both privacy and data protection [12]. The severity of each risk will depend on the circumstances in which each IoT application is deployed. For example, in smart healthcare, which is used to observe the daily health of patient or a system used to track the movement of patient/ elderly people, needs more attention since it deals with private information as well as personal security. In general, most communications in IoT occur automatically- devices decide to exchange data with their environment, potentially without user being aware of it. The failure to correctly control access to devices and information pertaining to them can lead to severe information security and privacy risk.

As IoT research and technology is not yet mature enough [12], there is no standard and unique mechanism to ensure proper security of both devices and data. The challenges that IoT are facing, such as scalability, availability, manageability and security, are still open and need to be addressed. In this paper, we tackle the security aspect and access control in particular. We argue that the conventional access control (AC) models, such as ACL (access control list) [9], role-based access control (RBAC) [9], attribute-based access control (ABAC) [9] and organisation-based access control (OrBAC) [9] do not respond to the access control requirements (see Section II) in IoT, which promotes the openness and collaboration where information is more exposed to attacks compared with closed system [6]. An adaptive and dynamic access control, that takes into account user's profile and behaviour to determine the risk associated with the access request, is required to affectively address the concerns of access control in IoT. There is an important concept in our proposed access control model that is adaptive risk-aware.

Adaptive risk-aware is a method of applying varying levels of stringency to access control based on the likelihood that access to a given user could result in its being compromised. As the level of risk increases, the access control enforcement process becomes more comprehensive and restrictive. In adaptive access control, different level of enforcement is applied to access request for different situation and context in order to minimise the risk associated with request if granted.

In our approach, each risk is measured by a value, which is expressed in access control policy and the access permission is granted based on that estimated risk value. The access restriction in the form of policy enforcement may be applied adaptively based on the estimated risk value.

This paper is structured as follows. Section II presents the access control scenarios and requirements in IoT. A comparison between different existing AC models against defined AC requirements is also discussed in this section. Section III is about risk model. Section IV presents the adaptive risk-aware access control models. Section V talks about access control system prototype and implementation of such prototype in Java based on XACML [14] policy language. Section VI presents the related work. Section VII is the conclusion and future work.

II. Access control scenarios and requirements

In this section, we present some access scenarios in IoT where threats are apparently prominent following by access control requirements. Two requirements are discussed in this section: legal and general access control requirements. The comparison of existing access control models against the defined requirements is also discussed in this section.

A. Threats in IoT: Access scenarios

Among 8 categories of threats [6] in IoT, software attack is an obvious cause for concern since IoT users generally use back-end application to manage and control devices or data. Software attacks (e.g. system or account hacking) can exploit entire systems, steal information, alter data, compromise or damage devices and deny service. Below are some real IoT scenarios where the threats exist and need to be addressed.

Scenario 1. We take a smart home scenario where home owner (user) routinely executes commands to smart devices using smart home application. Each user has an account, which can be used to access the smart devices. User can, for example, turn-on or off devices (e.g. smart door), check the video surveillance and other sensing devices. The interaction between user and smart devices has been happening in the more or less precise time interval, which creates an access pattern. Suppose that there is a situation where account is hacked and malicious user executes commands on devices in the strange way (e.g. turn-off CCTV when user is not at home). User has never executed such command when he is not at home. In such situation, how system intelligently react to such strange behaviour and prevent malicious user from executing those commands? In this example, we see that there is a level of risk associated with access permission if granted, the jeopardy of home safety. The access control system should be able to detect the risk and reacts accordingly.

Scenario 2. The second scenario is related to smart car in IoT context. In April 2015, Cyber security experts Charlie Miller and Chris Valasek [1] revealed a software flaw that allowed them to take control of a Jeep Cherokee on the move – all from a laptop computer at home. Hacking into the Jeep's electronics through the entertainment system, they were able to change the vehicle's speed, alter its braking capability, and manipulate the radio and windscreen wipers. In this kind of scenario, if the risk-aware is taken out of context and traditional access control, that is not able to detect the present risk, is used, system is not able to prevent malicious user from executing the dangerous action, for instance, suddenly increasing or dropping the vehicle speed. The improper change of vehicle speed can have fatal result.

Scenario 3. The third scenario concerns the smart healthcare system where personal and private information are processing. This areas of IoT requires high level data protection compared with other application domains [6]. For example, a system allowing physician to observe the daily health condition of patient or a device allowing to trace the movement of patient in house or healthcare institution. We can take a scenario of patient or elderly people tracking system, which provides the whereabouts information of a person.. In this system, a device is attached to a person and his physical location is reported to system. In a scenario where the system is hacked, hacker can get the information from the system and secretly track down the movement of the person. There is a risk, in this scenario, it concerns the personal safety (e.g. kidnapping).

In traditional access control, the access permission is assigned to a subject (user), which is authenticated by the username and password or other type of user's credential. Once user is authenticated, he can access resources (or devices) based on the pre-defined access control policy. In case of user credential is hacked, hacker impersonates the actual user and system could not detect without the help of intelligent system. This comes to the need of risk-aware system where system is able to estimate risk using some kind of machine learning techniques or other relevant methods [15] and then reacts to user's access request in accordance with a given situation although user is successfully authenticated. This risk-aware adds another level of control to resources, hence, making the system more secure and attack-aware.

Security myths around connected devices are plentiful [6], however, we provide three scenarios above in order to illustrate the importance of having risk-aware access control to devices as well as data pertaining to them.

B. Legal requirements

The objective of this work is to explore the scope of the major privacy issues raised by the IoT system in general. We identify the major legal challenges. These main challenges are seen through, amongst others aspects, for instance, the European convention on the human rights [11], the convention for protection of individuals with regard to automatic processing of personal data, European charter of fundamental rights [11] and general data protection regulation (GDPR) to be taken into effect by May 2018 [11]. These legislations put more emphasis on the use and processing of personal information and other privacy sensitive information (e.g health information). The privacy protection becomes a compulsory requirements when creating any system dealing with personal information, for instance, in GDPR [11], the concept of privacy-by-design and privacy-by-default [11] are the two major requirements when developing system dealing or processing personal information. Below, we provide the main requirements for personal data processing.

- **Purpose**. To prevent excessive use of data, user should only collect information for a specific purpose.
- **Consent/Access**. Data should never be transferred to a third party without clear approval of owner.
- **Accountability**. Data owner should be informed when personal data is processed.
- **Safeguards**. If IoT system is connected with third party entity such as cloud services, these providers must ensure that data safety is properly installed.

These legal requirements must be incorporated into the design of access control model in order to ensure the compliance with laws. Based on that vision and access scenarios in

[1] https://betanews.com/2015/11/30/the-security-risks-of-iot-devices/

Section II.A, we propose the access control requirements in Section II.C.

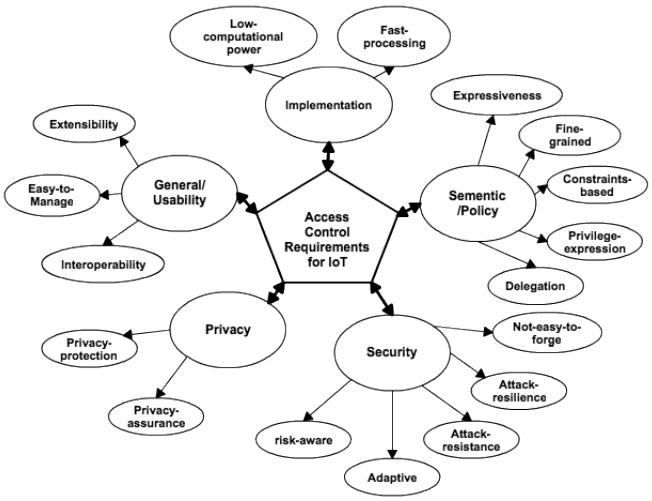

Figure 1. Access Control Requirements for IoT system

C. Access control requirements

The services, such as home monitoring, home automation, home security and smart health enable user control over a wide range of services by means of end-user devices. These transformations have introduced a wide variety of new risks. The potential for malicious activities ranges from mischief to crime and malicious hacking. The third party sensor can gather and monitor private data which can lead to burglary or any other form of troubles. Therefore, these unauthorised access needs to be checked. To securely control the unauthorised access requires the well-designed access control policy that takes into account all possible security risks. The model based on which the policy is defined must be able to respond to all the requirements and constraints under such environment. Based on our studies on legal and security issues, we classify the access control requirements into five main categories as following (see Figure 1).

1) General/usability. In general, access control system should be extensible, interoperable and easy to manage given the fast-advancing of IoT system and heterogeneity of devices and system.

2) Privacy. Future access control model should also support privacy protection given that large number of IoT scenarios are dealing with personal information directly or indirectly.

3) Security. Several security features must be embedded in the model such as forging issue, attack resistance, attack resilience, adaptive and risk-aware. Adaptive and risk-aware are two of the most important features required in IoT system since IoT promotes the concept of openness and collaboration. Openness with connected world is very susceptible to attack since it provides more attacking opportunities.

Table I
COMPARISON BETWEEN DIFFERENT EXISTING AC MODELS AGAINST REQUIREMENTS

	Easy-to-manage	Scalability	Low computational power	Less complex	Expressiveness	Granularity	Privacy expression	Risk-aware
DAC	×	×	✓	✓	×	×	×	×
MAC	×	×	×	×	✓	✓	×	×
ABAC	✓	✓	✓	×	×	✓	×	×
RBAC	✓	×	×	×	×	×	×	×
OrBAC	✓	✓	×	×	✓	✓	×	×
P-RBAC	✓	✓	×	×	✓	✓	✓	×
Family-RBAC	✓	✓	×	×	✓	✓	×	×

× Model does not have this property ✓ Model has this property

4) Semantics/policy. Most of access and usage scenarios in IoT are complex. The control of access in complex scenarios requires fine-grained access control policy with high level of expressiveness. A number of access constraints may also be needed to restrict the access to devices or data. In some IoT access scenarios, especially in smart healthcare and smart home, the privilege and delegation concepts are required. For example, in smart healthcare, physician needs a delegation right granted by patient or a special privilege to access data generated from health device.

5) Implementation. Major IoT scenarios deals with real-time or near real-time data (data from environmental sensors), hence, it is important to have very fast processing access control system. However, most of IoT devices constraint with power. Optimising the power usage is also important.

D. Comparison between different AC models

In this section, we compare standard access control models against the requirements we defined in previous section.

Discretionary access control (DAC) [9] is an access control model that the restriction of access to objects is done based on the identity of subjects to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission on to any other subjects. One implementation of DAC is ACL. DAC lacks of some features required in IoT (see Table I), such as scalability, expressiveness, granularity and privacy.

Mandatory access control (MAC) [9] refers to a type of AC model by which the system constrains the ability of a subject to perform some sort of operation to an object. In MAC, subjects and objects each have a set of security attributes and when a subject makes an attempt to access an object, an authorisation rule enforced by the system examines these security attributes and then the decision can be made whether the access is granted or not. MAC supports expressiveness and granularity, but it does not have the concept of privacy and risk-aware. Another disadvantage of MAC exists in the complexity of the configuration, since for each object's and

subject's security attributes must be determined. This tends to be very difficult for the system that works with large number of users and resources like IoT.

RBAC [9] is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC, such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. RBAC can be used to facilitate administration of security in large organisations with hundreds of users and thousands of permissions. Although traditional RBAC has the advantages over other existing models, such as DAC and MAC, it still lacks of some features, such as expressiveness and privacy expression. Moreover, it does not have the concept of risk-aware in its core model.

OrBAC [9] supports the control of data as well as user in system like organisation structure and access permission is granted based on user's role in that organisation. In addition, it can also express the access permission in contextual environment, role and data hierarchy, separation of duties as well as permission transfer, but there is no concept of privacy and risk-aware in core OrBAC.

P-RBAC [9] is an extension of the model RBAC, which provides complete support for expressing highly complex privacy-related policies. Its focus is to protect personally identifiable information and as such privacy-sensitive, taking into account characteristics, such as goals (purposes), conditions and obligations. P-RBAC has all of RBAC's features, but it does not support risk-aware expression.

Traditional access control models, such as DAC, MAC and RBAC are designed to be used in different contexts, some of their features match to our defined requirements, but some required features are missing. Given the IoT scenarios in Section II.A and the AC requirements in Section II.C, we argue that risk-aware feature should be incorporated in the model to fully address the access control issues in those scenarios.

III. Risk model

Risk can be interpreted as a probability of threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action [8]. In our risk model, each risk is associated with a risk-threshold, risk-evaluation function and the enforcement methods. We define a risk-threshold is a maximum risk tolerant that access control system is willing to accept when granting access request, and what kind of enforcement is required if risky access is permitted.

- Let R be a set of risks (r).
- Let T be a set of risk thresholds (t) where $t \in [0, 1]$.
- Let O be a set of risk avoidance enforcement Obligation (o) where O is some obligations that user or system needs to fulfil if a risky access permission is granted.
- Let F be a set of risk assessment functions where $f \in F$. Risk assessment function is a method used to evaluate the associated-risk. This function returns the probability of risk associated with the permission.

Definition 1: Risk expression

Let R be a set of risk (r), where $r \in R$. "r" has the finite domain of possible values, denoted as D where $d \in D, d = [0, 1]$. "r" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The risk expression of r has the form (r opr d).

let r_1 and r_2 are two risk variables. Then, $(r_1 \wedge r_2)$ or $(r_1 \vee r_2)$ are multiple risks conditioned in policy.

Definition 2: risk avoidance enforcement Obligation expression

---

Let O be a set of risk avoidance enforcement obligation variables (o), where $o \in O$. "o" has the finite domain of possible values, denoted as B where $b \in B$. "o" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of "o" has the form (o opr b). For example, user notification obligation has the form: $notify = true$.

If t_2 is the risk threshold, we can formulate our risk to access permission assignment as following.

(p, (($r \leq t_2$, f), o))

The above expression is read as a permission "p" is granted if the risk "r" assessed by risk-assessment function (f) is less than or equal t_2 (risk-assessment threshold) and this permission is further enforced by obligation "o". Suppose that we have U, which is a set of users (u). The user to risk-aware permission assignment can be formulated as following.

(u, (p, (($r \leq t_2$, f), o)))

Then,

- The request (u, p) is granted if the risk of granting (u, p) is less than or equal t_2. However, the obligation "o" stated in policy must be fulfilled;
- The request (u, p) is denied if the risk of granting (u, p) is greater than t_2.

The value (t) of risk (r) can be calculated using the risk-estimation function (f) based on risk-aware information that can be taken from different sources, such as user access history, environmental parameters, spatial/temporal information or information from external system (see Figure 3 for more details). Actually, estimating and managing risk is a case-by-case study given different nature and type of risks that may have in IoT system environment, hence, risk-evaluation function can not be generalised [15].

Example 1: risk-aware access control policy expression

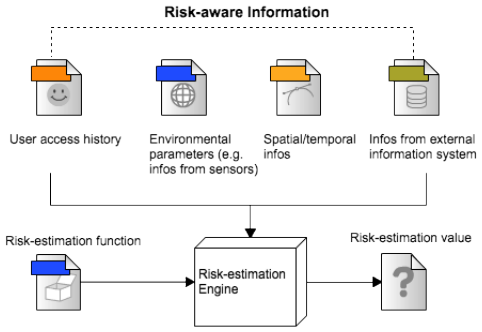

Figure 2. Risk-value calculation architecture

Policy: rule states that user "Edward" can turn-off the surveillance CCTV through his account by using web application if the risk-aware-account-hacking-detection (account-hacking) value is less than 0.2. And system needs to notify to Edward if the permission is granted. Then, we can express the policy as following.

(Edward, ((turn-off, CCTV), ((account-hacking $\leq$ 0.2), risk-aware-hacking-detection), notify=true)))

Although this approach increases the complexity of policy decision process at permission level, it is more secure than other existing access control models [9], which usually do not adopt the risk assessment in policy level, instead, use a global risk management at authentication level. For example, in IoT usage scenarios, user account may be hacked and malicious user may command on device in the abnormal and unreasonable way. If risk assessment is done at authentication level, it is not able to address this issue since hacker is already successfully authenticated.

This risk model can be incorporated with other existing access control models. In this paper, we extend attribute-based access control and P-RBAC to support our risk model. The idea of extending this two models is that ABAC and P-RBAC are the two well known access control models that are being used widely in many systems [9]. ABAC is well known for its ability to express fine-grained and complex policies and it is easy to understand and manage. The well known existing access control engine such as XACML is also implemented based on ABAC model. ABAC is good to be used in large number of IoT access scenarios in the domains, such as entertainment, traffic control, agriculture and transportation [3]. However, for some scenarios dealing with privacy sensitive or personal information, such as healthcare, smart home or surveillance system, P-RBAC is more appropriate since P-RBAC allows to express complex privacy sensitive policy with the support of condition, purpose and obligation.

IV. Adaptive Risk-Aware Access Control

We present two extended access control models: adaptive risk-aware ABAC and adaptive risk-aware P-RBAC.

A. Adaptive risk-aware attributed-based access control

ABAC [9] defines an access control model whereby access rights are granted to users through the use of policies which combine attributes together. ABAC is becoming well known and considered as a "next generation" authorisation model because it provides dynamic, fine-grained, context-aware and intelligent access control. ABAC uses attributes as building blocks in a structured language that defines access control rules and describes access requests. Attributes are sets of labels or properties that can be used to describe all the entities that must be considered for authorisation purposes. As shown in Figure 3, the traditional ABAC model consists of 4 main entities (e.g. subject, action, resource and environment) where each entity may hold multiple attributes.

- Subject attributes describe the user attempting the access e.g. age, clearance, department, role, job title...
- Action attributes describe the action being attempted e.g. read, delete, view, approve...
- Resource (or object) attributes describe the object being accessed e.g. the object type (medical record, bank account...), the department, the classification or sensitivity, the location...
- Contextual (environment) attributes deal with time, location or dynamic aspects of the access control scenario. For more details about ABAC, see in [9].

To formally incorporate the risk-aware concept into ABAC model, we propose the extension like shown in Figure 4. The risk-aware info (information) entity is responsible for providing the risk-value estimation at the time of request. The new extended ABAC policy should contain not only user, action, resource and environmental attributes, but also the risk-aware attribute(s).

Risk-aware information is considered as separate entity from environment attributes in ABAC model because in traditional ABAC, environment attribute is any information regarding the context of the access that might be used in making the access decision, such as, time, network or spacial context whereas risk-aware information is the information from different sources used for estimating the risk associated with request. In most cases, risk-aware information is a complex data sets that generally come from databases (e.g. access history) or external information system.

Extended ABAC policy expression

- Let U be a set of users (u);
- Let A be a set of actions (a);
- Let C be a set of resources (c);
- Let E be a set of environment attributes (e).

The permission assignment in ABAC is expressed as (u, p) where p is a permissions on resource. p=(a, c, e). The risk-aware ABAC policy expression is as follows.

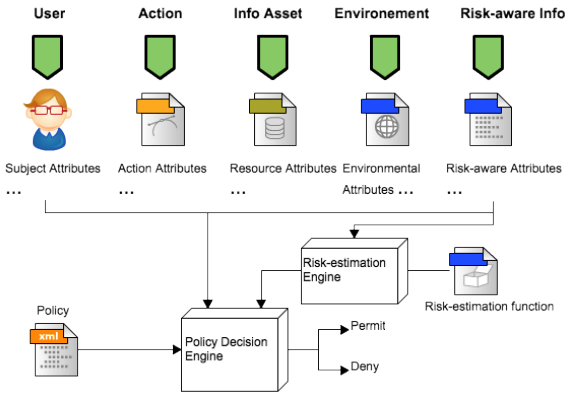

Figure 3. Adaptive and risk-aware ABAC

p= ((a, c, e), ((r , f), o))

Refer to Section III (risk model) for more detail. The complete risk-aware ABAC policy considering subject (or user) attribute can be expressed as follows.

p= (u, (a, c, e), ((r , f), o))

Definition 3: ABAC environmental variable expression

Let E be a set of environmental attributes (e), where $e \in E$. "e" has the finite domain of possible values, denoted as N where $n \in N$. "e" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of "e" has the form (e opr n). let e_1 and e_2 be two environmental variables. Then, $(e_1 \wedge e_2)$ or $(e_1 \vee e_2)$ are multiple environmental variables conditioned in policy. For example, time $\geq$ 20:10:00.

Example 2: risk-aware ABAC policy expression

Policy: rule states data user "David" can open the smart door through his account by using smart application in between 17:00:00 and 20:00:00 if the risk-aware-malicious-detection (malicious-user) value is less than 0.4. And system needs to prove that user is really David by letting David answer the secret question registered during account creation. Then, based on definition 1 and 2, we can express the policy as following.

(David, ((open, smart-door, $(time \geq 17:00:00) \wedge (time \leq 20:00:00)$), ((malicious-user ≤ 0.4), risk-aware-malicious-detection), prove(question)=true)))

B. Adaptive risk-aware privacy-aware role-based access control

Taking into consideration different access scenarios and risks associated with them in smart home, healthcare and other privacy sensitive systems, we propose an extended version of privacy-aware role-based access control (P-RBAC) [10]. It is called "adaptive risk-aware privacy-aware role-based access control". P-RBAC is an extension of the model RBAC [9]. It provides complete support for expressing highly complex privacy policies. Its focus is to protect personally identifiable information and as such privacy-sensitive, taking into account characteristics, such as purposes, conditions and obligations. In P-RBAC, data permissions are assigned to roles for a specific purpose. Conditions are the mechanisms to precisely define the authority over data to a specific role. Obligations are the necessary actions to be made before the actions on content can be exercised.

For adaptive risk-aware P-RBAC, two more entities are added to be able to address the risk associated with access request at permission level. They are the "risks" and "risk-avoidance enforcement". The "risks" entity is used to express the level of risk tolerance that a policy can support. "risk-avoidance enforcement" is some forms of obligation or duties or actions that user or system needs to perform before or after the request is granted. This risk-avoidance enforcement is similar to "obligation", but it is more complex since it may contain a lengthy procedure that user or system needs to follow to avoid risk.

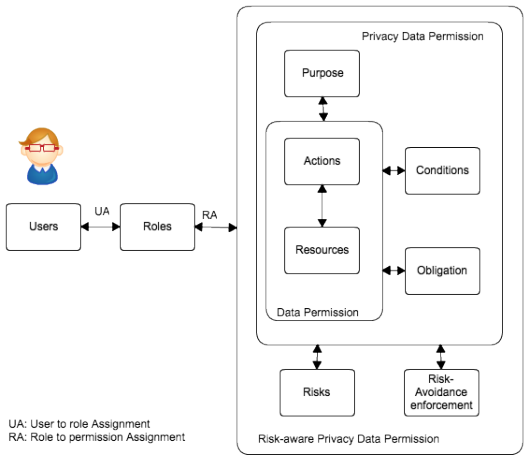

Figure 4. Adaptive, risk-aware, privacy-aware RBAC

Adaptive and risk-aware P-RBAC policy expression

- Let U be a set of users (u);
- Let L be a set of user roles (l);
- Let A be a set of actions (a);
- Let C be a set of resources (c);
- Let I be a set of conditions (i) ;
- Let Pu be a set of purpose (pu);
- Let O be a set of obligation (o);
- Let K be a set of risk-avoidance enforcement (k).

1) User to role assignment (UA): UA = (u, l)
2) Data Permission (DP) assignment: DP = (a, c)
3) Privacy Data Permission (PDP) assignment:

PDP = (DP, (l, pu, o)) or ((a, c), (l, pu, o))

4) adaptive, Risk-aware, Privacy-aware Data Permission (RPDP) assignment:
   RPDP = (PDP, ((r, f), k))) or ((((a, c), (l, pu, o)), ((r, f), k)))
5) Role to RPDP can be expressed as: (l, ((((a, c), (l, pu, o)), ((r, f), k))))

For risk-aware function expression, see Section III.

Definition 4: Condition expression

Let I be a set of conditions (i), where $i \in I$. "i" has the finite domain of possible values, denoted as J where $j \in J$. "i" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of "i" has the form (i opr j). let i_1 and i_2 be two conditional variables. Then, ($i_1 \wedge e_i$) or ($i_1 \vee i_2$) are also the conditions. For example, time $\geq$ 20:10:00.

Definition 5: Obligation expression

Let O be a set of obligation variables (o), where $o \in O$. "o" has the finite domain of possible values, denoted as B where $b \in B$. "o" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of "o" has the form (o opr b). For example, user notification obligation has the form: $notify = true$.

Definition 6: risk avoidance enforcement expression

Let K be a set of risk avoidance enforcement variables (k), where $k \in K$. "k" has the finite domain of possible values, denoted as H where $h \in H$. "k" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The risk avoidance enforcement variable of "k" has the form (k opr h). For example, user notification obligation has the form: $notify = true$.

Example 3: risk-aware P-RBAC policy expression

Policy: a rule states that every user in role "physician" can read heart-pulse from patient's smart wearable health-device for purpose of patient-health-follow-up whenever he wants given that the risk-estimation value is less than 60%. If the risk-value is in between 60% and 90%, physician needs to prove his identity by answering special question registered at the time of creating account. Physician needs also to notify patient every access.

Policy expression:

- DP = (read, heart-pulse)
- PDP = (DP, (patient-health-follow-up, notify)) or ((read, hearth-pulse), (patient-health-follow-up, notify))
- RPDP = (PDP, ((60% $\leq r \wedge r \leq$ 90%), prove-identity))) or ((((read, hearth-pulse), (patient-health-follow-up, notify)), ((60% $\leq r \wedge r \leq$ 90%), prove-identity)))
- Role to RPDP can be expressed as: (Physician, ((((read, hearth-pulse), (patient-health-follow-up, notify)), ((60% $\leq r \wedge r \leq$ 90%), prove-identity))))

Remarks: why we do not use "condition" entity to express risk? This is because the two entities have different nature. Conditions are environmental or system-oriented decision factors. Condition predicates evaluate current environmental or system status to check whether relevant requirements are satisfied or not and return either 'true' or 'false' [9]. Condition variables cannot be mutable since conditions are not under direct control of individual subjects. Some examples of condition requirements include current local time for accessible time period (e.g., business hours), current location for accessible location checking. Risk is the information from different sources used for estimating the risk associated with request. In most cases, risk-aware information is a complex data sets that generally come from databases (e.g. access history) or external information system.

In Extended P-RPAC, there are obligation and risk avoidance enforcement. Obligation is used to enforce overall access control policy whereas risk avoidance enforcement is used to prevent or minimise risk associated with request at policy decision level. Obligation at policy level is generally executed at Policy Enforcement Point (PEP) while risk avoidance enforcement is executed by a module at Policy Decision Point (PDP).

V. Access control system architecture

In this section, we present the adaptive risk-aware ABAC and its implementation in XACML policy engine [14]. For risk-aware P-RBAC, we consider it in our future work.

A. Risk-aware ABAC system architecture

As shown in Figure 5, the system consists of the following modules.

1) User is a Man Machine Interface acting as the intermediate layer between system and physical person.
2) PEP handles request from user and forwards it to policy decision point for further policy validation.
3) Recourses are the digital assets that are securely stored in system storage.
4) Obligation is a module handling different obligations that user or system needs to fulfil (e.g. notification).
5) PDP is responsible for validating the access control policy. It consists of three modules.
   a) Environmental attribute validation (EAV) is responsible for retrieving the environmental information from policy information point (PIP) or external information system.

b) OSAV is responsible for validating the object's and subject's attributes. These attributes are generally retrieved from PIP.
c) Risk-estimation is responsible for providing the risk estimation value, which is calculated using risk-estimation engine that is designed to support different risk-estimation functions.

6) Risk-estimation engine is responsible for calculating the risk-value based on defined risk-estimation function and the risk-aware information.
7) Risk-avoidance enforcement is responsible for enforcing some actions aiming to minimise or prevent the risk. This process is complex and sometime requires a lengthy procedure that user or system needs to follow. For example, if system detects that user is suspicious, system may require user to prove his identity either by answer question (question and answer registered when creating account) or use other credential to prove.

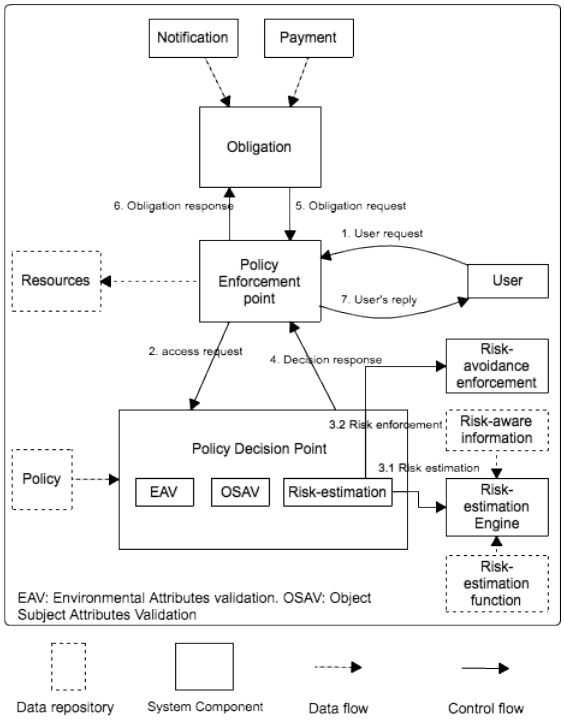

Figure 5. Adaptive, risk-aware ABAC Architecture

B. Implementation

In order to test our concept, we implement risk-aware ABAC in XACML. Some scenarios in smart home are used for validation and testing. We also develop the risk-estimation engine in Java and define the risk-estimation function for user account hacking scenario.

Risk and solution: account hacking and access pattern analysis. We take scenario 1 in Section II.A. We address the account hacking issue in smart home scenario. How to make an intelligent access control system being able to prevent hacker from executing harmful commands once he gets access to user's account.

A solution to tackle the above problem is to use user's access history as source of information for access pattern extraction. Then, this pattern is used as the reference for access permission decision. The access pattern can be defined based on relationship between different entities in access request and policy, such as user, action, devices, time interval and other environment and contextual constraints if any. With such information registered in access history we can use them to analyse the association between those entities. It is worth noting that we can add other parameters if we have in the association, however, in our example, we take only user, action, device, time as the entities.

Our idea is to find the relationship between user's request and time at which user often requests to execute the commands. Once the pattern is determined, we can rule out the request that does not fall into the defined pattern as unlikely from real user.

- Let U be a set of users (u) where $u \in U$
- Let A be a set of actions (a) where $a \in A$
- Let V be a set of devices (v) where $v \in V$
- Let M be a set of times (m) where $m \in M$

Given a user's request (u, a, v) and time m, determine the association between those entities. We propose to use association rule learning algorithm to determine their association. **Association rule learning (ARL)** is a rule-based machine learning method for discovering interesting relations between variables in large databases. It is intended to identify strong rules [13] discovered in databases using some measures of interestingness [13]. ARL is generally used to analyse the relationship between products in large-scale transaction data recorded by point-of-sale (POS) systems in supermarkets. However, it is also used in other areas, which require to determine the relationship between entities in the database.

Definition: let X and Y be two set of entities (or item sets) where X ∩ Y=0. X ⇒ Y is an association of X and Y. Let S be a set of transactions of a given database.

Confidence of rule $(X \Rightarrow Y)$ is an indication of how often the rule has been found to be true.

The confidence value of a rule, $X \Rightarrow Y$, with respect to a set of transactions S, is the proportion of the transactions that contains X which also contains Y.
Confidence is defined as: $\mathrm{Conf}(X \Rightarrow Y) = \frac{\mathrm{supp}(X \cup Y)}{\mathrm{supp}(X)}$

Support (or supp) is an indication of how frequently the itemset appears in the dataset. The support of X with respect to S is defined as the proportion of transactions "s" in the dataset which contains the itemset X. $\mathrm{supp}(X) = \frac{|\{s \in S; X \subseteq s\}|}{|S|}$

Apply ARL for risk value calculation. Suppose we have two sets of entities X and Y. X contains (u, a, v) and Y contains (m). We want to find the relationship between user

Table II
EXAMPLE: USER ACCESS HISTORY

Transaction	User	Action	Device	Time
1	Edward	Turn-off	CCTV	6PM
2	Edward	Turn-off	CCTV	6PM
3	Edward	Turn-off	CCTV	6PM
4	Charlie	Trun-off	Refrigerator	10 AM

performs action on device and time that action is executed. Since rule confidence is an indication of how often the rule has been found to be true, this means that, the higher confidence the lower risk. Thus, the risk value is defined as the reverse of rule confidence value. $1 - Conf(X \Rightarrow Y)$(see Section III).

Example 4: risk-value calculation

Suppose that we have the transactions like in Table II and a request (Edward, turn-off, CCTV, 6PM). Calculate the risk associated with the permission allowing Edward to turn off CCTV at 6PM given his past access history in Table II. $Conf((Edward, turn-off, CCTV) \Rightarrow 6PM)$= $\frac{\text{supp}((Edward, turn-off, CCTV) \cup (6PM))}{\text{supp}(Edward, turn-off, CCTV)}$=$\frac{3}{3}$, hence, the risk of allowing Edward to turn off CCTV at 6PM is 1-1=0.

There is one drawback for this approach that is we need to have a reasonable size of access history in order to define the risk threshold to be used in access control policy. This approach can not be applied in case of new user without access history.

Testing data set. In order to test the risk-estimation for account hacking scenario, we need access history. We generate a simulated access history for 50000, 100000 and 1000000 transactions (records) stored in the access log file with the data structure like in Figure 7.

Performance evaluation. The idea is to evaluate the general performance of risk-aware ABAC with the account-hacking risk estimation algorithms shown above. Since we use access history as the source of information for risk-estimation, larger access history can introduce larger delay for access control policy evaluation. Thus, it is important to observe the policy evaluation processing time given different sizes of access history. We used 60 access control policies expressed in XACML policy language for testing. We simulated 50 different access requests and find the average policy evaluation processing time. We tested our system in Macbook air 1.3 Ghz Intel Core i5, memory 8 GB 1600 MHz DDR3. The result is shown in table III.

As expected, the policy evaluation processing time is increased in accordance with the size of the access log. In case of load system, this issue can be a big challenge.

Table III
POLICY DECISION PROCESSING TIME

Experiment No	Log size	Average processing time
1	50000 records	156 milliseconds
2	100000 records	203 milliseconds
3	1000000 records	580 milliseconds

However, there are two possible ways for reducing the policy evaluation time. The first option is to minimise the size of the access-log; another is to increase the computational power of the system (e.g; parallel computing).

In order to minimise the size of access-log, we need to minimise the size of observation interval. Our proposed solution is to divide a large observation internal into many smaller intervals (equal size). Then, we define the risk threshold of each interval. The final risk threshold value, which is used in policy, is an average of the risk threshold values from the smaller intervals. With this method, the size of access log used to calculate the risk value is the size of access log of one interval (the most recent access-log), not the entire access-log. For example, instead of using many years access-log, we can use a year or a month access-log to evaluate the rule (policy).

VI. RELATED WORK

Although IoT field is rapidly gaining attention, there are a few researches focusing on access control in IoT [1] [5] [4] [2]. Most researches suggested existing access control models [9] to address access control in IoT. Below are some existing researches related to our work.

Mehdi et al [2] introduced a formal theoretical model for IoT collaboration AC model based on attribute and role based access control model. They also built data sharing framework based on the proposed model. Authors used the traditional ABAC and RBAC to address the access control challenges in IoT without considering risk in decision factor.

Blase et al [4] did a comprehensive survey of the current state of access control model for smart devices in homes. Based on their assessment of different access control models, they proposed to use role-based access control model. However, their study is very narrow by focusing only to smart home. This may not be suitable for other domain application such as surveillance system or most importantly healthcare domain where data needs high degree of protection given its values and sensitivity. Thus, fine-grained and complex policy expression is required.

Bruce et al [1] conducted a security analysis and improvements of authentication and access control in the Internet of Things. The authors proposed the improvement protocol for authentication and access control by introducing the cryptographic key in both authentication and access control processes. RBAC is author's primary study in the paper. Authors also built their system to validate its performance and the result indicates that the improved protocol possesses

many advantages against popular attack [6], and achieves better efficiency at low communication cost.

Rahul et al [3] proposed an access control model for home automation devices, which offers the capabilities to identify and connect physical devices into a unified secure system. The authors proposed to use Access Control List (ACL) as the access control security model to manage access to devices. Although ACL is simple to both understand and implement, it is not suitable for complex and fine-grained access control policies, which are needed in most of IoT scenarios.

Ricardo et al [5] proposed a model-based security toolkit for IoT, which is integrated in a management framework for IoT devices, and supports specification and efficient evaluation of security policies to enable the protection of user data. The authors's work is applied to a smart city scenario. The access control model, the authors used for building the frame work, is the improved RBAC model where the concept of trust and trust relationship is introduced.

Khalid et al [8] proposed a framework for Risk-aware Role based Access Control. The authors used different levels of risk control on RBAC model from user to role assignment, RBAC session and permission assignment. Our proposed model focuses only on permission level since it is designed to be incorporated with other models. Unlike that of ours, authors proposed a risk model specifically for RBAC.

VII. Conclusion

In this paper, we focus on the issue of access control in IoT. We introduced the general AC requirements taking into account the aspects of security and privacy. We also provided a short discussion and comparison of existing access control models against our defined set of requirements. Furthermore, the risk model and the extension of ABAC and P-RBAC to support our risk model are also presented. Finally, we propose the risk-aware ABAC system architecture and its implementation in XACML for proof-of-concept. Our future work is to look at the implementation of risk-aware P-RBAC and its deployment in IOT system, smart home in particular.

Acknowledgment

References

[1] Bruce Ndibanje, Hoon-Jae Lee and Sang-Gon Lee. Security Analysis and Improvement of Authentication and Access Control in the Internet of Things. Open access Sensors, 14(8), 14786-14805; doi:10.3390/s140814786, 2014.

[2] Mehdi Adda, Jabril Abdelaziz, Hamid Mcheick and Rabeb Saad. Toward an access control model for IoTCollab. The 6th International Conference on Ambient Systems, Networks and Technologies. Published by Elservier, Page 428-435, 2015.

[3] Rahul Godha, Sneh Prateek and Nikhita Kataria. Home Automation: Access Control for IoT Devices. International Journal of Scientific and Research Publication, Volume 4, Issue 10, October 2014, ISSN 2250-3153.

[4] Blase Ur, Jaeyeon Jung and Stuart Schechter. The current State of Access Control for Smart Devices in Homes. Workshop on Home Usable Privacy and Security (HUPS), July 24-26, 2013, Newcastle, UK.

[5] Ricardo Neisse, Gary Steri, Igor Nai Fovino and Gianmarco Baldini. SecKit: A Model-based Security Toolkit for the Internet of Things. The journal of Computer and Security (2015), page 60-76. Published by ELSEVIER.

[6] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad. Proposed Security Model and Threat Taxonomy for the Internet of Things. International Conference on Network Security and Applications (CNSA 2010). Recent Trends in Network Security and Applications pp 420-429. Published in Springer 2010.

[7] J. Sathish Kular and Dhiren R. Patel. A survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications. Volume 90. No 11, March 2014.

[8] Khalid Zaman Bijon, Ram Krishnan and Ravi Sandhu. A Framework for Risk-Aware Role Based Access Control. Communications and Network Security (CNS), 2013 IEEE Conference on Communication and Network Security. 14-16 Oct. 2013, National Harbor, MD, USA, USA.

[9] Assessement of Access Control Systems. National Institute of Standards and Technology. Technology Administration U.S. Department of Commerce. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[10] Ni Qun, Bertino Elisa, Lobo Jorge, Brodie Carolyn, Karat Clare-Marie, Karat John and Trombeta Alberto. Privacy-aware Role-based Access Control. ACM Trans. Information System and Security. vol.13, No.3, pages 24:1-24:31, July 2010. pages = 24:1–24:31,

[11] General Data Protection Regulation. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENGtoc=OJ:L:2016:119:TOC

[12] IoT Privacy, Data Protection, Information Security. ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

[13] Agrawal Rakesh, Imieliński Tomasz and Swami Arun. Mining Association Rules Between Sets of Items in Large Databases. SIGMOD Rec. June 1, 1993. Vol 22, No 2., New York, NY, USA.

[14] Extensible Access Control Markup Language (XACML). http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[15] Hany F. Atlam, Ahmed Alenezi1, Robert J. Walters and Gary 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), pages 254-260.