International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.79 (2015)

SPONGE: Tangible Device for M2M Data Collection in a Trusted Manner

Ki-Woong Park[1*], Sung Hoon Baek[2]
[1*]Dept. of Information Security, Daejeon University, Republic of Korea
woongbak@dju.kr
[2]Dept. of Computer System Engineering, Jungwon University, Republic of Korea
shbaek@jwu.ac.kr

Abstract— In this paper, we presents a tangible device termed *SPONGE*, enhanced with a novel interface driven by grasp-and-release actions. Pressure sensor, TPM (Trusted Platform Module), MCU with communication modules are deployed into the tangible device for collecting data in a M2M and trusted manner. The user can collect data more intuitively by grasping and releasing it by hands. In addition to that, one directional data collection mechanism enhanced with TPM makes it possible that even the users of *SPONGE* cannot modify or falsify the collected data. From our design of the *SPONGE* and its tamper-resistant data collection procedure, we built a prototype on an embedded system, which make the vehicle data collection system more objective.

Keywords: Machine to Machine (M2M) Communication, User Interface, Trusted Platform Module (TPM)

I. INTRODUCTION

In the provision of services under Internet of Things (IoT) paradigm, the objects of everyday life will be equipped with tiny sensing, computing, and communication modules. They frequently take part in communication for providing interactions with each other [1]. In an attempt to provide an intuitive data collection mechanism in a M2M and trusted manner, we presents a novel interface driven by grasp-and-release actions. Our design goal is to facilitate the data collection from the multiple computing devices by providing an intuitive interface using tangible device, namely *SPONGE*. Like the commonly performed absorbing operation of a physical sponge, *SPONGE* provides an intuitive interface for collecting digital data such as operation log or text from IT devices. Consequently, *SPONGE* allows users to physically grab a digital object from one computing device and release it for collecting data from the computing devices.

In order to provide a trusted data collection mechanism in *SPONGE*, we propose a tamper-resistant data collection mechanism, which stores collected data and protects it against data forgery and false modifications. To achieve it, *SPONGE* exploits the trusted platform module (TPM) [2]. By means of the TPM-enhanced data collection mechanism, *SPONGE* can store the collected data in a secure storage region of *SPONGE*. This study is an extension of our previous work [3], in which we only focused on the user interface design and usability perspective as a mobile clipboard. Our objective in this study however, is to devise a trusted data collection mechanism for digital tachograph and to present killing application scenario for improving usability of *SPONGE*.

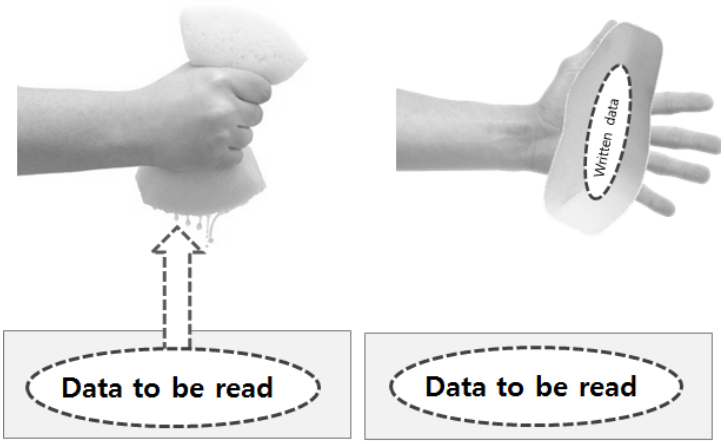

Figure 1. User interface of *SPONGE*: (a) grasp (read data from a device), (b) release (write data into *SPONGE*)

The remainder of this paper is organized as follows: In Section 2, we present the overall system design and conceptual implementation of the proposed data collection system. In Section 3, we illustrate an application scenario and the tamper-resistant data collection mechanism based on *SPONGE*. In Section 4, we present our related work. Finally, in Section 5, we present our conclusions.

II. SPONGE DESIGN AND IMPLEMENTATION

In this section, we present an overview of the proposed data collection system, termed *SPONGE*. We first introduce the *SPONGE* Interface of the proposed system and then describe its hardware and software architecture.

2.1 *SPONGE* Interface

This section presents proposed *SPONGE* interface. Figure 1 shows the interface by grasping and releasing device for collecting data from a computing device. In case of the grasping and releasing, the inside pressure of *SPONGE* device varies according to the grasping forces by the impact of grasping or releasing the device. The users' actions of grasping and releasing the device are mapped to read and store operations respectively just like grasping a sponge for absorbing liquid. When a user change the inside pressure of

the device due to the grasping force of user, the signal from the pressure sensor varies. Consequently, the signal which depends on the grasping performance is obtained by the output value from the pressure sensor.

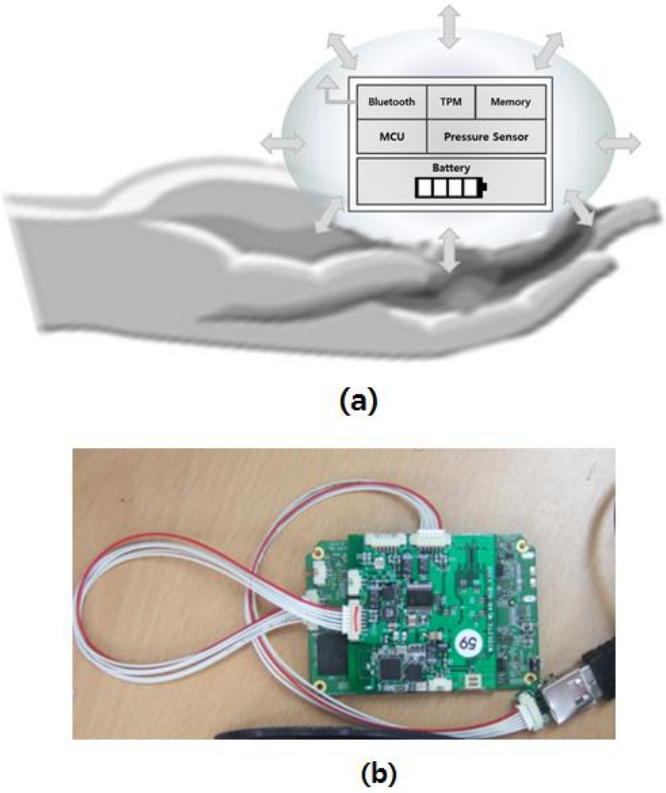

Figure 2. (a) *SPONGE* interface prototype, (b) Conceptual implementation

2.2 Hardware Architecture

To explore the benefits of the proposed data collection system that supports more intuitive read-and-store operations, we built the *SPONGE* device as a prototype. The *SPONGE* is a cordless that is designed mainly as a device for data collection with multiple computing devices in a M2M manner. Figure 2 shows an internal design and conceptual implementation. As shown in Figure 2-(a), the proposed *SPONGE* device consists of three sub-modules: the first one is a processing module, the second one is a sensor module and the last one is a communication module. As shown in Figure 2-(b), the processing module processes sensed data from the sensor module and then stores securely the received data into internal memory as a function of data collection system. The sensor module contains a pressure sensor on a flexible printed circuit board. In the soft-ball, all electronics devices are embedded on the substrate. This substrate is fixed by urethane sponge inside the soft-ball.

2.3 Software Architecture

In order to facilitate the *SPONGE* interface, we have developed a device driver for hiding the internal recognition mechanisms conceptually. It acts as an independent storage device. All applications and devices have access to the *SPONGE* can easily transfer data within a *SPONGE*. The implemented driver provides a backward compatibility for the conventional clipboard interface. For example, an application can send/receive data to/from another application of the other computing device because the clipboard is connected via TCP and shared among multiple computing devices. This driver interface was written in C# on .Net Framework 3.5 [6]. The difference with a conventional clipboard operation is that SPONGE accumulates the received data permanently inside non-volatile memory in SPONGE.

III. Application and Trusted Data Collection

3.1 *SPONGE* Application

As an application scenario, we assume that a user want to collect data from a digital tachograph which is a device equipped to a vehicle that records its speed and location with the driver's activity such as the driving time, breaks patterns undertaken by a driver [4, 5]. Figure 3 shows typical usage of *SPONGE* between vehicle equipped with digital tachograph and *SPONGE* device. When a user grabs the *SPONGE* with contacting the digital tachograph, the data is then stored into a volatile memory in *SPONGE*. It represents a situation in which the *SPONGE* virtually absorbs the data. Finally, when the user releases *SPONGE*, the data is written to a non-volatile memory in *SPONGE*.

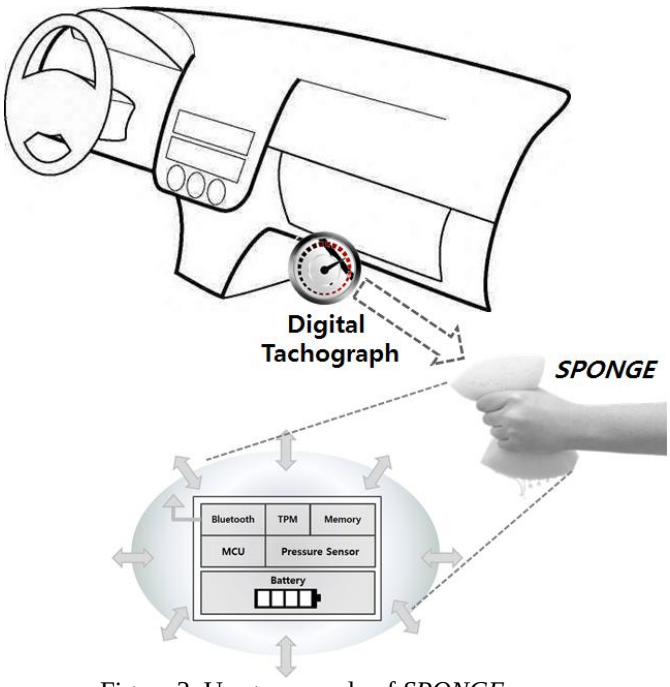

Figure 3. Usage example of *SPONGE*

3.2 Trusted Data Collection

SPONGE has a tamper-resistant data collection mechanism in which even the collectors cannot modify or falsify the

collected data. *SPONGE* exploits the trusted platform module (TPM). The TPM is a widely deployed security chip in commercial-off-the-shelf computing systems. It is designed for the purpose of secure storage and remotely determining the trustworthiness of a software stack [6]. More specific description of the trusted collection mechanism is described in [7] which is our previous work. *SPONGE* uses the following fundamental technologies of TPM.

- **Platform Integrity Measurement:** To ensure the trusted execution of *SPONGE*, we utilize a TPM. One of the important features of the TPM is a set of platform configuration registers (PCRs). The PCR values can only be changed by the *Extend()* function, which is an internal function of the TPM. It outputs a hash result with (current software stack + current PCR value), and then replaces the current PCR value with the output of this operation. To check the correctness of *SPONGE*, the TPM provides a *Quote()* function to return a digital signature of the current PCR values so that *Quote()* provides proof that the output of *Quote()* was generated on the correct software stack.
- **Secure Storage with the TPM:** The TPM provides a means of storing data in a secure fashion. The *Seal()* function encrypts the input data with a TPM key and specified PCR values. The *Unseal()* function decrypts the encrypted data only when the specified PCR values and the key are matched with the status of sealing [2]. *SPONGE* uses the *Seal()* and *Unseal()* functions to protect the stored data in such a way that the data can only be decrypted by *SPONGE* itself.
- **Data Integrity with the TPM:** The TPM has built-in support for a monotonic counter. The increments of this type of counter are in single steps, and the value of the counter is only incremented by the *IncrementCounter()* function. In addition, the TPM has a mechanism that creates a signature of the current tick value of the TPM. The tick data includes a signature of the current tick value and its update cycle [8]. These functions are utilized in our verification mechanism. The verification mechanism enables the central server to determine whether the *SPONGE* has been executed without a block or a data loss.

When we assume the above application scenario described in Section 3.1, a normal data collection mechanism may come at a price. For example, a collector may modify or delete its logged data for false modifications by counterfeiting the collected data from the digital tachograph of their vehicle [9]. As a remedy to the problem, we suggest a trusted data collection mechanism and deployed into *SPONGE*, which is protected against forgery and false modifications by collectors.

IV. Related Work

There have been several trials in seeking to find an adequate user interface which substitute existing interfaces such as mouse, keyboard and other ordinary input devices. Bricks [10] is a user interface that allows direct control virtual objects by physical handles for control. Illuminating Clay [11] is a clay type interface for real-time computational analysis of landscape models. If user alters the shape of clay, that depth of the clay works as an input to a library of landscape analysis functions through the ceiling mounted laser scanner. While the prior papers focused on the user interface for a domain specific application, this paper focuses on the general purpose tangible device to facilitate the copy-and-paste operation among the multiple computing devices for transferring data. For that reason, another related field of this work is an intuitive copy-and-paste operation scheme. InfoPoint [12] provides data transfer operation in the real world using hand-held device. The hand-held device has small camera which detects makers and files on the display of desktops or laptops. Using the cameras, buttons and wireless LAN, they implement drag-and-drop motion which provides the data transfer between two computers. In the point of transferring data, InfoPoint is fresh trial using new equipment. Through the learning from past experiences in order to provide tangible or intuitive user interfaces [13-15], this paper suggests that a physically grabbing object and the capability of using realistic hand interaction will enhance the intuitiveness of copy-and-paste interaction. Therefore, we suggested a sponge -type device and user interface to facilitate the data collection operation among the multiple computing devices by providing an intuitive interface, namely *SPONGE*.

V. Conclusion

In this paper, our aim was to present a novel interface driven by grasp-and-release actions, and its application as a mobile data collection system for interacting digital tachograph for intuitive data collection in a trusted manner. To accomplish this task, we proposed and designed a tangible device and its interface. In order to provide the trusted data collection, we deployed a TPM-based collecting mechanism in which even the users cannot modify or falsify the collected data. Consequently, the user can conduct a data collection from *SPONGE*-compatible devices more intuitively by grasp-and-release it by hands. The proposed system also can be integrated into server computing platforms as a black box for verifying system operations.

References

[1] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems 29.7 (2013): 1645-1660.
[2] S. Pearson and B. Balacheff, Trusted computing platforms: TCPA technology in context, ser. HP Professional Series. Prentice Hall PTR, 2003.
[3] K.-W Park, W. Choi, and K.H. Park, "SqueezeBall: Enabling Intuitive Copy and Paste using Soft Ball-Type Device as Mobile Clipboard," IEEE International Symposium on ISWC 2010, Late Breaking Results Session
[4] J. Ferreira, et al. "Wireless Vehicular Communications for Automatic Incident Detection and Recovery", Proceedings of the 10th Portuguese Conference on Automatic Control, Jul, 2012
[5] Schweppe, et al. "Security and privacy for in-vehicle networks", IEEE Vehicular Communications, Sensing, and Computing, pp.12-7, June 2012
[6] N. Aaraj, A. Raghunathan, and N. Jha, "Analysis and design of a hardware/software trusted platform module for embedded systems", ACM Trans. Embed. Comput. Syst. 8, 1, Article 8, Jan 2009.

[7] K-W. Park. "*T-BOX*: Tamper-resistant vehicle data collection system for a networked digital tachograph", IEEE ICT for Smart Society (ICISS), 2013
[8] D. Schellekens, et al. “Remote Attestation on Legacy Operating Systems With Trusted Platform Modules”, Electronic Notes in Theoretical Computer Science, Volume 197, Issue 1, February 2008.
[9] Kargl, et al. "Secure vehicular comm. systems: implementation, performance, and research challenges," Communications Magazine, IEEE , vol.46, no.11, pp.110,118, November 2008
[10] George W. Fitzmaurice, Hiroshi Ishii, William A. S. Buxton, “Bricks: laying the foundations for graspable user interfaces”, SIGCHI conference on Human factors in computing systems pp. 234 – 241, 1995.
[11] Matthew G. Gorbet, Maggie Orth, Hiroshi Ishii, “Triangles: tangible interface for manipulation and exploration of digital information topography”, SIGCHI conference on Human factors in computing systems pp. 49 – 56, 1998.
[12] Kohtake, N., Matsumiva, K., Takashio, K., Tokuda, H., "Smart Device Collaboration for Ubiquitous Computing Environment, Workshop of Multi-Device Interface for Ubiquitous Peripheral Interaction", UbiComp2003.
[13] Pintrac T et al., “SqueezeOrb: A Low-Cost Pressure-Sensitive User Input Device”, ACM symposium on Virtual reality software and technology, 2008
[14] Dinesh K. Pai et al., “Tango: A Tangible Tangoreceptive Whole-Hand Human Interface”, 1st Joint Eurohaptics Conference and Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems
[15] Ross T. Smith et al., “Digital foam interaction techniques for 3D modeling”, ACM symposium on Virtual reality software and technology, 2008