Access Control Requirements in IOTs: In context of smart home system environment.

Annanda Th. RATH *
University of Namur
Faculty of Computer Science
Namur, Belgium
rta@info.fundp.ac.be

Jean Noël Colin †
University of Namur
Faculty of Computer Science
Namur, Belgium
jnc@info.fundp.ac.be

ABSTRACT
Although connected devices and smart homes are now marketed to consumers, little is known about what are the general access control requirements for the devices in such system. The concept of smart home where users can control their devices remotely (e.g. through Internet) can raise many issues, such as security, privacy and personal safety and improper access control to those devices can provide a gape for intruder to hack the system and manipulate the devices in the way he wants. Thus, securing access to devices is the primary issue that needs to be tackled in order to make smart homes possible. In this paper, we present the access control requirements for IOT system, focusing on smart home environment where we take into account different dimensions, such as privacy, security, devices limitation, management issue and usability. These requirements should be matched when designing the future access control model to be used in smart home environment.

Categories and Subject Descriptors
H.4 [**Information Systems Applications**]: Security and privacy

General Terms
Theory

Keywords
E-health, Analogue attacks, Security, Privacy, Watermark, Fingerprinting

1. INTRODUCTION
With the advance of Internet technology and the availability of smart devices with affordable prices, people start to think about connecting and controlling those devices through Internet in order to facilitate the daily life of people. This is when the concept of IOT starts to take shape. The Internet of Things (IoT) [7] is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoTs system can be applied in different domains ranging from transportation, agriculture, health and importantly smart home. Smart homes [13] in which devices communicate with each other and provide remote monitoring and control features have yet to reach the mainstream. This is because these devices offer a range of capabilities and potential security and privacy concerns. These concerns need to be addressed if we want to realise the deployment of such system since many countries (e.g. european countries, USA , Canada , etc.) have their own legislations [3][1] assuring the privacy protection, fundamental of human right and citizen security protection.

While smart homes with the interactive features of connected devices can benefit users, they can also introduce opportunities for abuse. Intruder might cause lights to turn on or off, thief might disable automated door-locks and bad person might snoop on house/room-monitoring cameras. The access-control mechanisms familiar from decades of use in high computing systems may not be appropriate for home environments given the limit ability of the devices in both memory and computational power.

Researchers have only begun to explore the requirements of access control for home devices, using qualitative interviews exploring hypothetical situations and the experiences of early adopters who might not be representative of the overall market [10]. We come at the problem from different dimensions, looking at devices currently available, the knowledge of users, the legislations and security. We identified the access control requirements that are able to address all the challenges and concerns of controlling access to devices in the interactive smart home environment.

The rest of the paper is structured as following. Section 2 presents some scenarios in smart home environment. In this section, we explore different types of problems in the smart home access scenarios. The scenarios covers the in-home access and the remote access through Internet. Section 3

*To be completed.

†To be completed.

presents the access control requirements for smart home, we also discuss about the legal requirements, focusing mostly on European legislations [3] (privacy protection and fundamental human rights). Section 4 explores the related work on access control requirements and a short discussion on devices control, which will not be addressed in deep in this paper. Section 5 is the conclusion.

2. SCENARIOS AND CHALLENGES

We present in this sections some usage scenarios in smart home along with the addressing challenges. We focus on three important access scenarios: in case of home automation, accessing devices through Internet and a more specific case, home renting scenario (property transfer rights, permanent or temporary).

2.1 Home automation with smart devices

The first scenario concerns the interaction between user and smart devices installed in the house such as, light, heater, refrigerator, smoke detector, TV, CCTV and smart door or window. Suppose that with the support of some sensor devices, user is able to command by voice or by mobile API [9] to activate or regulate those devices according to his wishes. For example, command to regulate the heater in case the temperature is not comfortable or allow the sensor to do it automatically when it senses home is too hot or too cold. Another example is in case of the fire in the house, smoke detector detects the event and signals the water pumping system to release water or consider a larger system when smoke detector detects fire, it sigmas fire station to send the firetrucks. Another prominent scenario in smart home is the control of the smart door. The door opens itself when user arrives or the door locks itself when user forgets to lock or goes outside, or the door will sound in case user forgets to take the key with him.

With above given examples, we can see that in most of the cases, the sensors depends on the information provided by other sensors in order to activate the actuator [13]. The information provided by malicious sensors can cause unpleasant consequences. Assuring the communicating devices are the real one is the important issue in order to provide the reliable smart home service. In other words, controlling the access to information of the sensors is important in order to prevent the attacks by malicious sensors or users.

2.2 Control devices through Internet

The second scenario considers a large system where user can interact with smart devices at home through Internet. For example, user wants to watch the CCTV installed in the house when movement detection sensor detects abnormality in the house. Another example is when user wants to turn on/off TV, light or closes window remotely. In order to do so, user needs to communicate with system installed in smart house through Internet with the support of a specific API designed for that purpose. However, this service also introduces opportunities for abuse if improper access control is used since there is always a possibility that malicious user, through API, can break into the system and command the system in a way different from what user intends for. For example, stealing the CCTV stream can lead to severe privacy violation, security and personal safety. Turn on or off light or disconnect electricity supply for equipments in the house can lead to unpleasant consequence (e.g. if freezer is turned off, foods are spoiled) .

2.3 Home renting with specific devices usage allowance

The third scenario concerns the access of devices in smart home system in case of house/apartment renting either for long or short periods of time, or allowing someone (e.g. friends) to stay in the house for vacation. Assuming that house owner rents a house to a particular person and he can use a set of devices in the house, but not all of them, during his stay. For example, user can use all the devices except air conditioner or TV is disconnected every two hours if there is no activities to avoid unnecessary use of electricity. Or the system sends notification to house owner in case there is the over use of electricity or water. In such scenario, how to define the access control policy for user in such a way that limits the actions of user in accordance with house owner's wishes.

3. ACCESS CONTROL REQUIREMENTS

In order to define the access control requirements, we need to consider different factors, such as legal issues, usage scenarios, deployment and usability. These factors are the primary keys to define the access control requirements based upon which the access control model is built.

3.1 Legal requirements

The objective of this work is to explore the scope of the major privacy issue raised by the smart home system and IOTs 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 [1], the convention for protection of individuals with regard to automatic processing of personal data [3], European charter of fundamental rights [2] and Directive 95,46/EC on the conception of individual with regard to the processing of personal data or the new european data protection regulation to be taken into effect by May 2018 [5]. These legislations put more emphasis on the use and processing of personal information and other privacy sensitive information (e.g health information, bank account, etc.). The data generated from smart devices in smart home system such as CCTV, smart door or TV is considered as personal information, which is covered by laws [3]. The privacy protection becomes a compulsory requirements when creating any system dealing with personal information, for instance, in the new privacy protection laws [5], the concept of privacy-by-design and privacy-by-default [5] are the two major requirements, which are considered as the prerequisites when developing system dealing or processing the personal information [4].

Below, we provide the main requirements for controlling the processing of personal data under European law (Directive 95/46/EC) from article 10 and 11 and the new data protection laws [5].

- **Preventing the excessive use of personal data**. The smart home system must be able to prevent the

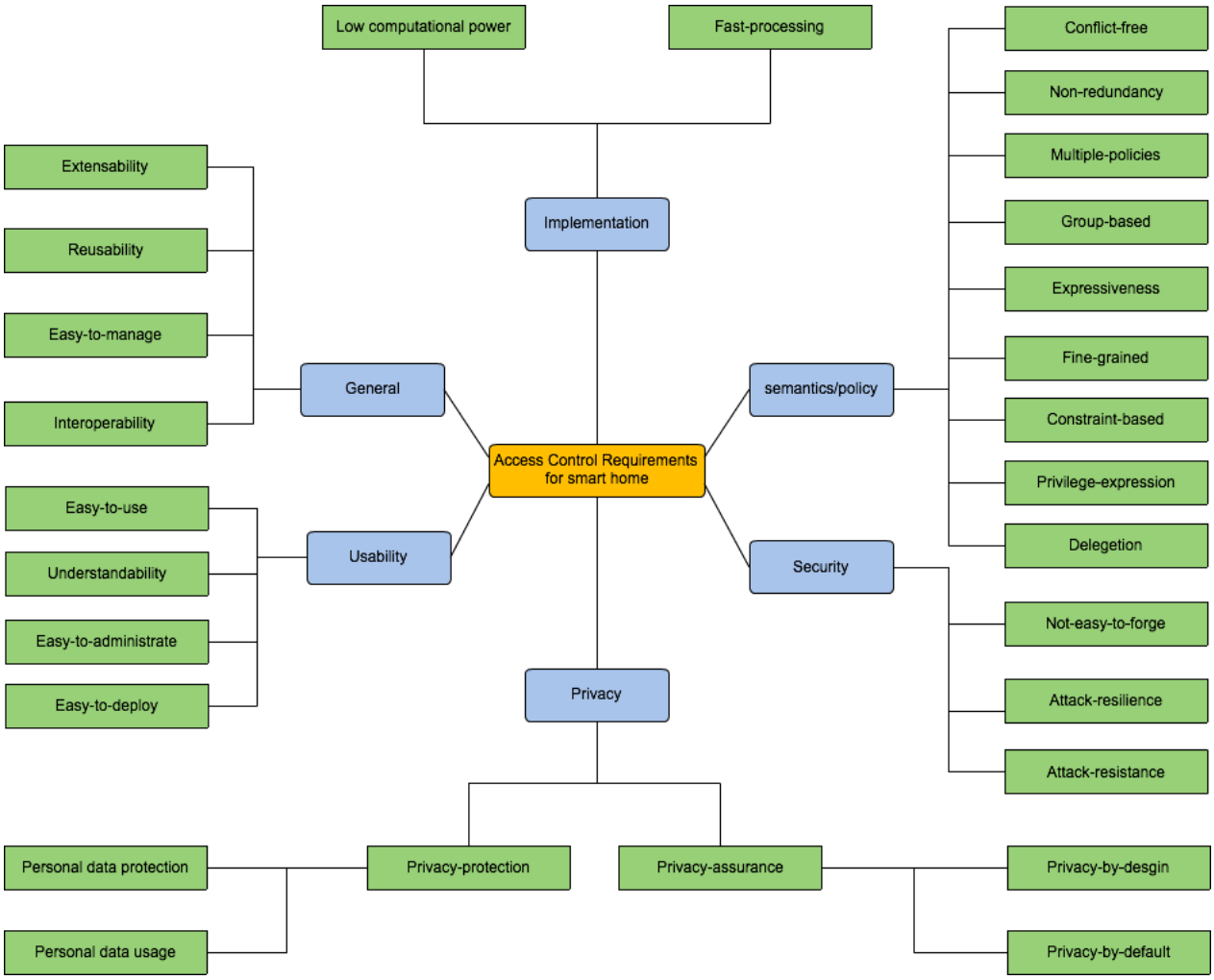

Figure 1: Access Control Requirements for smart home

excessive use of personal data generated from different sensors. In order words, the collected personal data should be used for the purposes it allows for. For example, the data collected from CCTV, installed in the house, must be kept secure and it is processed when there is request from authorised user.

- **Preventing the unauthorised access and use of data**. The smart home system must be able to limit access to only authorised users or devices and it should be able to prevent any unauthorised access to the devices. The secure user authentication and authorisation should be achieved to ensure the proper protection of both, data and system. Furthermore, the device authentication should also be considered in order to prevent any malicious devices from joining the network.
- **Ensuring the accountability of personal data usage**. As required by laws [5], data owner should be informed when personal data is processed. By this, smart home system should be able to track and report all the abnormal activities in the system. For example, when someone accesses CCTV video stream or when people open the door or his bedroom, this activity should be reported to home owner.
- **Data processor responsibility**. If the smart home system is connected with third party entity such as, cloud service or other service provider, these providers must ensure all the data protection security required under the laws [5].

These legal requirements must be incorporated into the design of access control model in order to ensure the compliance with laws and avoid problem in the deployment phrase. Based on that vision, we propose the access control requirements, in next section, designed to control the information sharing between different smart devices in smart home system environment.

3.2 Access control requirements

Services such as home monitoring (camera), home automation (control over home appliances, home access, etc.), and home security (connected alarm system) 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. Hacking into cameras, violating privacy, and accessing content (pictures and movies) are some of the security threats introduced by the new era of connected homes. These violations of accessing the content of home automated devices can led to many dangerous outcomes. 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 smart home environment. Based on our studies (e.g. legal issue, propriety of smart home devices and scenarios), we classify the access control requirements into six main parts: general, usability, privacy, security, semantics/policy and implementation.

1. General requirements consists of four main requirements: extensibility, reusability, easy-to-manage and interoperability. These requirements reflex the nature of smart home system, which is a part of a large network/system and it is consistently evolved.
   - Extensibility: The smart home is rapidly involving and new devices with different features may come up. Thus, access control model should be general enough to support extensibility to add desirable features in the future.
   - Reusability: The policy reuse should be provided. The model should support the reuse of existing policies. For example, in case where old device is removed and replaced by the new one.
   - Easy-to-manage: The model should support the easy-to-control and understanding of policy definition and management given the background of smart home users. Majority of smart home users may have limited knowledge in IT.
   - Interoperability: With smart home, user can access smart devices through Internet (e.g. cloud service), it is inevitable that different could service providers may implement different models, hence, it is important that the future access control model can work with model without going through major modification.
2. Usability requirements consists of four requirements: easy-to-use (user-friendly), understandability, easy-to-administrate and easy-to-deploy. Since smart home system may be controlled by common people (people with less knowledge in IT), usability of the future model is really important. Complex model and system may not attract users, leading to less public support.
   - Easy-to-use (user-friendly): When in doubt, the simpler is better. It is important that the future model/system provides easy-to-use concept.
   - Understandability: The model should be able to support the simple policy definition, which is easy to understand for common people. Common people are the major smart home users.
   - Easy-to-administrate: In the cases of more complex access scenarios in smart home (e.g. renting house or apartment), home owner may act as administrator, defining the access control policy for the renter. Administrating the access control policy should be relatively easy so that common people can do the job.
   - Easy-to-deploy: This relates to the deployment of the access control system. The installation of the access control system in smart home can be done by technical person or home owner. However, if it is easy to deploy, it can be done by home owner, which can make it more cost benefit.
3. Privacy is considered as an important aspect in smart home since many smart home devices can pose privacy issues when deploying them, the most important of which are CCTV, smart door and GPS device. In some countries, privacy protection is considered as need-to-fulfil requirement for information system dealing with

privacy issue like smart home. Taking into account the privacy laws [5], future access control system should ensure two important things: Privacy protection and privacy assurance.

- Privacy protection concerns on how to protection private data in smart home system, how to control the access to different privacy-sensitive devices. Privacy-sensitive data, for instance CCTV stream, can be shared between different systems. For example, in the scenario where user accesses his CCTV stream remotely through cloud or service provider, how to ensure that data is well protected and it is not leaked while passing third party system. Usage control of personal data in smart home is also required since data generated from different smart device can be shared and used by different external system[1].
- Privacy assurance is one of the most important features in smart home that can increase individuals' trust and willingness to deploy and use such system. Privacy assurance covers the strategic planning related to information assurance, policies and guidelines in case of privacy violation. Risks assessments and management and Incident response and management are also part of privacy assurance. In order to accomplish privacy assurance in smart home system environment, two approaches must be used: Privacy-by-design and privacy-by-default.
  (a) Privacy-by-design, we need to take privacy into account throughout the whole engineering process when designing smart home starting from the design of privacy access control system to control and manage the smart devices as well as the data generated from those devices. The concept is an example of value sensitive design that takes human values into account in a well-defined manner throughout the whole process.
  (b) Privacy-by-default. Studies [13] have shown that users often don't understand privacy controls. Thus, the privacy-by-default concept should be introduced in order to protect privacy information of individual even with those who has no concern or not be award of it. "privacy by default" is expressed in Article 23 of the proposed EU Data Protection Regulation [5], for example, data controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

[1]External system is the system connected with smart home and provides supportive service. For example fire station system provides firetruck service to reported firing house.

4. Security is an important feature for access control system because if someone breaks the access control system, it means he can control the access to the entire devices in the system. Most of the smart devices used in smart home system are wireless and if the access control system is deployed at home it can be forged. Given its importance, three security features should be achieved: not-easy-to-forge, attack-resilience and attack-resistance.
   - Not-easy-to-forge, the future access control system should be able to address the forging problem. The mechanism against forging should be implemented in the access control system itself to prevent such thing from happenning.
   - Attack-resillience, attack is sometime inevitable, however, resilience to attacks is what the future access control system should achieve. The proper procedure or mechanism should be defined to recover or react in time of attack.
   - Attack-resistance, as stated before, in the scope of smart home system where devices are connected through wireless communication, the chance of attack is higher compared with wire network since in smart home network, physical connect may not be necessary. Attacker can just stay outside the home and tries to get through the network. Thus, resisting to such attack is important in order to provide a safe heaven for smart home user.
5. Semantic/policy. To prevent access to smart home system by unauthorised users or devices, we need to control the access by means of access control policy in which the access rules are defined along with some variables and constraints. This policy defined who or which devices can get access to the information of other devices in which circumstances. There are several requirements for policy definition.
   - Conflict-free. Given the dynamic nature of smart home where devices can joint and leave network easily. New devices may be added, the old one may be replaced by more advanced device. In smart home environment, devices are likely dependent; meaning devices need information from each other in order to perform an operation. Defining an access control policy for such scenario is complicated and conflict can happen. Thus, to ensure the well functioning of the system, policy conflict should be addressed properly.
   - Non-redundancy. Old device can be replaced by new one, the new access control policy may need also to be created for new device. The new policy and the old one are actually the same since it applies to the same type of device. If the new one is created and at the same time keeping the old one, the policy redundancy can happen. The future access control system should consider this problem in order to provide the optimal performance of the system.
   - Multiple policies. As stated before, in smart home environment devices are dependent. Multiple policies of dependent devices should be combined in

some easily-understood way (e.g. union or intersection). For example, when the smoke alarm rings and the temperature rises, the water pumping actuator should be activated. The access control policies applied for smoke detector and temperature detector should be combined.

- Group-based. Given the dynamic nature of smart home system where different users and devices may involve in the system, it is not natural and management troublesome to assign the access control policy to the individual person or device because person can be frequently changed (e.g. home renting scenario), devices can also be replaced or added (e.g. replace old smoke detector sensor by a more sensitive one). The abstract group should be created and policy assignment should be linked to that group. The individual person or device is assigned to the group. With this arrangement, any change in group structure does not harm the policy assignment to the group, consequently it provides an easy-to-manage environment for the smart home user.
- Expressiveness. In smart home environment, the access control policies applied to devices or users should be flexible in order to respond to the dynamic nature of the system. It should be able to express the access control policy for different access scenarios involving different constraints and contextual information that may require in policy expression.
- Fine-grained. The simple and high level policy expression may not be sufficient given the complex nature of access control and security required in smart home system. The more granular policy expression that takes into account all the aspects of control such as privacy, safety, contextual information, etc. is required in order to fulfil the security requirements in smart home system environment.
- Constraint-based. In general, the decision to allow or deny access to devices is based on many constraints. For example, to activate the water pumping machine in case of fire, the information from temperature and smoke detectors are the important constraints. Constraint plays an important role in sharping the access control policy and provides a fine-grained access control policy.
- Privilege-expression. The future access control system designed for smart home should be able to provide the privilege expression that allows the distinction of access rights between different group of users. For example, the different access rights between the house owner and renter or the different rights between house owners and visitors (friends).
- Delegation. This feature is important in house renting scenario where house owner may have to delegate some rights to the renter so that he can perform the permitted actions during his stay.

6. Implementation. When implementing the access control for smart home, two important requirements should be taken into account: Low computational power and fast-processing.

    - Low computational power, the choice of the access control system architecture and topology may have the big implication on the access control model and mechanism used in smart home environment. There are two possible options for access control system implementation: distributed and centralised system. Distributed system allows all the sensor to have its own access control model and the request is processed locally in the sensor. The distributed system has some drawbacks given the limitation of sensor for both memory and computational power. With limited memory and computational power, highly complex policy expression with many variables and constraint can not be used since complex policy always needs high processing power and time. Second option is the centralised system where all the device (e.g. sensors or actuators) are connected to a central access control server where every request must get though the server. The policy validation is performed at the central server, which acts as the middleware between user and devices.
    - Fast processing. Most of the communication in smart home scenarios are in real-time, hence, it is important to have the fast policy validation in order to perverse the real-time parameter.

Home automation is a step toward what is referred to as the "Internet of Things," in which everything has an assigned IP address, and can be monitored and accessed remotely. It gives user access to control devices in home from a mobile device anywhere in the world. The remote access to devices can pose many challenges in term of security, privacy and safety of house owners. The design of the access control model and ultimately the implementation of such model should be carefully addressed in order to comply with all the security and legal requirements. The requirements we presented so far represent all the necessary requirements that covers, in general, all aspects of smart home environment ranging from utilisation, privacy, security, policy expression and implementation. These requirements can be considered as the guidelines for access control system design and development.

4. RELATED WORK

Internet-connected devices in smart homes present both benefits and risks for users. On the one hand, researchers have found in qualitative interviews that smart homes can be used to help family members with special needs [8], demonstrate the success, ease the control of climate and irrigation systems and infrastructure [26], and save energy [19]. On the other hand, Internet-connected devices can create potential risks, allowing attackers to capture users' private moments [7], modify security systems, or prevent users from accessing their devices [9]. In general, capturing access-control preferences in a usable manner is a complex task. Existing access-control systems, that are deployed in the closed system, required high computational power and have privacy tolerance do not fit for the smart home requirements.

Most of the researches on access control in smart home proposed the access control model based on the small defined set of scenarios [7]. Some focus on security of data and do not consider the privacy and safety issue [8][13]. Others propose a simple model with less complex policy expression [13] by using the simple Access control list (ACL) [6]. Below are some searches on access control for data and devices in IoTs system environment.

Blase et al [7] studied the current state of access control for smart devices in homes. They present different access control models and then match those models to a very limited set of defined requirements from a small set of scenarios in smart home (e.g. lighting system). Finally they proposed to use role-based and delegation to control the access to smart devices in homes. The research discusses the interesting things, but do not address general access control requirements for smart home that involve not only access control to devices, but also security of the data and privacy. The role and delegation alone are not sufficient to cover all practical access scenarios in smart home.

Rahul et al [13] proposed the access control for IoT devices. They proposed the mechanisms to authenticate devices by means of tagging. Each device is tagged with a unique identity. The identity of each device is then hashed and stored in database. Each time device asks to joint the network, it needs to provide its identity, which is used to compare the identify stored in the database. Rahul used access control list as the mechanism to control the devices. This research focuses only on the access control to devices, but not the data generated from those devices.

Mehdi et al [11] proposed the access control model for IoT-Collaborative. The authors proposed two collaborative access control models: CollabRBAC and CollabABAC. CollabRBAC is based on the role-based access control model [12] and CollabABAC is based on the attribute-based access control model [15]. There is no privacy issue addressed in the design of these two models. The two access control models support the least privilege principle, separation of duties and contextual information expression. These are not new since the existing extended-RBAC [14] can also support these features.

Bruce et al [8] studied and identified the security issues in IoTs and proposed the authentication and access control to address the issues. The authors proposed the use of cryptography techniques and access control models such as RBAC to address the security issues in IoTs. In the paper, authors provides also a brief summary of different authentication protocols, which can be used in IoTs system. Again, the privacy and others important requirements are not fully addressed in this paper.

J.Sathish et al [9] conducted a survey of IoTs on security and privacy issues. Their work is partly related to our work since our interest is to bring together all the data and devices protection issues in IoTs including the security and privacy. The missing part of their work is that they do not address the privacy issue based on any legislations, instead they raised a general privacy concern in IoTs. This general concern may not be sufficient if we want to realise the deployment of smart home system. Different countries may have different legislations applied for the use and processing of personal information [3], hence, study those legislations is important.

5. CONCLUSION AND FUTURE WORK

In this paper, we outlined the general access control requirements for smart home system. Those requirements covers all important aspects for controlling the access to devices and data in smart home environment including the usability aspect, privacy, security, policy expression and implementation. These requirements can be used as the guidelines upon which the access control model can be developed.

Our future work focuses on the design and development of the elaborated access control model that can be used to address the general access scenarios in smart home environment. The smart devices management and fraud-avoidance (e.g. forged devices) issue will be also addressed along side access control model.

6. REFERENCES

[1] European convention on the human rights. http://www.echr.coe.int/Documents/Convention_ENG.pdf, latest access: June 2016.

[2] European charter of fundamental rights, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm, latest access: June 2016.

[3] 2014. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://www.dataprotection.ie/ Latest access: November 2016.

[4] . Iot privacy, data protection, information security. *White paper, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753* (2014).

[5] 2016. EU general data protection regulations, https://en.wikipedia.org/wiki/General_Data_Protection_Regulation, latest access: November 2016.

[6] 2016. Access Control List, https://en.wikipedia.org/wiki/Access_control_list, latest access: November 2016.

[7] Blase Ur, Jaeyeon Ung, Stuart Schechter. The current state of access control for smart devices in homes. *Workshop on Home Usable Privacy and Security (HUPS)* (24-26- July 2013). Newcastle, UK.

[8] Bruce Ndibange, Hoon-Jae Lee, Sang-Gon Lee. Security analysis and improvement of authentication and access control in the internet of things. St. Augustine, FL, USA.

[9] J. Sathish Kumar, Dhiren R. Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications 90*, 11 (March 2014).

[10] Kim, T. H.-J., Bauer, L., Newsome, J., Perrig, A., and Walker, J. Challenges in access right assignment for secure home networks. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security* (Berkeley, CA, USA, 2010), HotSec'10,

USENIX Association, pp. 1–.

[11] mehdi Adda, Jabril Abdelaziz, Hamid Mcheick, Rabeb Saad. Toward an access control model for iotcollab. *6th International Conference on Ambient Systems, Networks and Technologies* (2015), 428–435. ELSEVIER, ScienceDirect.

[12] Ni.Qun, Bertino, Elisa, Lobo, Jorge, Brodie, Carolyn, Karat, Clare-Marie, Karat, John, Trombeta, and Alberto. Privacy-aware Role-Based Access Control. *ACM Transaction Information and System Security 13* (July 2010), 24:1–24:31.

[13] Rahul Godha, Sneh Prateek, Nikhita Kataria. Home automation: Access control for iot devices. *International Journal of Scientific and Research Publications. 4*, Issue 10 (October 2014).

[14] Wainer, J., Kumar, A., and Barthelmess, P. Dw-rbac: A formal security model of delegation and revocation in workflow systems. *Inf. Syst. 32* (May 2007), 365–384.

[15] Yuan, E., and Tong, J. Attribute based access control a new access control approach for service oriented architectures (soa). *Workshop, Ottawa, ON, Canada* (April 2005).