Semantically Enriched IoT gateway for Wearable Devices

Kangho Hur[1,2], Sangjin Shin[1], Sungkwang Eom[1], Minjae Song[1] and Kyong-Ho Lee[1]

[1]Department of Computer Science, Yonsei University, Seoul, Republic of Korea
[2]Software Center, Samsung Electronics
{khhur, sjshin, skeom, mjsong}@icl.yonsei.ac.kr,
khlee@cs.yonsei.ac.kr

Abstract. With the advance of wearable devices, an IoT (Internet of Things) gateway should support the efficient forwarding, processing, and provisioning of the streaming data obtained from them. We propose a semantically enriched IoT gateway working on a smartphone for wearable devices. The proposed gateway supports (a) an efficient consolidation and compression of heterogeneous streaming sensor data, (b) privacy preserving data processing by semantic reasoning, and (c) a selective data sharing through their social networks according to a degree of sensitivity. Experimental results with the prototype implementation show the potential of the proposed IoT gateway for novel user experiences based on semantic web technologies.

Keywords: Internet of Things (IoT), IoT Gateway, Wearable Device, Semantic Reasoning

1 Introduction

In the landscape of the Internet of Things (IoT), various physical objects such as wearable devices may be involved with their owners' social networks. Thus, wearable devices can be part of human social networks and even build their own social networks. This brings a new paradigm called Social Internet of Things (SIoT) [4], which integrates IoT and Social Network Services (SNS). In SIoT, as a bridge between heterogeneous objects and the Internet, an IoT gateway has a role of forwarding, processing, and provisioning the data streams generated by objects [2]. Especially, considering emerging wearable devices that cannot usually be connected to the Web directly, gateways are required to enhance the full potential of IoT/SIoT.

However, current IoT gateways don't provide semantic information related to sensor data which are distributed among various wearable devices. The data streams obtained from wearable devices containing privacy sensitive information such as heartbeat rate can be published and shared through the Web. They may cause an unintended exposure of private data. Thus, gateways should ensure the privacy-preservation of sensitive data [3]. In this paper, to overcome the limitations of existing gateways, we propose a semantically enriched IoT gateway working on a user's smartphone. The traditional semantic approaches were mainly performed on a server side (or cloud based) to guarantee better performance and accuracy. However, they do not guarantee the privacy-preservation of sensitive data.

2 The Proposed Architecture

As shown in Fig. 1, the proposed architecture is divided into three main layers:

- Data collecting layer (DCL): collects raw sensor data from wearable devices and consolidates/integrates raw data.
- Data abstraction layer (DAL): transforms the collected raw data into semantic data based on a domain ontology.
- Data sharing layer (DSL): shares the inferred semantic data with SNS groups depending on the sensitivity degree of data and the social distance from the groups.

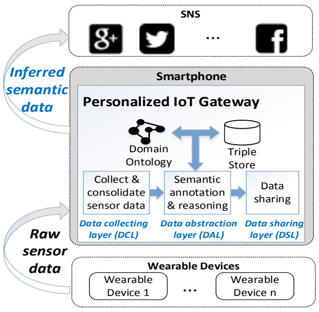

Fig. 1. Overall system architecture

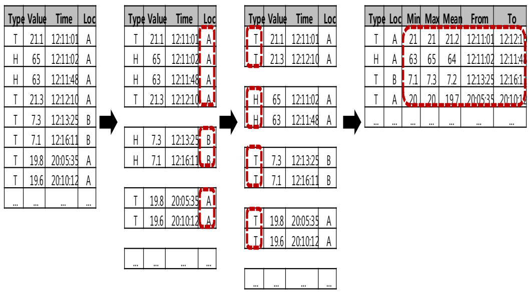

Fig. 2. Process of data archiving

2.1 Data collecting/consolidating layer (DCL)

Since wearable devices collect heterogeneous sensor data continuously in real-time, an efficient mechanism of storing and processing streaming data is very important; especially considering resource-constrained characteristics of mobile devices. To avoid processing a large amount of data on a smartphone itself, the proposed gateway transforms and merges the raw data in consideration of the time, location and sensor type, as shown in Fig. 2. In the first phase, we split streaming data into subsets with the same location (e.g., latitude and longitude). In the second phase once again, the streaming data is split into groups based on sensor types. Finally, we merge subsets into a single record that contains statistics information such as min, max, and avg. As a large volume of streaming sensor data is accumulated continuously, an efficient data compression is an essential for resource-constrained mobile devices.

2.2 Data abstraction layer (DAL)

Through DCL, the amount of data to be processed is reduced. However, the data representations should be more machine-interpretable. Thus, semantic annotation and reasoning on the raw data based on the proposed domain ontology (as depicted in Fig. 3) are required to draw an upper-level knowledge, in which privacy sensitive part is cut out. When semantic annotation is finished, rule-based reasoning is applied to the newly generated semantic data. We use AndroJena[1] as a reasoning engine. To perform rule-based reasoning, rules are defined in advance. Decision rules are defined in order to make upper-level conclusions, as shown in Table 1.

---

[1] https://code.google.com/p/androjena/

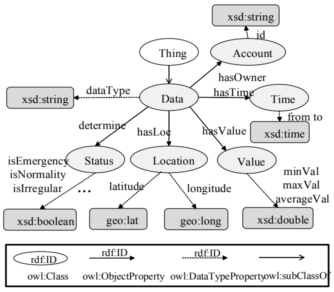

Fig. 3. A part of domain ontology

Table 1. A part of decision rules

Decision rules
[**emergency**: (?h datatype heartBeatRate), (?h hasValue ?val), lessThan(?val, 10) → (Status isEmergency true)
[**heartbeatIncreasing**: (?h datatype heatBeatRate), (?h hasValue ?val), greaterThan(?val, getLatestValue(heartBeatRate)) → (Status isHBRIncreasing true)
[**needExcercise**: lessThan(getTodayTotalValue (steps), 5000),greaterThan(getTo dayTotalValue(steps),2500) → (Status isInactive true)

Table 2. Data type and classification

Lv.	Description	Data type
L1	Cannot be used to track a user's status	temperature, humidity, illuminance
L2	Can be used to track a user's status	time, location
L3	May indicate a user's heath status indirectly	steps (calories)
L4	May indicate a user's health status directly	heartbeat rate

2.3 Data sharing layer (DSL)

In DSL, the upper-level knowledge is shared with SNS groups depending on the sensitivity degree in terms of privacy and social distance. The social distance is the degree to which users are willing to associate with whom have different social characteristics. Much research about the correlation between the social distance and the data sensitivity reveal that they are in inverse proportion [1]. For instance, in case of less sensitive data such as air temperature or humidity, they may be shared with the public. In case of more sensitive data such as calorie consumption, only friends may get access to them. For highly sensitive data such as heartbeat rate, the allowed audiences are limited to special groups (e.g., family members and practitioners), which are connected to the owner with stronger relation. Thus, we use the inverse proportionality between social distance and data sensitivity as the data sharing strategy.

3 Experimental Results

In order to evaluate the performance, scalability and feasibility, we have implemented the proposed IoT gateway on a smartphone. All experiments were conducted on Samsung Galaxy Note3 and Samsung Gear2. The actual data sets are provided by a smartphone and a wearable device. To enable selective data sharing, we classified the sensed data according to the sensitivity in terms of privacy. Table 2 shows the data type and classification (L1, L2, L3 and L4) used in our experiments.

3.1 Evaluation of streaming data processing

In order to evaluate the proposed method of processing streaming data, we collected more than 1,500 KB of data during 5 hours (18,000 records per each sensor type). Furthermore, experiments were conducted 6 times by changing range from 2m to 60m to evaluate our approach with different conditions. It means that the moving range can be used as a threshold value to split data set into groups based on locations. We measured the sizes of compressed data and compared them with those of original data. Fig. 4 shows the sizes of consolidated data. From the result, we confirmed that a user's low-mobility pattern leads to a better data compression performance. However, in case where the moving range is too short (2~5m), the consolidated data size is similar to the original one. The reason for this is that sensors generate data every second with different locations. As a result, records are not merged.

3.2 Performance evaluation of reasoning

We performed two kinds of experiments in the process of reasoning: 1) the memory consumption and 2) the processing time for different amount of input data. Fig. 5 shows the results in terms of 1) and 2). By increasing the amount of data step by step, we checked the changes of the memory usage. We found that there was no relation between the memory usage and the amount of data set. This is because the memory usage is mainly influenced by Android OS, which manages memory itself such as garbage collection. Also we measured the execution time for semantic annotation and reasoning. As shown in the result, for all the data sets, the processing times consumed by reasoning tasks were yielded as 47.2s, 77.9s, 172.6s and 449.9s, respectively.

3.3 Evaluation of selective data sharing

We also demonstrated the use of the proposed gateway through a real SNS scenario on Facebook. As shown in Fig. 6, a user's privacy information (as shown in the red box), which may indicate a user's health status indirectly, was allowed only to her friends. Non-private information (as shown in the blue box) was allowed to the public. The experimental result shows that 1) raw stream data were integrated and translated correctly into our semantic model 2) the target audience of the post was selectively determined by the degree of sensitivity as we defined.

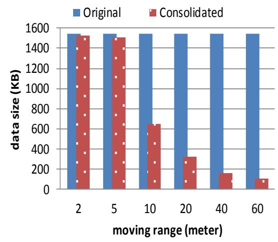

Fig. 4. Consolidated data size

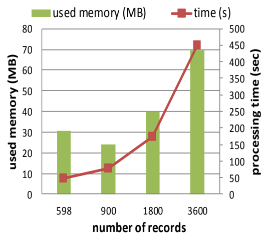

Fig. 5. Performance of semantic annotation/reasoning

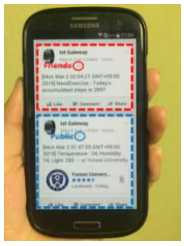

Fig. 6. Screenshot of publishing data on Facebook

Acknowledgement

This research was supported by the National Research Foundation of Korea (NRF) funded by Korea government (2013R1A2A2A01016327) and Samsung Electronics Co., Ltd.

References

1. Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., and Hubaux, J. P., Adaptive information-sharing for privacy-aware mobile social networks, Int'l Conference on Ubiquitous computing (UbiComp), pp. 657-666, 2013.
2. Carlson, D., Altakrouri, B., and Schrader, A. An Ad-Hoc Smart Gateway Platform for the Web of Things, IEEE Int'l Conference on Cyber, Physical and Social Computing (CPSCom), pp. 619-625, 2013.
3. Grzegorz J. Nalepa and Szymon Bobek, Rule-Based Solution for Context-Aware Reasoning on Mobile devices, Computer Science and Information Systems (ComSIS), 11(1), pp. 171-193, 2014.
4. Atzori, L., Carboni, D., and Iera, A., Smart things in the social loop: Paradigms, technologies, and potentials. Ad Hoc Networks, 18, 121-132. 2014.