A Privacy Control Method based on K-Anonymity for Smart Home

Sopicha Stirapongsasuti[1] Wataru Sasaki[1] Keiichi Yasumoto[1]

Abstract: Smart home equipped with various smart devices (sensors, connected appliances, etc) is attracting attention thanks to its ability to provide smart services like automatic life logging, elderly monitoring and smart appliance control. It is very useful for a service provider to automatically identify daily living activities from sensor/appliance data in a home to provide such smart services, but at the same time it is risky for each home dweller (user) to upload all the data generated in a home because the high-privacy information might be exposed to malicious attackers. In this paper, we define a threat model for smart home users where a malicious attacker(s) can access all or part of the smart home data uploaded to the untrusted cloud server (service provider) and at the same time can physically observe part of the activities from outside through lighting over window, water/power meter counter, and so on, hence the attacker can identify the association between the data in the cloud server and the home by matching the uploaded data and the physically observed data. Then, we propose a privacy control method for smart home users to take measures to the threat. The proposed method is based on k-anonymity which is a well-known property of the data often used for protecting location privacy and guarantees that the attacker cannot narrow down the number of applicable people within k when trying to identify the person from the data. In the proposed method, targeting a residential area with a number of smart homes, for each pair (a, t) of an activity a and a time period t, the number of the homes/users which/who are doing a at t is computed as k and the value of k is shown to the inhabitant doing a at t for making decision on if he/she may upload the data of (a, t) to the cloud or not. In order to know an appropriate threshold of k for upload/no-upload for each pair (a, t), we computed values of k from the existing smart home datasets and asked 18 participants to answer upload/no-upload for each pair of activity and time period by showing the computed value of k. As a result, we confirmed that our method based on k-anonymity can help privacy control for activities data generated in smart home.

1. Introduction

A smart home or connected home has received much attention in the past decade due to expeditious development of sensors and automated appliances which can facilitate dwellers, especially elderly people. Smart home can provide smart services like automatic life logging, elderly monitoring, smart appliance control and so on. However, responses of sensors and electricity consumption of appliances reflect activities of daily living (ADL) performed by the dweller(s) of a home, hence it it not so difficult to extract a sequence of ADLs of the dweller through analysis of such sensor and appliance data (e.g., with machine learning). Automatically identifying ADL and its sequence occurring in a home is very useful for a service provider to provide smart services like elderly monitoring and anomaly detection, but it is risky for each home dweller (user) to upload all the data generated in a home because the high-privacy information (e.g., absent time/ sleeping time (risky for burglar), toilet time/ frequency, etc) might be exposed to malicious attackers and/or living activity patterns might be tracked by them.

In this paper, we define a threat model for smart home users where a malicious attacker(s) can access all or part of the smart home data uploaded to the untrusted cloud server (service provider) and at the same time can physically observe part of the activities (ADLs) from outside through lighting over window, water/power meter counter, and so on, hence the attacker can identify the association between the data in the cloud server and the home by matching the uploaded data and the physically observed data. Then, we propose a privacy control method for smart home users to take measures to the threat. The proposed method is based on *k-anonymity* [1] which is a well-known property of the data often used for protecting location privacy and guarantees that the attacker cannot narrow down the number of applicable people within k when trying to identify the person from the data. In the proposed method, targeting a residential area with a number of smart homes, for each pair (a, t) of an ADL a and a time period t, the number of the homes/users which/who are doing a at t is computed as k and the value of k is shown to the inhabitant doing a at t for making decision on if he/she may upload the data of (a, t) to the cloud or not. In order to know an appropriate threshold of k for upload/no-upload for each pair (a, t), we computed values of k from the existing smart home dataset from the Center for Advance Studies in Adaptive Systems (CASAS) [2] and asked 18 participants to answer upload/no-upload for each pair of activity and time period by showing

[1] Nara Institute of Science and Technology

the computed value of k. As a result, we confirmed that our method based on k-anonymity can help privacy control for activities data generated in smart home.

2. Related Work

The growth of implementing IoT devices causes some privacy issues. Recently, the news [3] has exposed the well-known smart speaker developed by Amazon called Alexa recording the couple's conversation and inadvertently sending it to the husband's colleague. Because Alexa implements the Natural Language Processing (NLP) to construct a virtual assistant, there is a possibility that Alexa mistakenly detected the conversation as a command to send the voice data. As such, the miss-operation in IoT device could greatly affect a user's trustworthiness to IoT devices. Even though researchers and developers could make an effort to invent new technology, it would be deplorable if there is no user because of the privacy leakage. This gives a significant advantage of a privacy control in IoTs and increases a high motivation to find solutions for this problem.

A lot of efforts have been made to establish trustworthiness to IoT devices. The key is how to protect security of IoT devices and user's privacy. For the security protection, a challenge is which state or layer of IoT architecture should be protected. Suo et al. [4] studied some research progress of security in IoT and provided a concept based on secure architecture consisting of perceptual layer, network layer, support layer and application layer. Perceptual layer is a layer that aggregates data through hardware such as sensors or embedded hardware. Thus, this layer needs authentication and/or data encryption to protect data transmission between node to node or node to server. A lot of encryption techniques have been proposed so far [5–9]. In the network layer, the security mechanism has much contribution against a variety of security attacks, e.g. viruses, man-in-the-middle attack, counterfeit attack, service attack (DDoS), etc. Several researchers proposed methods to protect security. Raza et al. [10] proposed an End-to-End (E2E) secure communication. Sivaraman et al. [11] provided a method to control privacy for smart home in network level using Security Management Provider (SMP). Also, an integration approach such as inter-connection model between IP enabled WSNs with the Internet [12] has been found in this layer. The next two layers, support layer and application layer have more interactions and affect users in terms of usability and data processing. This means both layers have a high importance to increase a user's trustworthiness. Because most IoT users who are not familiar with this area of study can not understand how the lower layers work, but they could determine or trust the quality of service/procedure in IoTs based on their closest layer. Therefore, improvement on security in both layers is the key benefit to maintain users and keeps our products/services for long-running. Support layer (or transport layer) is a layer that involves data processing, data transportation and implementing intelligent decision of learning network behavior. There are some studies in the support layer. For example, Kothmayr et al. [13] used the DTLS protocol to implement two-way authentication scheme for the IoT system. Hummen et al. [14] studied the use of certificates for peer authentication in the Web of Things. In the application layer, which has the most interaction to user than the others, ideas to protect security in this layer can focus on user authentication, password management and key agreement between network. In this paper, we focused on security in the application layer which has few studies but it is essential to users.

There has been proposed a method on privacy protection for IoT devices using anonimization technique. Malekzadeh at el. [15] presented an idea to secure the perceptual layer by using mobile data anonymization to remove user-identifiable features. This method greatly advocates IoT security and privacy, but there is still a privacy concern with monitored activities. For example, an attacker could access to a smart home database stored in the cloud[*1]. Also, if the attacker notices an activity in a database at specific time which matched one observed home, the attacker could identify dwellers and their activities from the database.

For privacy protection, a property of data called k-anonymity [1] is often used. There are many studies that guarantee k-anonymity in location data, but to the best of our knowledge, there are few studies to utilize k-anonymity to protect user's privacy in uploading the smart home data.

3. Proposed Method

In this section, first we define the target threat model for smart home and then describe the proposed privacy control method.

3.1 Threat Model

Assumptions on target area, homes and activities

Let $Area$ denote the target residential area. Let H denote the set of smart homes in $Area$. Let ADL denote the set of activity types that can occur in each home $h \in H$. Let $T = \{t_1, ..., t_n\}$ denote the set of time periods in a day, for example, we use the time periods: (0-6), (6-9), (9-12), (12-18), (18-20), (20-23), (23-0) for our experiment in Section 4. Let $s(a, t, h)$ denote the sensor data generated for activity a during the time period t occurring at home h. The user of h can upload the data $s(a, t, h)$ to a (untrusted) cloud server where the data is anonymized by changing h to a pseudonym h'. It is not possible to estimate h from h'. We assume that the pseudonym h' for h is changed every day. We assume that the server allows service provider(s) and possibly attackers to access the uploaded data.

Assumptions on attacker

An attacker(s) can wander over $Area$ and observe each home $h \in H$ from outside to infer an activity $a \in ADL$ performed by the user of h. Figure 1 demonstrates the overview of threat model.

[*1] Such database storing activities logs might be open to public and/or service creators, hence potential attackers can easily access such data.

Let $o(a, t, h)$ denote the physical observation of activity a during t at home h by the attacker.

The attacker(s) can observe the activity of h only in two consecutive time periods per day due to his/her budget/cost constraint. That means when the attacker obtains $o(a, t_i, h)$ and $o(a', t_{i+1}, h)$, he/she cannot get data for time periods t_1 .. t_{i-1} and t_{i+2} .. t_n

The attacker can access the cloud server and download a series of data $s(a, t_i, h'), s(a', t_{i+1}, h'), ...$ but cannot directly infer which home of H actually corresponds to h'

The attacker tries to perform the inference attack by matching $o(a, t_i, h)$ and $o(a', t_{i+1}, h$ and $s(a, t_i, h')$ with $s(a', t_{i+1}, h')$. When the attacker succeeds the identification of the home h such that $h = h'$, he/she will know (from the data downloaded from the server) the activities performed in other time slots other than t_i and t_{i+1} of the day without any additional cost (i.e., physical observation for these periods).

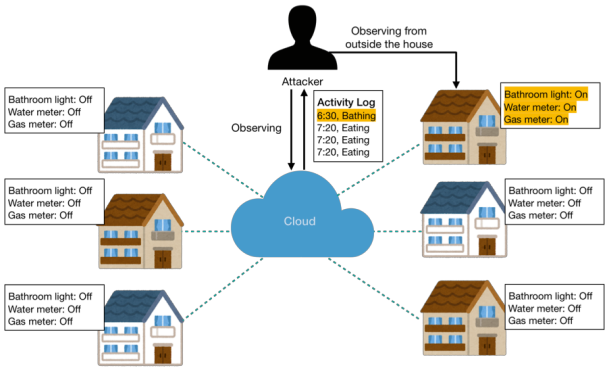

Fig. 1: Threat Model: an attacker who can download the activity logs and can physically observe houses from outside can identify the owner of the activity log.

3.2 Proposed privacy control scheme

Let us suppose that a home/user h is doing activity a during time period t and sensor data $s(a, t, h)$ has been generated. Now h needs to decide whether to upload the data $s(a, t, h)$ to cloud server or not. In this case, if there are sufficiently many homes/users in *Area* who are doing the same activity a at the same time period t, we can regard that it will be difficult for the attacker to identify h from the home just by matching the data with his/her observation.

Therefore, we employ *k-anonymity* [1] of the activity data as an index for controlling the privacy level.

Below, we show the proposed scheme to help each user make decision on upload or not-upload the data.

Step 1:Computation of k for each activity/time pair (a, t)

Step 2:Acquisition of upload decision for each activity/time pair (a, t) with k from user h

Step 3:Learning of upload decision for new pair of (a, t)

We describe some more detail for each step below.

Step1: Computation of k for each activity/time pair

If all data from every home $h \in H$ in *Area* are available, we can easily calculate k for each pair (a, t). In section 4, we show k values computed for the open smart home dataset from CASAS.

Step2: Acquisition of upload decision for each activity/time pair (a, t) with k from user h.

The privacy exposure level (i.e., data upload decision) will typically differ depending on k, the activity and the time as well as the user's subjective feeling. Therefore, it is needed to know what k is acceptable for each user and for each pair of activity and time period to upload the data. In section 4, we show our experiment to obtain the subjective threshold of k for upload of each pair (a, t) through questionnaire to participants.

Step 3: Learning of upload decision for new pair of (a, t)

Once we obtain decisions for many activity/time pairs from many users, we may be able to predict the decision for a pair (a, t) by a new user h' or for a new pair (a', t') by existing user with machine learning. This will be our important future work.

4. Experiment

In this section, first we explain the dataset used for the experiment and the method for computing k value with the computed results. Then, we design a questionnaire for knowing which k value for each pair of activity and time period is acceptable to upload the data by ordinary smart home users.

4.1 Computing k-anonymity of the open smart home dataset

We use 24 smart home open datasets from CASAS. These datasets include sensor data when the subjects spent their daily life in smart homes. We utilized the annotation of each activity in the datasets including start time and end time of activities. Some of the datasets could not be used for our purpose due to lack of annotation data. In addition, some datasets had an experiment with two subjects doing activities in the same home. Since we analyzed activities individually in order to evaluate k-anonymity, so we accumulated annotation data from 27 subjects in total.

However, each dataset in CASAS has unequal number of activity types because of the experimental designs. Some datasets have 30 activity types while the lowest number of activity types in a dataset is 5. To solve this issue, we selected five activities common in all the datasets, i.e. working, sleeping, going from bed to toilet, cooking, and eating. Morover, CASAS datasets used the time in UTC format and it is necessary to covert time format to local time to analyze activities based on the correct period of time in human's daily life.

Also, there is an issue of how to select the appropriate duration to compute k-anonymity. To compute k value from annotation data, activities of each dataset in smart home should be considered in day-by-day basis because our

method assumes that k value would be generated differently depending on subjects' routine in every day. For example, a subject A was cooking during 11.00-12.00 a.m. and a subject B was also cooking at that time on the third day of an experiment. While a participant C was cooking at the same period of time on the next day. In this case, the k value of cooking activity should be 2 for the third day and 1 for the forth day of an experiment. It is not appropriate to calculate k value as a sum (i.e., 3), since in this case an attacker(s) could identify the participant C by observing the home in the fourth day and matching the data from the cloud. Therefore, in this study, specifying the experiment duration is essential to investigate k-anonymity for each activity.

To determine a proper experiment duration, we reconstructed all datasets to contain only start time and end time of activities including the subjects' annotation. Then, we counted the number of days including each activity in each dataset. Finally, all datasets were combined into one dataset and we ranked the frequency of days including each of activities. The ranking showed that the top 10 of ranking is composed of duration between 10 days to 14 days of experiments.

To select a suitable duration, all activities duration are distributed to each hour and converted to histogram. Figure 2 shows the shapes of distribution of all days (top), 10 days (middle) and 14 days (bottom) of experiments. The y-axis denotes the normalized accumulated value and the x-axis denotes the hours in which the activity occurs, starting from 0.00 to 23.00. Although the shape of both shorthened periods (10 days and 14 days in the figure) are similar to the case of all days (top), the result of the absolute error (in percentage) reveals that 14 days case has higher error than the case of 10 days as shown in Table 1. Therefore, we chose 10 days to represent all datasets.

As k-anonymity is calculated for each activity occurring in specific period of time. So we need to define certain periods and investigate which activities occurred during a period. The different division for period of time could affect k-anonymity when analyzing datasets. Also, if periods of time are divided correctly, the result of analysis would provide a significance of k value on each period of time. In this work, we select periods of time depending on day-parting of TV program in UK. The reason is the TV program dividing periods by following people's activities. For instance, there are two periods of TV program called the national prime time which are 17.30 – 20.00 and 20.00 – 23.00. These periods are the peak time that have the highest number of people watching TV. Also, it can be understood that the national prime time is the time when people come back to their home. Thus, our decision choosing periods of time based on TV program could benefit in analyzing k-anonymity properly. Hence, according to the TV program in UK, time is divided to 7 periods, i.e. 6.00-9.00, 9.00-12.00, 12.00-18.00, 18.00-20.00, 20.00-23.00, 23.00-0.00, and 0.00-6.00.

The result of k values computed from the datasets is shown in Table 2. Each k value is the average of 10 days and it is rounded down to evaluate by questionnaire participants. Here, all k values are scaled by multiplying by 5 because a number of homes in open datasets are small and could affect the participants' answer. Hence, the total number of homes in the datasets is also multiplied by 5, that is $5 \times 27 = 135$. Moreover, the result of k values shows that in some periods of time, k value is zero (i.e., no activity occurred in the period of time). For instance, few dwellers could go from a bed to toilet during 18.00-00.00, while we could find a lot of people working from 12.00 to 18.00.

Activity	Duration	
	10 days	14 days
Working	35.96	39.91
Sleeping	24.11	24.2
Bed to toilet	46.64	37.44
Cooking	37.48	46.66
Eating	38.35	45.49
Average	36.91	38.74

Table 1: The percentage of absolute error compared with the case using all days data

4.2 Designing a dynamic questionnaire

Since we could not know if k value computed for each pair of activity and time period is suitable or not as the privacy level (i.e., uploadable or not) in the point of users' view. Thus, all k values computed for pairs of activity and time period need to be evaluated by the smart home dwellers. Thus, we decided to create a questionnaire to acquire participants' decision for upload to k value of each pair. We asked participants who had an experience in spending daily life in a smart home of our university [16]. All participants were shown the information about k value of each activity in the different periods of time. Then, they were requested to select if the activity happened in that period of time is reasonable to upload to the cloud.

According to our threat model, an attacker(s) is capable of observing 2 continuous activities from 2 continuous periods of time. Designing a static questionnaire would not support our concept of threat model because participants would have different opinions when selecting proper activities to upload to the cloud. For this reason, a dynamic questionnaire is an appropriate option to actualize our idea concretely.

In order to construct a dynamic questionnaire, there is an issue to consider: how to create an adaptive data when a participant selects since the first question (or the first period of time). The solution of this problem is to compute k value for a combination of two continuous activities. To clarify, when a participant chooses activities from the first period of time, the next period of time will be changed to calculated joint k value. That means every time when a participant makes a decision of selecting activities to upload, the joint k values are shown except the first period of time. The reason to let participants select activities from the joint k-anonymity is that we would like participants to consider the

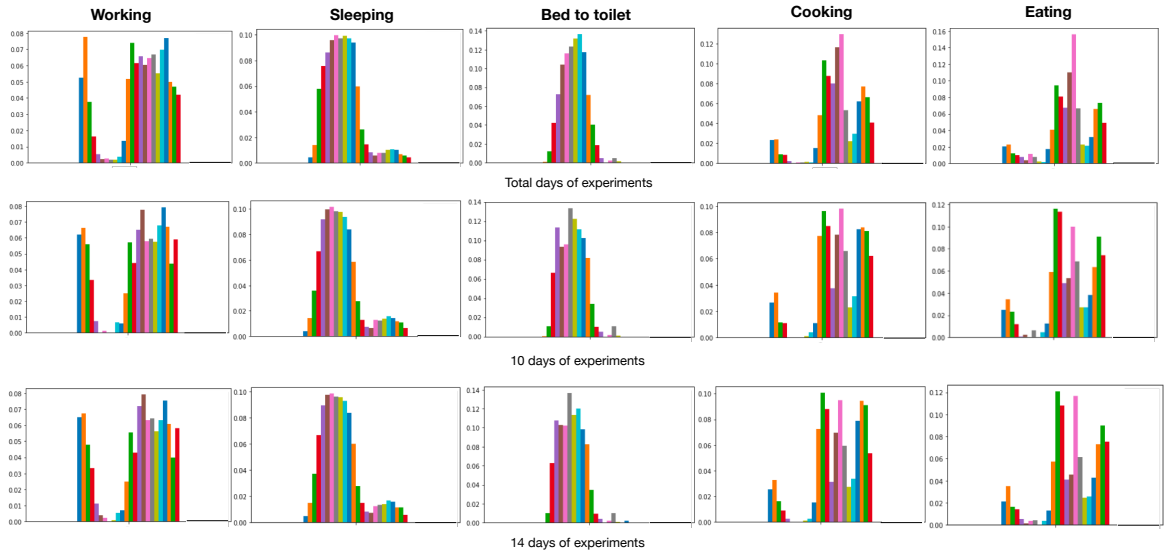

Fig. 2: The first row illustrates histograms of activities from total days of experiment duration and the next is from 10 days and 14 days respectively.

Table 2: k-anonimity by analyzing open datasets (the number of homes (the maximum value of k) is 135)

Activity	k value for each period of time						
	6.00-9.00	9.00-12.00	12.00-18.00	18.00-20.00	20.00-23.00	23.00-00.00	00.00-6.00
Working	10	15	65	35	45	10	45
Sleeping	25	40	25	15	15	0	50
Bed to toilet	40	30	10	0	0	0	25
Cooking	0	35	85	15	55	10	25
Eating	0	20	80	10	35	10	20

effect of continuous activities. In the first period, k values are set to the original values and in the second and later periods joint k values by using the following formula (here, we assume that 70 % of users doing some activity in the current period did some activity in the previous period). Here, $k_{i,j}$ denote the k value of j-th activity in i-th time period and k_i^{min} denote the minimum k value in i-th time period.

$$k'_{i+1,j} = min\{k_i^{min}, k_{i+1,j} \times 0.7\} \quad (1)$$

An adaptive questionnaire is developed by using an online survey development tool [17] which can generate a questionnaire as adaptive and collect answers from participants in real time. The questionnaire is distributed to 18 participants who had an experience and/or have a knowledge in smart home research and development. In the next section, we demonstrate the results from questionnaire and explain some significant results.

5. Result and Discussion

The participants who answered a questionnaire composed of 3 women and 15 men. They are from 23 to 53 years old and the average of participants' age is 28 years old. Figure 3 illustrates the result of uploading decision in terms of activity. According to the graph, the cooking activity and eating activity are uploaded to a cloud server more frequently than the others because participants decided to upload more than half of "not to upload." While the sleeping activity is prone to be a privacy information due to the "not upload" frequency more than the "upload" frequency. Considering k value evaluation based on periods of time, the top 3 ranking of "upload" answers are periods at 12.00-18.00, 9.00-12.00, and 18.00-20.00, respectively. This can be interpreted that most participants prefer to upload their activities during day time more frequently than night time. Especially at 23.00-00.00 and 00.00-6.00, most participants would like to protect their privacy due to frequent "not uploading" decision. It can conclude that the strategy based on K-anonymity in smart home can support a privacy control in smart home. However, there is a limitation to quantify the privacy level because of the user's preference. To solve this problem, we need to collect more data from participants. Also, we should apply the k-anonymity to other activities in smart home.

6. Conclusion

In this paper, we proposed a privacy control method for smart home users to help make decision on if he/she may upload the activity data or not, avoiding him/herself from identified by the attacker. The proposed method employs k-anonymity which is a property of the data that guarantees the attacker cannot narrow down the applicable people within k, and computes and shows the user the value of k (the number of homes which are doing the same activity) for his/her activity a performed during time period t for helping decision making on if the data may be uploaded to the untrusted cloud server or not. We computed values of k from the existing smart home dataset from CASAS and asked 18

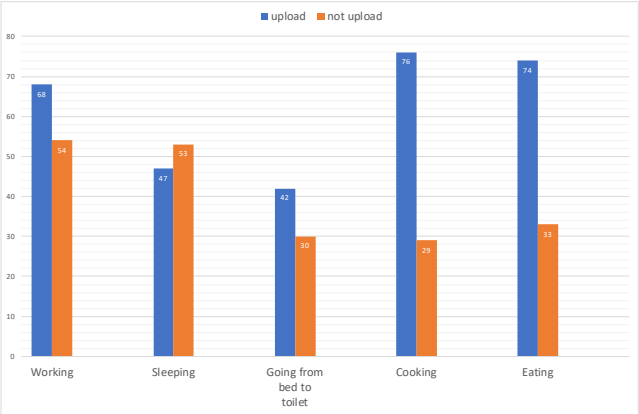

Fig. 3: Uploading decision from a questionnaire based on activity.

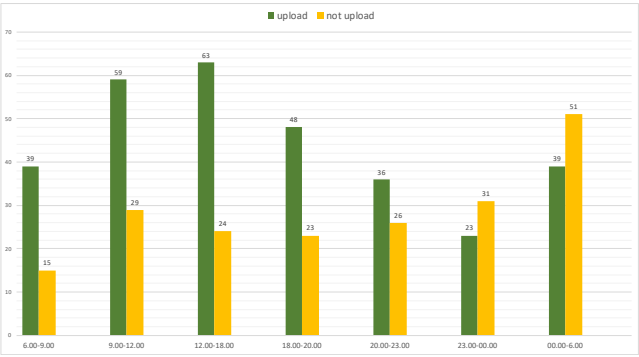

Fig. 4: Uploading decision from a questionnaire based on periods of time.

participants to answer upload/no-upload for each pair of activity and time period by showing the computed value of k. As a result, we confirmed that our idea of K-anonymity can support a privacy control of based on activities of a participants.

As part of future work, we are planning to build a machine learning model trained with the users' upload decision (for pairs of activities and time periods), which predicts the decision of upload for new user and for new pairs of activity and time period.

Acknowledgment

This work was partly supported by JSPS KAKENHI Grant Number 17KT0080.

References

[1] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, 1998.

[2] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan. Casas: A smart home in a box. *Computer*, 46(7):62–69, July 2013.

[3] C. Niraj. Is alexa listening? amazon echo sent out recording of couples conversation. https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html. Accessed: 2019-05-10.

[4] H. Suo, J. Wan, C. Zou, and J. Liu. Security in the internet of things: A review. In *2012 International Conference on Computer Science and Electronics Engineering*, volume 3, pages 648–651, March 2012.

[5] Xuanxia Yao, Zhi Chen, and Ye Tian. A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Computer Systems*, 49:104 – 112, 2015.

[6] Hossein Shafagh, Anwar Hithnawi, Andreas Droescher, Simon Duquennoy, and Wen Hu. Talos: Encrypted query processing for the internet of things. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, SenSys '15, pages 197–210, New York, NY, USA, 2015. ACM.

[7] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani, and P. Liljeberg. On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, 36(6):25–35, Nov 2016.

[8] R. Kotamsetty and M. Govindarasu. Adaptive latency-aware query processing on encrypted data for the internet of things. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–7, Aug 2016.

[9] Youssef Khazbak, Junpeng Qiu, Tianxiang Tan, and Guohong Cao. Targetfinder: Privacy preserving target search through iot cameras. In *Proceedings of the International Conference on Internet of Things Design and Implementation*, IoTDI '19, pages 213–224, New York, NY, USA, 2019. ACM.

[10] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig. Securing communication in 6lowpan with compressed ipsec. In *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, pages 1–8, June 2011.

[11] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and privacy control for smart-home iot devices. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 163–167, Oct 2015.

[12] J. Granjal, E. Monteiro, and J. S. Silva. A secure interconnection model for ipv6 enabled wireless sensor networks. In *2010 IFIP Wireless Days*, pages 1–6, Oct 2010.

[13] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brnig, and Georg Carle. Dtls based security and two-way authentication for the internet of things. *Ad Hoc Networks*, 11(8):2710 – 2723, 2013.

[14] René Hummen, Jan H. Ziegeldorf, Hossein Shafagh, Shahid Raza, and Klaus Wehrle. Towards viable certificate-based authentication for the internet of things. In *Proceedings of the 2Nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, HotWiSec '13, pages 37–42, New York, NY, USA, 2013. ACM.

[15] Mohammad Malekzadeh, Richard G. Clegg, Andrea Cavallaro, and Hamed Haddadi. Mobile sensor data anonymization. In *Proceedings of the International Conference on Internet of Things Design and Implementation*, IoTDI '19, pages 49–58, New York, NY, USA, 2019. ACM.

[16] Kenki Ueda, Morihiko Tamai, and Keiichi Yasumoto. Kenki ueda, morihiko tamai, keiichi yasumoto: A method for recognizing living activities in homes using positioning sensor and power meters. In *IEEE PerCom Workshops 2015*, pages 354–359, 2015.

[17] Devsoft Baltic. Online survey creator. https://surveyjs.io/Home/Licenses.