Context Sensitive Access Control in Smart Home Environments

Sofia Dutta*, Sai Sree Laya Chukkapalli*, Madhura Sulgekar*
Swathi Krithivasan*, Prajit Kumar Das†, Anupam Joshi*
* *University of Maryland, Baltimore County*, Baltimore, MD, USA
{sofiad1, saisree1, madhus1, skrithi2, joshi}@umbc.edu
† *Cisco Systems Inc.*, Fulton, MD, USA
prajdas@cisco.com

***Abstract*—The rise in popularity of Internet of Things (IoT) devices has opened doors for privacy and security breaches in Cyber-Physical systems like smart homes, smart vehicles, and smart grids that affect our daily existence. IoT systems are also a source of big data that gets shared via cloud. IoT systems in a smart home environment have sensitive access control issues since they are deployed in a personal space. The collected data can also be of highly personal nature. Therefore, it is critical to build access control models that govern who, under what circumstances, can access which sensed data or actuate a physical system. Traditional access control mechanisms are not expressive enough to handle such complex access control needs, warranting the incorporation of new methodologies for privacy and security. In this paper, we propose the creation of the PALS system, that builds upon existing work in attribute based access control model, captures physical context collected from sensed data (attributes), and performs dynamic reasoning over these attributes and context driven policies using Semantic Web technologies to execute access control decisions. Reasoning over user context, details of information collected by cloud service provider and device type our mechanism generates as a consequent access control decisions. Our system's access control decisions are supplemented by another sub-system that detects intrusions into smart home systems based on both network and behavioral data. The combined approach serves to determine indicators that a smart home system is under attack, as well as limit what data breach such attacks can achieve.**

I. Introduction

Integration of Smart Home Automation devices into people's lives is on the rise. Innovations in this domain started with a goal of finding a more convenient way to carry out daily routines but have gradually evolved into necessities of life. Proclivity towards ease of use demanded that such systems be controlled via a press of a button, over the internet. Along with their convenience, these systems are vulnerable to attacks. They include several categories of SMART HOME DEVICES like, smart displays, smart refrigerators, smart cameras, smart doorbells, smart locks, smart smoke detectors, smart speakers, streaming devices and smart thermostats. Reports suggest that by 2030, there will be over 50 billion devices connected to the internet [1] and thus prone to attacks.

Smart home systems sense and generate a lot of data. Unfortunately, a lack of good privacy and security solutions for smart devices has been a major cause for concern and created significant access control challenges. Most IoT systems are built using deployed sensors that talk to proprietary APIs. Services exposed by APIs are also of a proprietary nature. On top of which, manufacturers provide intelligent applications driven by data, from those services. Such a vertical architecture, strictly controlled by manufacturers, hampers horizontal interoperability [2]. On the other hand, typical Smart Home deployments consist of heterogeneous collection of devices from several manufacturers. As a result, a comprehensive access control solution that permits user to constrain device operation is difficult to create. Such a solution also needs to be coupled with a system that detect attacks on the smart system it protects. For this aspect of the problem, we build on our previous work [3].

A related problem is that a lot of data gathered in home by smart devices is also shared with the cloud. In the past decade, several breaches have occurred that led to leak of millions of users' Personally Identifiable Information (hereafter referred to as: USER PII). The data breach at Yahoo affected 3 billion users [4]. Most leaks have occurred due to some fault of the cloud service provider. Despite all the leaks organizations have not declared that they will stop collecting users' personal information. Every violation of user privacy has been followed up with promises of better security in future. While that is commendable, it is also necessary to investigate better access control over USER PII. Specifically, enabling consumers to make appropriate choices in matters of what data will they allow to be collected by in home IoT devices to share with the cloud.

We use policies defined using semantic web languages, and grounded in attribute based access control (ABAC) models [5], to both control access to smart home devices and control the flow of data from these devices to the cloud. Such techniques have been used before in related work in domains like, mobile applications [6], [7], [8], smart meeting rooms [9], [10], [11], Online Social Networks [12], Internet of Things setups [13].

In this paper, we propose the creation of PALS (**P**rivacy via **A**noma**L**y-detection **S**ystem) a system focused on context sensitive access control over cloud data collection in SMART HOME ENVIRONMENT. It defines access control policies based on context that control the behavior of smart home devices and sensors. It also controls information flow to the cloud. For that aspect, we use as an example Google Nest's

privacy policy [14] and USER PII it collects, along with other user and environmental attributes to define ABAC rules written in the Semantic Web Rule Language (SWRL) [15]. PALS is capable of executing these ABAC grounded access control rules by reasoning over attributes of the user, environment, devices used, information collected to grant or deny access to USER PII data. Attributes also describe who or what is requesting the queried data. Our goal here is to enable users control over the devices, and the data that gets collected and uploaded to cloud-based services by their smart home devices. We have built a Knowledge Graph of concepts extracted from the privacy policy of cloud service providers and instances of those concepts that were detected to have potential privacy implications. Our Knowledge Graph (KG) was built on top of our previous work [16], [13], [6] that enhances the concept of CONTEXT in a SMART HOME ENVIRONMENT and includes new concepts of USER PII and SMART HOME DEVICES to help define rules for controlling data access. We have also presented several use cases where USER PII would potentially be at risk of leaking and their privacy can be protected via our ABAC policies.

The rule creation process in PALS is supplemented by a rule improvement system that uses anomaly detection in a SMART HOME ENVIRONMENT by analyzing network and behavioral data. The anomaly detection system presents its results to users in order to create a user feedback mechanism that might allow users to make better choices for their privacy and security. Users are able to do so in a manner similar to ones presented in our previous work [6]. Users of PALS can choose to handle their access control policy by adding, removing, generalizing or specializing the contextual antecedents in a rule. A study of the feedback process and it's results is beyond the scope of the current paper.

In the following sections, we will provide an overview of the PALS system and explain how our system implements a privacy preserving solution in a SMART HOME ENVIRONMENT by using facts generated by user input on results of an anomaly detection system. Following that, we discuss scenarios where we envision scenarios where PALS will be instrumental in leak of USER PII. In Section V, we discuss how a KG driven context-sensitive access control system could support better privacy reasoning over a broad domain of SMART HOME DEVICES and the data they send to their cloud back-ends. Finally, we conclude the paper with our vision of how PALS can better protect USER PII in the future.

II. RELATED WORK

Popular mechanisms for access control like Role Based Access Control (RBAC) [17] and Attribute Based Access Control (ABAC) [5] have been used to manage user data privacy and security in various domains. In the mobile domain, Ghosh et. al. [18] used semantically rich context models to manage data flow among applications. The CRêPE system [7] was one of the first implementations of ABAC models using XACML standard [19] for fine-grained context-related policy enforcement on mobile. Unlike the next set of work we discuss, CRêPE, didn't use Semantic Web for its ABAC rules. PALS extends the techniques learned in mobile domain to apply them to SMART HOME ENVIRONMENT and uses context-sensitive policies to define access USER PII when queried by cloud-based services. Our ABAC model's attributes represent the 'data being accessed', 'user context', 'device type' and an implicit query from a cloud-based service like Google Nest.

Kagal et. al. [9] have showed us how policy based security and distributed policy management can be used as an alternative to traditional authentication and access control schemes. Rei, a policy language described in OWL and modeled on deontic concepts of permissions, prohibitions, obligations and dispensations [20], [9], have used Semantic Web technologies to express what an entity can or cannot do and what it should or should not do. Access privileges in Rei are associated with users, agents etc. via credentials and entity properties. Thus allowing Rei to describe a large variety of policies ranging from security policies to conversation and behavior policies. In PALS we have defined policies that controls access to USER PII in a SMART HOME ENVIRONMENT when queried by a cloud entity. KAoS [21] uses description-logic-based ontology of a computational environment, application context, and policies using DAML. KAoS differentiated itself from others by supporting runtime policy changes and extensibility to a variety of platforms. In ROWLBAC [22], the Web Ontology Language (OWL) [23] was used to support the standard RBAC model and extending OWL constructs was used to model ABAC. All of these systems have used Semantic Web technologies for their implementation. In PALS, we use Semantic Web technology through a KG that enables us to define a hierarchical context model for users, devices and user data and contains facts added by our supplementary anomaly detection engine. Using this model and rules in the Semantic Web Rule Language [15] we are able to produce access control decisions in a SMART HOME ENVIRONMENT. In short, we have achieved goal of access control in a different domain with proven and effective techniques from other domains.

The hierarchical notion of context defined in this paper is an extension of our previous work [18] where the part_of relationship was defined for stating that a location is subsumed by another bigger location. In our Knowledge Graph for this paper, we have extended the relationship to define deeper hierarchy of location in a SMART HOME ENVIRONMENT and added the notion of subsumption to activity context and device types, as explained in Section III.

A model for context-sensitive policy based access control for IoT was presented in our previous work [13], where we proposed a system design that achieves such a goal for an IoT environment. We capture access control policies using the ABAC model represented in OWL. We used a vehicular IoT use case for describing our policies in that work. PALS tries to achieve capturing of policy modifications by detecting anomalies in a SMART HOME ENVIRONMENT and then presenting them for refinement to an administrator or user. The user can then choose to reject the anomaly as invalid, accept

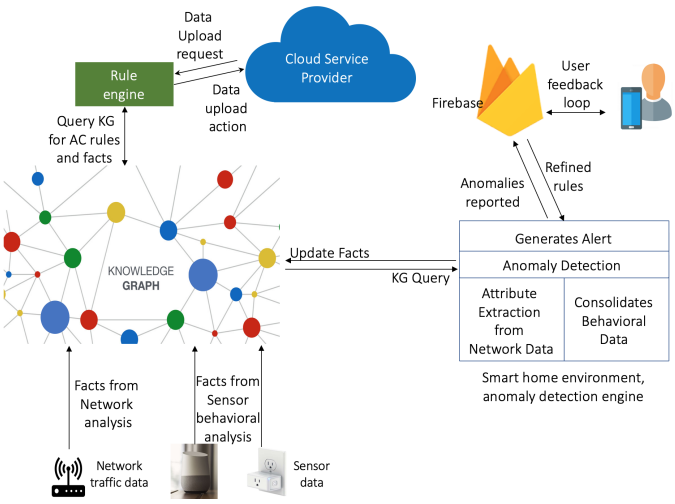

Fig. 1. PALS System Architecture

the anomaly as something that needs to be prevented or choose a more generic or specific contextual condition where the rule should apply.

Research from Ma et. al. [24] have indicated how a relatively small amount of information can lead to significant privacy leaks. Via this work we have attempted to show how a context-sensitive system that detects anomalies in data access patterns could use SWRL rules to protect against such side-effects leaks.

III. System Overview

In this section we focus on the system architecture for PALS. There are two parts to PALS. The first part consists of a KG that gets queried by a rule execution engine and allows us to reason over contextual facts and rules that are derived from privacy policies for cloud backed IoT systems like Google Nest [14]. The second part of the system includes an anomaly detection engine that detects potential attacks presents them to users and updates facts and rules in the KG. The system architecture shows the flow of access control decisions in PALS, when data is requested by a cloud service provider and updates to the KG are performed using information from the anomaly detection system, see Figure 1 for details. The anomaly detection system uses data collected from network traffic and sensor behavior in a Smart Home Environment. Our KG contains facts and rules that apply to a specific Smart Home Environment where our system is deployed. Using rules in access control policy for the current environment and monitoring the network and behavioral data, PALS is able to detect changes in data collected from the devices in the home. We then detect abnormalities in the data collection or device operation behavior with the help of an HMM model developed in our previous work [3]. An android app on the user's mobile notifies them of detected anomalies that might indicate a potential attack on their home's smart home setup. Facts about the detected anomalies are added into the KG to be used for refining rules in the future. The policy refinement is supported by the underlying ontology in our Knowledge Graph (described further in Subsection III-C). A deeper discussion on the policy refinement is beyond the scope of this paper but at a high level it involves using a human-in-the-loop machine learning mechanism that allows iterative modifications to access control policies in a Smart Home Environment, similar to our work in the mobile domain [6].

A. Monitoring Network Data

The PALS system monitors network packets and analyzes them to detect potential abnormalities and attacks. For example, a smart home device usually connects to a cloud service created or managed by its vendor, and smart devices from two different manufacturers do not interact with each other, unless explicit APIs exist for cross-device functionalities. In our work, we have incorporated Zeek [25], an open-source network analysis framework, to analyze network level activity. Logs generated by Zeek contain information about HTTP sessions, server responses etc. which can provide context for our access control policies. The inbound and outbound traffic is mirrored from router to Raspberry Pi for examining all the activities of devices. We identify network incidents such as monitoring the connections from certain IP addresses range, detect SSH Brute Force attacks, dropping the connections from specified subnets, etc. customized rules are written in Zeek scripting language. Even the intranet traffic is taken into consideration for monitoring to detect abnormal state. The network anomaly detection part of PALS then generates alerts for users to regard and decide whether a certain observed pattern is indeed an anomaly or not. The feedback is then used to update facts in the KG that can help in future access control decisions.

B. Behavioral Anomaly Detection

In addition to network analysis PALS, uses a model we developed, that captures behavioral anomalies that are not evident at the network layer. In order to create this model, the status of devices present in Smart Home Environment are fetched with the help of Google APIs [26]. The trained HMM model from our previous work [3] is used to detect anomalous behavior for devices in a Smart Home Environment. We do this by identifying abnormal sequences of device behavior and flagging potential attacks to users. For example, in an experiment we observed that the washing machine in our smart house got activated at 3 PM in the afternoon, when user was not at home. Our HMM model helped us detect this event as an anomalous activity because the Absolute Log Probability score for this event exceeded our threshold for normal behavior. PALS alerts users immediately via notifications from our Android app installed on their mobile device, if and when such an anomaly is detected. Any anomaly detected by sensors are also stored in the KG and after obtaining feedback from users, facts about the event and if needed, associated rules are appropriately updated. The updated facts and rules help PALS

better handle user privacy and security in the future, and avoid any potential risks from data leaks.

C. Knowledge Graph for Access Control Decisions

Context has been defined by Dey and Abowd [27] as:
Definition 1:

> "[...] any information that can be used to characterize the situation of an entity (i.e., identity, location, activity, time). An entity is a person, place, object or events that is considered relevant to the interaction between a user and application, including the user and applications themselves."

In PALS, context definition is extended from our earlier work [6], but with a focus on a SMART HOME ENVIRONMENT. We have created a Knowledge Graph with concepts that describes the SMART HOME ENVIRONMENT by extending the W3C IoT-Lite [28] and Semantic Sensor Networks ontologies [29]. This coupled with the ABAC ontology, allows us to capture physical context collected from sensed data (Attributes) about a smart home and then use this to define context dependent access control policies . We consider Location, Time, Activity, Roles etc. as the context related to the user and assign different properties to the sensors based on their functionalities. For example, CO Monitor will have a property named 'alarmStatus' value of which can be 'ON' or 'OFF', depending on the current status of the smart device. The Sensor knowledge graph stores collected real time data from the sensors or devices in the smart home. Our KG that defines the access control policies. We perform semantic reasoning over these attributes and context driven policies to decide if access should be granted to the user for a particular action, as described in section IV.

A modern smart home deployment allows creation of location as places that can be semantically associated with a home. Our ontology permits to capture these nuances in the context. For example, it makes sense to define a Home as a Place but a semi-private room might not necessarily be part of a home and the generic concept of a 'Room' does not semantically represent a place. So, we define 'Room' as a generic location while a 'Semi-Private Room', 'Private Room' and 'Public Room' as places. See Figure 2 for details. Activity context is defined in terms of Work related, Leisurely and Household. Each of these categories could be associated with varying levels of privacy and security needs, as we discuss in Section IV. Antecedents in our SWRL rules also take into consideration temporal context, as defined in our ontology. See Figure 2.

We have defined places in a SMART HOME ENVIRONMENT like study rooms and bedrooms, using the part_of relationship to semantically associate with the hierarchical notion of location within a home.

Our previous work [6] allowed us to preserve privacy by sharing data with varying levels of granularity, as specified in the policies. Granularity was controlled via usage of a more generic or specific value of location that allowed our policies to remain semantically consistent. We extended

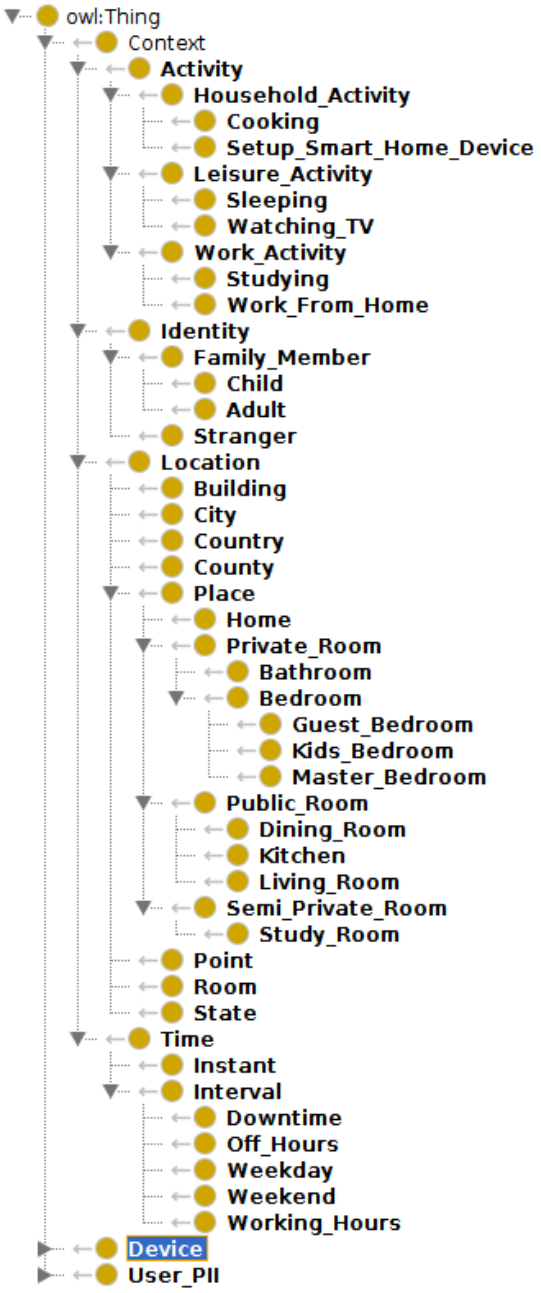

Fig. 2. Definition of Context in the PALS KG

the earlier semantic notion of lowest location specification from a "room" to go to deeper into a home. We achieved this by defining concepts of places within a home that are similarly defined using the "Part Of" transitive property to denote different levels of abstractions for location context in a SMART HOME ENVIRONMENT. That is, we previously defined location hierarchy as:

$$\texttt{country} \xleftarrow{\texttt{partOf}} \texttt{state} \xleftarrow{\texttt{partOf}} \texttt{county} \xleftarrow{\texttt{partOf}} \texttt{city} \xleftarrow{\texttt{partOf}} \texttt{home}$$

We have now extended the location related ontology, for

example, we have extended it to include rooms within a home as shown below:

home $\xleftarrow{\text{partOf}}$ semi-private room $\xleftarrow{\text{partOf}}$ study room

home $\xleftarrow{\text{partOf}}$ public room $\xleftarrow{\text{partOf}}$ dining room

home $\xleftarrow{\text{partOf}}$ public room $\xleftarrow{\text{partOf}}$ kitchen

home $\xleftarrow{\text{partOf}}$ public room $\xleftarrow{\text{partOf}}$ living room

home $\xleftarrow{\text{partOf}}$ private room $\xleftarrow{\text{partOf}}$ bathroom

home $\xleftarrow{\text{partOf}}$ private room $\xleftarrow{\text{partOf}}$ bedroom

home $\xleftarrow{\text{partOf}}$ private room $\xleftarrow{\text{partOf}}$ master bedroom

home $\xleftarrow{\text{partOf}}$ private room $\xleftarrow{\text{partOf}}$ kids bedroom

home $\xleftarrow{\text{partOf}}$ private room $\xleftarrow{\text{partOf}}$ guest bedroom

In our current ontology, we use the `owl:sameAs` property to incorporate certain classes and properties from the Platys [30], [6], [31], [32] and Place [33] ontologies. These ontologies have been previously used for defining user location and activity context in a hierarchical manner. Extensions of that are being applied to a SMART HOME ENVIRONMENT via the current work. See Figure 2 that defines activity generalization.

The context hierarchy enables policies to be defined as "Deny access to CRASH REPORTS when CHILDREN are involved in STUDYING" (Example 3.1 shows how this rule can be defined in SWRL using concepts and instances from the KG). The context hierarchy then allows us to generalize the rule to "Deny access to CRASH REPORTS when FAMILY MEMBER are involved in WORK ACTIVITY." This is particularly useful if we consider a situation where some families might care only about privacy when it comes to children, while others might care for everyone's privacy in the family. Such generalization enables powerful abstractions that can allow users granular and better control over their data in a highly personal situation like a Smart Home Deployment.

Example 3.1:

```
@prefix sme:<https://www.ebiquity.org/
ontologies/sme/0.1>.
@prefix swrlb:<http://www.w3.org/2003/11
/swrlb>.
sme:Crash_Reports(?requestedData) ∧
sme:familyMemberInRoom(?aMember) ∧
sme:ageOf(?aMember,?someAge) ∧
swrlb:lessThan(?someAge,"18") ∧
⟹
accessDenied(?requestedData)
```

In the next section, we discuss a number of these privacy use cases that apply to such a setup.

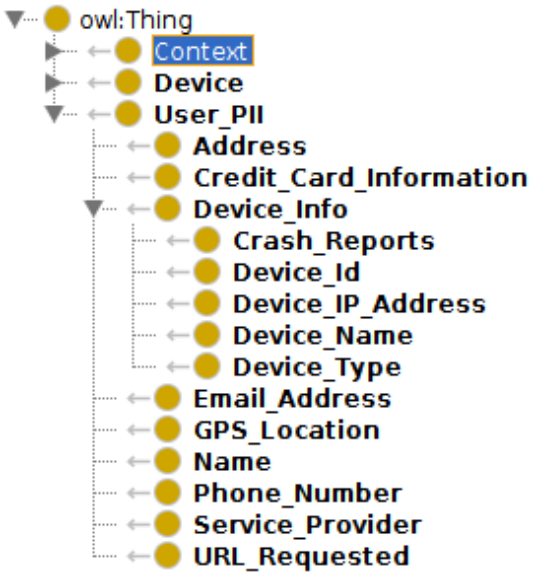

Fig. 3. Concept of "User PII" as defined in the PALS KG

IV. USE CASE SCENARIOS

PALS is a system that enables users control over their data. Here, entities that need to be protected are implicitly being queried by a cloud-based service that supports smart devices in a modern home. For this paper, we used Google's Nest line of home automation devices and from Nest's privacy policy [14], obtained information about data that they collect. We have already shown how our ontology allows us to express highly granular privacy policies using attributes that define contextual situations. Let's look at some situations where USER PII might be at risk and need to be protected. See Figure 3 for definition of USER PII as per Google Nest.

Use Case 1: *Deny regular collection of data that could allow inference of* PHYSICAL ADDRESS. Google Nest claims that they require regular data collection of a number of pieces of information from their devices, including credit card information, name, email, device IP, GPS coordinates. While it makes sense that name and email might be required to be collected during setup steps but it does not make sense for these to be collected regularly. Additionally, device IP, GPS coordinates and credit card information can leak actual physical address of a user. Therefore, we believe that we should always deny access to data that might reveal such information, and most certainly not allow this to be collected at regular intervals.

Use Case 2: *Deny access to data that could allow inference of schedule for* CHILDREN. When it comes to a home environment, users will most probably want strict control over data collection about minors. Particularly when children come home or leave for school or other activities that might let inference to be made about their schedule.

Use Case 3: *Grant access to* EMAIL, PHONE NUMBER, DEVICE IDENTIFIER *data during activity* SETUP SMART HOME DEVICE. Our ontology does allow the flexibility of

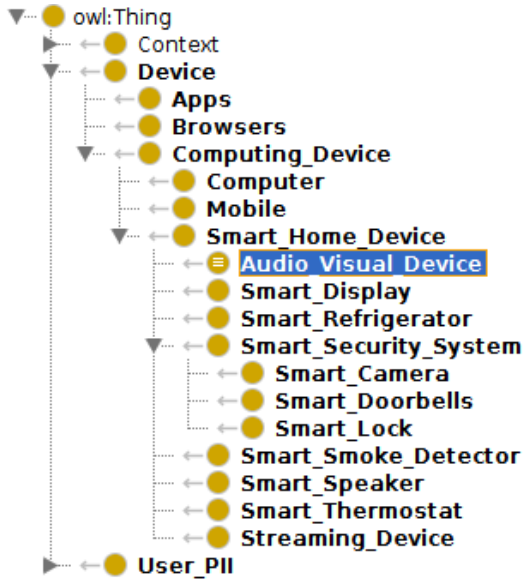

Fig. 4. Concept of "Device" as defined in the PALS KG

granting access to some user data when it is absolutely required. At setup time it makes sense to allow information like email, phone number and device identifiers to be collected. However, we are still not allowing access to every piece of DEVICE INFO, as might be requested by the cloud backend.

Use Case 4: *Deny access to crash reports that could contain data of when the device was turned on during* WORK DAY. Access to crash reports could allow inference of schedule of people in the household. This is because the crash reports would typically contain information about when the device was started or stopped. During a typical work day kids might come to the house or leave during the day and uploading this data could lead to privacy leaks.

Use Case 5: *Deny access to physical* SMART SECURITY DEVICES *during* DOWNTIME *if user identity is* STRANGER. PALS also enables rules to be defined that can handle physical security of the home. Imagine that the users forget to lock the front door. Most modern smart home systems are capable of auto locking after a preset timeout period. However, such settings commonly require to be appropriately configured. Using a context sensitive access control system allows us to infer that it is in-fact an appropriate contextual configuration, i.e. DOWNTIME and protect users physical privacy and security. Our ontology defines physical security devices as SMART_SECURITY_DEVICES, which is a `owl:disjointUnionOf` SMART_CAMERA, SMART_LOCKS and SMART_DOORBELLS see Figure 4 for details. Additionally, we also define the concept of non-family members that should not have access to physical security devices in the home, specifically it is night time or DOWNTIME.

Use Case 6: *Deny access to* AUDIO VISUAL DEVICES *during* DOWNTIME *if user identity is unknown*. DOWNTIME would also signify that users would not want to be disturbed via unwanted video calls, a real possibility, given the existence of Google Nest Hub. Therefore, we have defined the concept of AUDIO_VISUAL_DEVICES that is a `owl:disjointUnionOf` SMART_CAMERA, SMART_DISPLAY and SMART_DOORBELLS. This allows us to define access control rules that group multiple device types into a single rule.

Let's also take a look at some use cases from an anomaly detection perspective.

Use Case 1: You can not access kitchen devices such as coffee machine, unless you are home. Typically, being home would be captured by sensing the presence of the users phone, and this context would modulate whether commands could be issued to the kitchen devices.

Use Case 2: Kids are not permitted to watch TV during 10PM-7AM. Using time from the system, commands to the smart plug controlling the TV will be blocked if they originate from a device associated with a child.

These use cases showcase how USER PII data can be protected from being leaked in a SMART HOME ENVIRONMENT via access control policies defined using Semantic Web technologies. Using our HMM model we are also able to detect anomalous scenarios where the user might want to create new policies or modify currently defined policies. Our hierarchical ontology definition allows for addition, removal, generalization and specialization of antecedents for access control rules as shown by the use cases above, for anomaly detection. Next, we discuss how our system PALS can be used in a broader scenario involving a more diverse category of devices from a variety of manufacturers.

V. BROAD APPLICABILITY

Using the context, device and user data definitions from our ontology it is possible to express complex sets of constraints in SWRL restricting access to devices or the generated data. Thus, it is a powerful tool for handling data privacy. Adding new concepts that define new types of devices are fairly easy. Generalization of context, device type and data entity also allows for creation of generalized policy that can protect against leakage from a broad class of devices or variety of manufacturers.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we described PALS, a system that provides access control in a SMART HOME ENVIRONMENT. It uses context sensitive policies that were created based off on online privacy policies available from cloud service providers like Google Nest suite of products. Our access control policies allows our rule engine to perform dynamic reasoning over user context, details of information collected by cloud service providers and device type on which the access request is received and generates as consequent an access control decision. Our system uses an anomaly detection engine to generate alerts about suspicious activities in a SMART HOME ENVIRONMENT. Using network traffic and sensor behavioral data we are able to determine the events that ought to be

brought to users' attention. A feedback loop allows us to improve our from sensors present in the cloud to identify deviations from the normal state.

In ongoing work, we hope to extend our model by generating additional anomalies to make it more robust and secure. Additionally, our initial policy generation process needs to be automated by collecting data from more service providers. To automate the policy generation process we envision creating an Named Entity Recognizer trained on Cloud Privacy policy terminologies. This will allow us to easily identify the privacy and security related terms that are being referred to by a service provider and might require to be protected.

ACKNOWLEDGMENT

This research was partially supported by a grant from NIST and the Maryland Industrial Partnerships.

REFERENCES

[1] FinancialNewsMedia. (2019) Why the internet of things (iot) platform market is expected to reach $74 billion by 2023. [Online]. Available: shorturl.at/yKMR4

[2] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for iot interoperability," in *2015 IEEE International Conference on Mobile Services*, June 2015, pp. 313–319.

[3] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, "Anomaly detection models for smart home security," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE, 2019, pp. 19–24.

[4] E. Singer. (2019) Cybersecurity lessons from the biggest data breaches of the decade. [Online]. Available: https://cloudacademy.com/blog/cybersecurity-lessons-from-the-biggest-data-breaches-of-the-decade

[5] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, no. 6, pp. 79–81, June 2010.

[6] P. K. Das *et al.*, "Context-dependent privacy and security management on mobile devices," *Ph. D. Dissertation*, 2017.

[7] M. Conti, B. Crispo, E. Fernandes, and Y. Zhauniarovich, "Crêpe: A system for enforcing fine-grained context-related policies on android," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1426–1438, 2012.

[8] S. Dietzold and S. Auer, "Access control on rdf triple stores from a semantic wiki perspective," in *ESWC Workshop on Scripting for the Semantic Web*. Citeseer, 2006.

[9] L. Kagal, T. Finin, and A. Joshi, "A policy based approach to security for the semantic web," in *International Semantic Web Conference*. Springer, 2003, pp. 402–418.

[10] H. Chen, T. Finin, A. Joshi, L. Kagal, F. Perich, and D. Chakraborty, "Intelligent agents meet the semantic web in smart spaces," *IEEE Internet Computing*, vol. 8, no. 6, pp. 69–79, 2004.

[11] L. Sun, H. Wang, J. Yong, and G. Wu, "Semantic access control for cloud computing based on e-healthcare," in *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*. IEEE, 2012, pp. 512–518.

[12] Y. Cheng, J. Park, and R. Sandhu, "A user-to-user relationship-based access control model for online social networks," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2012, pp. 8–24.

[15] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, and M. Dean, "SWRL: A semantic web rule language combining OWL and RuleML," World Wide Web Consortium, W3C Member Submission, 2004.

[13] P. K. Das, S. Narayanan, N. K. Sharma, A. Joshi, K. Joshi, and T. Finin, "Context-sensitive policy based security in internet of things," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016.

[14] Google. (2019) We want you to understand the types of information we collect as you use our services. [Online]. Available: https://policies.google.com/privacy?hl=en-US#infocollect

[16] N. K. Sharma and A. Joshi, "Representing attribute based access control policies in owl," in *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)*. IEEE, 2016, pp. 333–336.

[17] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," *arXiv preprint arXiv:0903.2171*, 2009.

[18] D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy control in smart phones using semantically rich reasoning and context modeling," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*. IEEE, 2012, pp. 82–85.

[19] S. Godik, A. Anderson, B. Parducci, P. Humenn, and S. Vajjhala, "Oasis extensible access control 2 markup language (xacml) 3," Tech. rep., OASIS, Tech. Rep., 2002.

[20] L. Kagal, T. Finin, and A. Joshi, "A policy language for a pervasive computing environment," in *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*, June 2003, pp. 63–74.

[21] A. Uszok, J. M. Bradshaw, and R. Jeffers, "KAoS: A Policy and Domain Services Framework for Grid Computing and Semantic Web Services," *Trust Management –Lecture Notes in Computer Science*, vol. 2995/2004, pp. 16–26, 2004.

[22] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham, "Rowlbac: Representing role based access control in owl," in *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '08. New York, NY, USA: ACM, 2008, pp. 73–82. [Online]. Available: http://doi.acm.org/10.1145/1377836.1377849

[23] S. Bechhofer, "Owl: Web ontology language," in *Encyclopedia of Database Systems*. Springer, 2009, pp. 2008–2009.

[24] C. Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, "Privacy vulnerability of published anonymous mobility traces," *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 720–733, 2013.

[25] Zeek. (2019) The zeek network security monitor. [Online]. Available: https://www.zeek.org/documentation/index.html

[26] Google. (2019) Smart home. [Online]. Available: https://developers.google.com/assistant/smarthome/overview

[27] A. K. Dey and G. D. Abowd, "Towards a better understanding of context and context-awareness," in *First Int. symposium on Handheld and Ubiquitous Computing (HUC)*, 1999.

[28] M. Bermudez-Edo, T. Elsaleh, P. Barnaghi, and K. Taylor, "Iot-lite ontology," *w3. org*, 2015.

[29] M. Compton, P. Barnaghi, L. Bermudez, R. GarcíA-Castro, O. Corcho, S. Cox, J. Graybeal, M. Hauswirth, C. Henson, A. Herzog *et al.*, "The ssn ontology of the w3c semantic sensor network incubator group," *Journal of Web Semantics*, vol. 17, pp. 25–32, 2012.

[30] P. Jagtap, A. Joshi, T. Finin, and L. Zavala, "Preserving privacy in context-aware systems," in *Semantic Computing (ICSC), 2011 Fifth IEEE International Conference on*. IEEE, 2011, pp. 149–153.

[31] P. K. Das, D. Ghosh, P. Jagtap, A. Joshi, and T. Finin, "Preserving user privacy and security in context-aware mobile platforms," in *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2019, pp. 1203–1230.

[32] P. K. Das, A. Joshi, and T. Finin, "Capturing policies for fine-grained access control on mobile devices," in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2016, pp. 54–63.

[33] L. Zavala, R. Dharurkar, P. Jagtap, T. Finin, and A. Joshi, "Mobile, collaborative, context-aware systems," in *Proc. AAAI Workshop on Activity Context Representation: Techniques and Languages, AAAI. AAAI Press*, 2011.