)©2013 International Conference on Advances in ICT for Emerging Regions (ICTer): 185 – 188

My Sensors: A System for Secure Sensor Data Sharing over Internet

E.M.D. Siriwardane[1], Asanka Sayakkara[2], E.M.W.V.Ekanayake[3], Kasun De Zoyza[4]

University of Colombo School of Computing, University of Colombo
No. 35, Reid Avenue, Colombo 7, Sri Lanka

[1]dilangem@gmail.com, [2]asanka.code@gmail.com, [3]ekvijitha@gmail.com
[4]kasun@ucsc.cmb.ac.lk

Abstract— Privacy of sensor data should be considered since it is evidence for the behaviour and life style of the sensor owners. Some people attempt to store their data in the third party servers like the Cloud Computers. This is unsafe for the reason that user does not know whether third parties access their valuable data. Monitoring sensor data will be an essential for researches and several other aspects. In this research work, a mechanism is introduced for saving the information outside the Cloud severs while using the infrastructure of those servers. My Sensors system includes its own request handling mechanisms to access those data saved.

Keywords— Cloud Computing, Sensor Data, Data Store, Local Agent

I. INTRODUCTION

Accessing sensors through the internet is vital in view of the fact that the user is able to manage them even if the sensors are at a distant place. Smart sensor systems are capable of communicating through informative outputs. Hence those smart sensors can be connected to IP enable instruments. Most commonly used IP enable devices like smart-phones consist variety of sensors such as accelerometer, barometer, light sensors, etc. People attempt to accumulate the data detected to assist monitoring, controlling and maintaining the properties [1].

Today, cloud computing is a popular topic among the people who work in the information technology sector and the people who need more storage for saving their information. In cloud computing, particular storage and the software resources are provided for the end users. The data stored in those severs can be accessed from anywhere at any time, if an internet connection is available. It reduces the cost of storing, purchasing and maintaining the memory devises and servers [2]. Since the infrastructure of the companies which offer those memory spaces are larger, the small companies tend to acquire these services from cloud systems.

Even though the consumers achieve the above advantages, they are not aware of who the people deal with their personal information are. Third parties may have the access to the cloud machines. Those data may be stored in a place which is more than thousand kilometres away from the client. The end user may do not know where the servers are situated. Thus lack of control of consumer's own information is a major issue while the cloud services are consumed. There is no ensuring that customer is able to always access the stored documents. If the service of the cloud company is terminated it is difficult to get their data back [3, 4].

Sensor data is able to expose information of various activities to outside. Readings of the light sensor networks inside a house can facilitate to manage power inside it. As an example house owner can control the lights, routers and many more equipment's whenever he needs to do, while residing outside the premises. Inevitably this leads to save power. As this is one time data access, storing these data in a cloud server is not mandatory.

Google established Google app engine which allows the user to build own applications on the Google cloud platform. Variety of Application Programming Interfaces (APIs) are provided to ease the developing process of the web applications. In this research work, a technique is introduced for handling the users of the sensors in a secure manner. Google app engine simplify the mechanism of user handling. As Google has a rich infrastructure, the research project attempt to set up a methodology to share the sensor data with others via the Google app engine without saving the data within the cloud. The information will be saved outside the server for future use.

The rest of the paper is organized as follows. Section II describes how the system enhances the privacy of the sensor data. Section III introduces the techniques to optimize the request handling and standardize the requests with the TikiriDB. Section IV presents a discussion by comparing the My Sensors system with the related work. Section V mentions future works to improve My Sensors system. Finally Section VI concludes the paper.

II. ENHANCING PRIVACY OF DATA

A. Secure Data Transfer

The My Sensors application assumes that all the sensors and the users are members of the system. Each member must contain a Google account and they should register with My Sensors using Gmail address. Google App Engine makes the user handling and the authentication uncomplicated, utilizing a user handling API. That API is able to detect whether the members Signed-in and if not it redirects them to the sign-in page for signing-in or creating a new account [5].

Data integrity is a major issue of the cloud computing. The Cloud does not divide the data into sensitive data and common data. When the data is on a cloud, anyone from any location can access the data when it is required [6]. Accessing sensor data at any time provides security concerns. Therefore My Sensors System does not allow the users to get the data from the sensors at anytime. User should send a request to a particular sensor if the data is required. The owner of the sensor allows acquiring the information if he recognizes the person who sends the request.

978-1-4799-1276-6/13/$31.00 ©2013 IEEE

If the owner of the sensor accepts the request, he will show the available parameters of the sensor. User who needs data is able to select the parameter list desired from the data store of the sensor. Here our system defines parameters as all the information regarding a sensor such as date, time, location and detected values. But still the owner of the sensor can avoid accessing the data of some of the parameters preferred by the user. Above procedure can be summarized using the figure1.

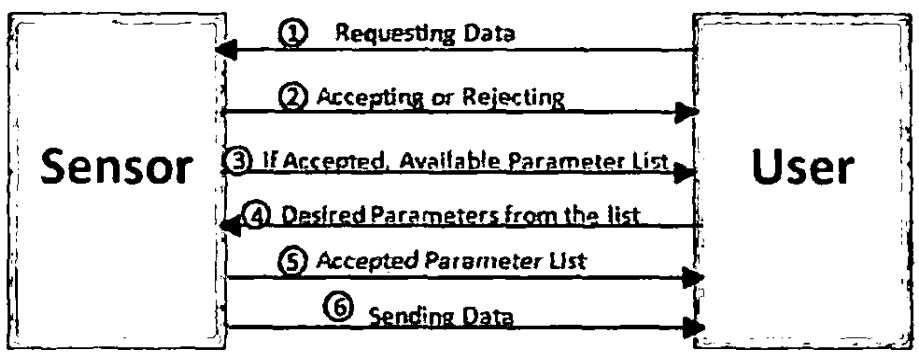

Fig. 1 The two way communication between the sensor and the user for initializing the data transferring.

Above procedure is convenient for data transferring since controllers of the sensors know exactly what the information is received by the receivers. Without the permission and availability of the owner of the sensor, any one cannot reach the data.

B. Secure Data Storing

As previously discussed, storing the sensor data in a cloud database is not safe. While the sensors detect the data, that information must be saved in a data store. Data store can be explained as a database in a system while data table stands for a table inside it. After the user acquires the particular information they desire, there must be a data store for saving. Since My Sensors avoid storing the information in a central database, the sensor and the user must have their own data stores.

My Sensors project isolates its members' data stores from the cloud network. For that purpose each member requires their own agents. Therefore making connection for transferring data means making connection between two agents. The figure 2 shows how the two agents are connected with each other.

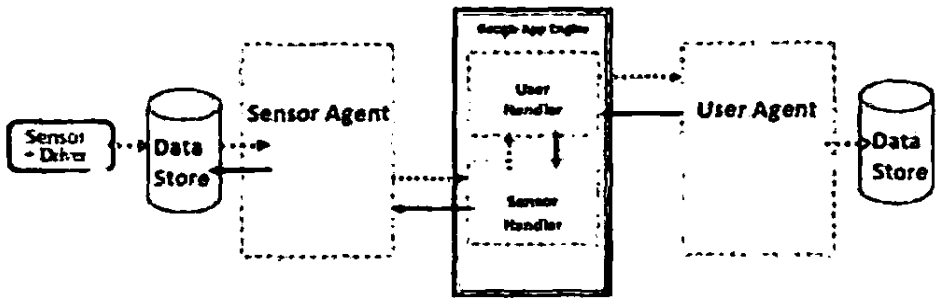

Fig. 2 The architecture of the system

The sensor and its data store along with the local agent, all are managed by the owner of the sensor. If the local agent of the sensor is disconnected then the receiver has no connection with the sensor side data store. This diminishes the possibility of stealing the data.

The sensor is controlled by a driver which collects data from the sensor and saves in the data store. The Sensor and the driver are independent from the rest of the My Sensors System. The owner of the sensor has the full freedom to make changes to the driver. Therefore controller is capable of controlling server as required and those drivers are located in the controller's personal devices like computers and smart phones. Those drivers are not stored in an intermediate server or a Cloud for handling the sensor. This minimizes the risk of running the sensor by a third party.

One of the advantages of the My Sensors System is anyone can combine any sensor with their own drivers to the system. The software elements of the My Sensors application only deal with the data store connected to the sensor. Therefore replacing a detector does not effect on the rest of the divisions of the system as far as data store and the tables are not altered.

Table 1 shows the structure of the table in the data store associated with the sensor. This research work identified three of the main requirements related to sensor data.

1. Requesting for past data
2. Requesting for current data
3. Requesting for future data

Requesting current data means user wishes for acquiring the data which is detected at the instant he sends the request. For this intention, controllers are able to offer direct access to the sensor. But this research work does not suggest connecting the sensor to the system directly. The sensor agent will state in the sensor data store when it require current data and driver check the data store persistently for verifying whether its agent need current data. Instead of linking the sensor with the sensor agent directly, a specific row of the table is utilized for saving the data and it is updated once a current data request is received.

The system is able to transfer data within a user defined time period which starts from the time when the request received. The example 3 of the section III clearly shows how the request must be sent to obtain the future data. If required the driver updates a particular row as stated above. Then the system get the data from that row in every specified number of seconds for the user defined time period.

C. Managing the Member Related Functions

As shown in the figure 2, Software system within the App Engine is divided into two parts. The classes which handle the user information and functions belong to the User Handler. must generate a specific session for the user and it must maintain the user related attributes until the user terminates the connection with the app engine.

Sensor Handler sustain the session of the sensor until the sensor is disconnected. The Sensor Handler does not allow the user access the web pages and sensor related software sectors. passes the warning and error messages while the users attempt to reach those unauthorized divisions of the system. If the user attempt to get into those areas at multiple times, the Sensor Handler makes a record and informs the sensor. Hence the owner of the sensor has the privilege to decide whether allow the particular user to acquire sensor data in the future.

III. Request Handling

A. *Prioritizing Multiple Requests*

At the same time as a sensor communicates with particular user, that sensor may receive requests from multiple users. Those requests must be queued for responding after the current data transfer. The controller of the sensor may confused while choosing the next user for sending the information. My Sensors Application introduces a method for making the best choice out of varies requests.

This research work recognized 4 major factors which must be considered for prioritizing the user requests.

1. According to user requested data type
2. Time taken for data transferring
3. Reliability of the user
4. Relationship between user and controller

Data transfer time varies with respect to the requested data type. Hence a predefined data type priority list is maintained in data store of "My Sensors" system to prioritize user sensor data requests.

If a specific user requires a large number of data then other users must wait for relatively long time until that data transmission is over. This is not reasonable for receivers who want only few numbers of data. Therefore the requests which intend to receive a small amount of data must be offered a higher priority.

TABLE I
THE STRUCTURE OF THE DATA STORE TABLE

Row No.	Para 1	Para 2	Para 3	Para 4	----	Para n
1						
2						
--						
m						

Number of parameters required by the user = x
Number of rows required by the user = y
Number of data= x.y
Thus if the product of x and y is smaller then higher priority must be given.

Reliability of the user is much important when the sensor data is shared. This can be determined by using the number of warnings given by the Sensor Handler during the past activities of the user within the My Sensors System. If there is a higher number of warnings the system provides a lower priority even though that user requires lower number of data.

Relationship between the owner and a specific user can be determined by using email address of the owner. Due to the good relationship between those two parties, owner of the sensor may send the data to that receiver before sending to others in the queue despite the previous two factors.

Prioritizing the requests by the system is only a suggestion for the controllers of sensors to find out the next user from greater number of requests. The controller has the freedom to choose the next request. The My Sensors System will prioritize the requests utilizing only the first three factors because those factors can be determined as discussed above. Nevertheless the controllers of the sensors must prioritize the requests according to the 4th factor.

B. *Standardizing the Requests*

This research project attempted to use a query language for standardize the request. My sensors project should have integrated a query processor to the system for handling the queries. This query processor accepts, passes, and executes the syntax of the query language.

TABLE 2
DATA OF A POWER SENSOR STORED IN THE SENOR'S DATA STORE TABLE

ID	date	time	voltage	current	power
1	15-01-2013	12.01	231	0.15	34.65
2	09-01-2013	08.00	230	0.15	34.50
3	09-01-2013	20.00	235	0.18	42.30
4	10-01-2013	08.00	231	0.13	30.03
5	10-01-2013	20.00	234	0.16	37.44
6	11-01-2013	08.00	230	0.12	27.60
7	11-01-2013	20.00	234	0.15	35.10

Table 2 shows the voltage, current and power data measured by a power measuring sensor. As a standard the present sensor data are saved in the first row. As explained previously, this row must be updated if any current data requests are found by the driver. For standardizing requests the data store and the table associated with the sensors must be named according to a standard. The data store must be named as "sensors" while the table must be named with the email address assigned to the sensor.

Assume that the email address assigned to the power sensor is powerunit.05@gmail.com. The query language is almost similar to the conventional query language. Following statement shows a simple example (Example1).

```
SELECT date, time, power FROM
powerunit.05@gmail.com WHERE voltage > 230
```

TABLE 2
RESPONSE FOR THE EXAMPLE1

date	time	power
09-01-2013	20.00	42.30
10-01-2013	08.00	30.03
10-01-2013	20.00	37.44
11-01-2013	20.00	35.10

Following example (Example 2) shows a statement for requesting the present power data.

```
SELECT date, time, power FROM
powerunit.05@gmail.com WHERE id=1
```

The query language was modified to acquire the data, within a period of time after requesting data. TikiriDB query language semantics were referred while doing those modifications [7]. Query in the following example (example 3) returns date, time and power data in every 2 seconds intervals for duration of 8 seconds.

```
SELECT date, time, power FROM
powerunit.05@gmail.com SAMPLE PERIOD 2 FOR 8
```

IV. RELATED WORK AND DISCUSSION

Controlling sensors over internet is a new trend in the world. Smart home technologies are rapidly growing and those inventions are used for Home Automation and Energy Management and so on. Most of those systems transfer data over internet. The technology is widely used in sports sectors.

Various sensors utilized to monitoring sportsmen's activities to develop the standards of sports. As an example the sportsmen share their muscle and weight amounts with their teams on fitness networks to improve their skills [6]. If any opposition team have hands on such vital information, it will be a waste of their effort, time and money. My Sensors system can be used to produce such systems in a secure way.

IrisNet is a project deployed to solve several problems of transferring sensor data over internet. Its main objective is developing efficiency of the data handling of the sensor networks [8]. *SenseWeb* presents an open infrastructure for sharing and geocentric exploration of sensor information [9]. The thesis named *Handling Live Sensor Data on the Semantic Web* attempted to handle live sensor data in semantic web [6]. My Sensors Application can be recommended for those systems for enhancing the security of data sharing by altering some features of each system as required.

TikiriDB is a research work which allows sharing Wireless Sensor Network Databases with the advantage of multi-user access. Mainly it includes three modules a query processor, routing module and an access control module [7]. It allocates the user to make requests using queries. In My Sensors project the software system executes the functions done by those three modules. The User Handler and the Sensor Handler find the appropriate user for sending the data. This is the main function of routing module. As stated in section II My Sensors system control the access and it is a complicated process as discussed. Therefore there is a relationship between these two projects. Objectives and the architectures of the two projects considerably different. TikiriDB is for wireless sensor networks while My Sensors is designed for all the sensors which consist informative outputs. TikiriDB already has the multi-user accessing facility. My Sensors will be developed for handling multi-user access in the future.

The goal of the *Sensing Web* project is opening the data obtained from sensors to the public. According to the Sensing web project normal World Wide Web does not share the raw data and most of the information is manually edited by the humans. The Sensing Web directly communicates with the sensors and supplies the detected data to the users. It attempted to formulate a new world-wide social information infrastructure called Sensing Web since general web is not suitable for sensor data sharing [10]. My Sensors project also understood this unsuitability and invented a different mechanism for data sharing as described in previous sections. It shares the raw data over the general World Wide Web and there is no need of additional network. And direct communication between sensors and users is terminated as mentioned earlier.

V. Future Work

My Sensors project was developed for handling one user at a time. Since multi-user handling improves the efficiency of the system, the project will extend the research work for inventing a method of multi-user handling. In this project still only one sensor is considered per a controller. In the future, the project is looking forward to transfer data of sensor networks. Thus the owners of those sensor networks will be able to connect numerous sensors to the My Sensors System and achieve the benefits of secure data transfer.

VI. Conclusions

The My Sensors System consists a complicated system structure but the users and the controllers of the sensors are not allowed to experience the complexity. Using the query statements, the users are able to express what they require from the sensors clearly.

My Sensors application is capable of acquiring the past data from the data store connected to the sensors. There is no any direct connection between the sensor driver and the internet. Hence even if the sensor is disconnected the person who controls the sensor is able to send the past data stored. In this case the current data and the future data cannot be sent. If the internet connection of the machine associated with sensor is disconnected, any one does not use that machine cannot reach to the sensor data. Therefore storing the sensor data in a personal machine is safe rather than storing data in a third party server like Cloud servers. Hence the administrators of the sensor data stores have the opportunity of saving data safely and preventing user access by disconnecting the internet connection.

Numerous mechanisms were developed by several research projects for sharing sensor data over World Wide Web Since some of them does not considered the security issues, My Sensors is a system which can be utilized to enhance the privacy of data of those systems.

Acknowledgment

The authors of this research paper would like to acknowledge the past researches of the Sustainable Computing Research (SCoRe) group of University Of Colombo School Of Computing.

References

[1] Jr.B.F. Spencer, M. E. Ruiz-Sandoval,and Narito Kurata, Smart Sensing Technology: Opportunities and Challenges [Online]. Available: http://www.uscert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf

[2] A. Huth and J. Cebula, The Basics of Cloud Computing. (2013) [Online]. Available:http://www.uscert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf

[3] J. Stroup, Is Your Personal Information Safe in the Cloud? [Online]. (2013) Available: http://idtheft.about.com/od/Data-Security-Tech/a/Cloud Computing.htm

[4] N.C. Ellegaard, (2013) Cloud Computing. [Online].Available: http://www.itretsforum.dk/uploads/media/Drafting_Cloud_Computing_Contracts_by_Niels_Chr_Ellegaard.pdf

[5] (2013)The Users Python API. [Online]. Availbale: https://developers.google.com/appengine/docs/python/users/

[6] T. Hummel, "Handling Live Sensor Data on the Semantic Web," B. Eng. thesis, Faculty of Economics and Business Engineering Institute of Applied Informatics and Formal Description Methods, Karlsruhe, Germany, July. 2012.

[7] N.M. Laxaman, M. D. J. S. Goonathillake, K. De Zoysa., *TikiriDB: Shared Wireless Sensor Network Database for Multi-User Data Access*, IITC, 2010.

[8] S. Nath, A. Deshpande, Y. Ke, P. B. Gibbons, B. Karp, and S. Seshan. "IrisNet: An Architecture for Internet-scale Sensing Services.",2003

[9] Grosky, W.I.; Kansal, A.; Nath, S.; Jie Liu; Feng Zhao, "SenseWeb: An Infrastructure for Shared Sensing," MultiMedia, IEEE , vol.14, no.4, pp.8,13, Oct.-Dec. 2007doi: 10.1109/MMUL.2007.82

[10] M. Minoh,K. Kakusho, N.Babaguchi, and T. Ajisaka. "Sensing Web Project-How to handle privacy information in sensor data." In 12th International Conference on Information Processing and Management Uncertainty in Knowledge-Based Systems, pp. 863-869. 2008.