Journal of Engineering and Applied Sciences 13 (Special Issue 1): 2447-2451, 2018
ISSN: 1816-949X

A Study on the Technical Solution for Personal Information Protection in Telematics Environment

[1]Da-Un Chung, [2]Kyung-Su Yeo, [3]Sang-Hyun Kim and [4]Sang-Bok Lee
[1]Department of Smart Convergence Consulting, Hansung University, Seoul, South Korea
[2]Department of Information Systems, The-K Non-Life Insurance, Ltd., Seoul, South Korea
[3]Department of Mechanical Systems Engineering, Seoul, South Korea
[4]Department of Industrial and Management Engineering, Hansung University, Seoul, South Korea

Abstract: Along with the development of IoT, telematics technology has also been applied to automobiles. Thus was a risk of leakage and exposure of private information. The purpose of this study is to investigate a method to protect against the leakage and exposure of personal information. After examining the case in relation to the telematics environment, we define the personal information and propose a technical method to protect the personal information. We investigated the personal information generated in the telematics environment and investigated the vulnerability such as leakage or exposure to the generated personal information data and then studied the technical measures to protect the personal information data. That is to study the technical solution through application of data management framework to protect personal information in the telematics environment. It is possible to reduce the damage of personal information leakage caused by application of telematics technology and enhance the reliability of the telematics technology.

Key words: Telematics environment, telematics technology, private information extrusion, data management framework , protection of personal information, possible

INTRODUCTION

The development of both IoT (Internet of Things) technology and wireless network communication technology are changing from riding in the vehicle to cultural space elements with contents available. Vehicles that the technology is applied in the telematics environment are not only media that receives and uses various services with information but also transforming them into a subjective element to create, transmit and receive information. For this reason, a large number of companies from many fields are planning to integrate and utilize a variety of technologies in the telematics environment and to connect or utilize them in business (Francois *et al*., 2009).

In the telematics environment, the information and services that are used with vehicles and the various information generated are related to personal information. Such personal information is transmitted and received using various communication technologies such as wireless internet, sensor network, Bluetooth, satellite communication and so on. In this process, unencrypted or unmanaged personal information may cause accidents pertaining to loss, theft, leakage, tampering and damage (Nobuhiro and Manabu, 2014; Kaminski *et al*., 2011). For spreading and developing the telematics, created personal information data is safely managed and protected to be trusted from users. The purpose of this study is to investigate the threats regarding personal information and personal information generated in the telematics environment and to study the technical measures to protect personal information data (Eichler *et al*., 2005).

MATERIALS AND METHODS

Personal information

Personal information in the telematics environment: Personal information may be defined as information that identifies an individual in order to cause harm and damage about all such parts such as the individual's identity, property, physical body and social status.

In recent years, everyone knows about necessity of protecting personal information through various accidents and incidents. Furthermore, the importance of protection was emerged with the development of information and communication technology. It has been supplemented legally and institutionally and applied to

Corresponding Author: Sang-Bok Lee, Department of Industrial and Management Engineering, Hansung University, Seoul, South Korea

Table 1: Personal information of telematics environment

Types	Contents	Remarks
General information	Name, social security number, driver's license number, address	Driver information
Vehicle information	Vehicle type, vehicle price, vehicle driving record	
Communication information	Various communication information used in the vehicle	
Location information	GPS usage information	Navigation

each field on account of leakage and infringement of various personal information. The personal information produced in the telematics environment may be used for general information such as name, social security number, driver's license number, address, etc. used for various services, information related to vehicle such as vehicle type and vehicle value, e-mail, communication contents and location information related to the position information of the GPS or personal portable devices. Table 1 is types of personal information that can be generated in the telematics environment.

Necessity of protecting personal information in the telematics environment: In the telematics environment, there are no cases related to leakage and damage of personal information but this can be happened in a variety of ways. Personal information in the telematics environment can cause a lot of damages such as leakage or seizing personal information generated by the combination of characteristics of wireless network and GPS satellite communication, leakage of personal information due to network attack.

The personal information generated in the telematics environment is different from the static personal information created in the existing network. That is, it can cause damage different from the existing personal information, since, dynamic personal information such as the route and place of the driver and the passenger is generated as well.

Insurance companies like automobile insurance companies have launched insurance products with utilizing of driving habits, mileage application as well as discounted products with black boxes and used through commercialization about things that are not recognized as personal information. Insurance products with utilizing of driving habits make use of the driver's driving habits, the driving time and place and so on and information that can be considered as personal information such as accident location or vehicle number is opened or used when reading images related to accidents using black box. This information is uncontrolled and can not even be cryptographically processed, resulting in causing other damages. Concentration on driving information related to the vehicle driving with telematics service can be an obstacle to populate the telematics due to the issue of

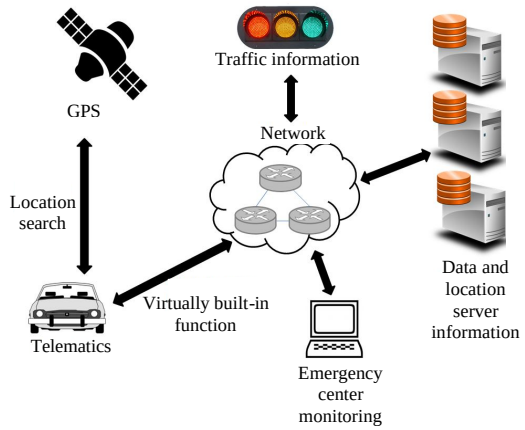

Fig. 1: Telematics system structure diagram

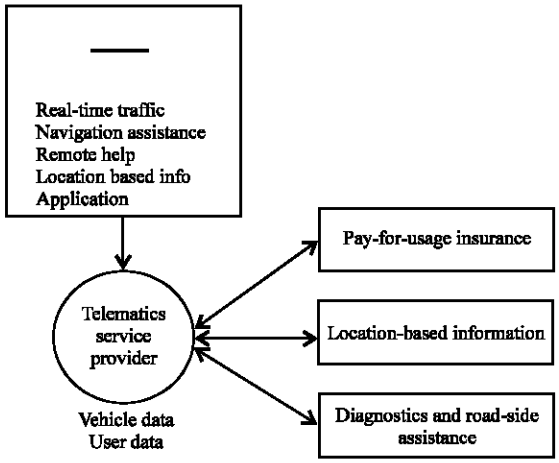

Fig. 2: Information related to telematics occurrence

privacy infringement and leakage of personal information even though there are positive aspects of convenience in the telematics environment.

Figure 1 shows simple schematization of telematics system structure. GPS communication, internet communication and communication between various sensors in the telematics environment generally transmit and receive information through the telematics and smart devices. This information is integrated into its own server storage using the information. Figure 2 shows the information related to the generated and used in the telematics system (Duri *et al*., 2002).

RESULTS AND DISCUSSION

Technical measures to protect personal information

Technical measures to protect personal information in telematics environment: In the telematics environment, a variety of issues due to leakage of personal information

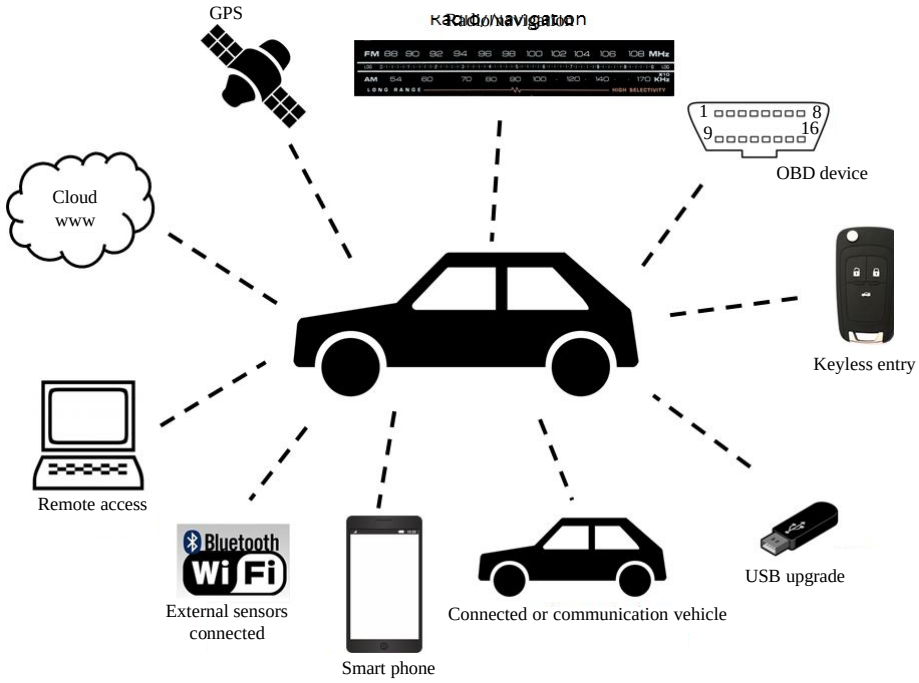

Fig. 3: Telematics attack threatening elements

can be occurred. User consent regarding personal information is required and there should be consent and access control in terms of personal information collection and control. As for personal information utilization, technical measures for risk prevention should be introduced. In addition, monitoring and correction are required as well.

As to vehicle, the various devices and environments surrounding the vehicle can be a path to infringe upon personal information in the telematics. Figure 3 shows the telematics attack threatening elements.

The attack threatening elements include internet, Cloud, OBD device, GPS satellite, transmission and reception between other vehicles, remote control key, external sensors, USB and upgrade through it, radio and navigation, Bluetooth and WiFi access through mobile devices. This lets personal information of vehicles and passengers to be collected (Prabu *e t al*., 2011; Foster *et al*., 2015; Daniel, 2014).

Collection: In the telematics environment, personal information is created in real time. Personal information such as location information is created through movement of the vehicle and GPS communication. Spying on movement of specific person or private life can cause problems through collection of such information.

In addition, it can be a path for collecting personal information through the wireless network communication of the wireless terminal device equipped in the vehicle. In particular, the location information through the GPS device can be collected without the consent of the customer and the collected information is highly probability of infringing on privacy.

Besides, theft and loss of devices in the vehicle can also be used to collect personal information. For instance if the vehicle with black box is stolen, the route and place of the vehicle can be easily collected together with the image information. The transmission and reception of data may be detected and collected when moving towards destination in the navigation.

Unauthorized access: Accessing, browsing or using personal information by an unauthorized person such as a hacker or a cracker can also be a large blind spot in protecting personal information in the telematics environment. This unauthorized access can lead to problems such as manipulating or leaking personal information.

Errors: The damage may occur due to some reasons such as mechanical defects or errors in the terminal device, leakage of personal information or wrong transmission due to errors in the network or GPS communication.

When upgrading related devices or sensors, malfunctions and errors may be occurred due to the influence of malicious codes or unexpected situation that the generated information is forcibly transmitted to another location (Koscher *et al*., 2010).

Illegal use: Personal information in the telematics environment that has been collected, unauthorizedly accessed or leaked on account of errors may be used for commercial or illegal purposes without the consent of the second or third anonymous person. In that case, this can lead to serious damage towards social issues beyond personal damage.

Personal information protection technology in the telematics environment: There are quite a number of protection technologies to protect personal information in the telematics environment. There are some protection technologies such as privacy policy creation, encryption for personal information and related stored data, filtering technology, anonymization technology and cookie control for vehicle wireless devices. Personal information is necessary to be classified and defined to apply these technologies and personal information protection policy should be needed. In addition, it is essential to introduce framework for telematics through preparation of access control measures.

In the telematics environment when personal information is exposed or leaked due to satellite communication, theft, unauthorized access and errors, data encryption is the most important technology to protect personal information in the telematics environment.

It is necessary to protect the personal information data as original source protection in order to protect personal information in the telematics environment. The major reason for protecting data is that the users who access and use the telematics technology can obtain reliability and data protection based on reliability can extend the utilization of the telematics technology.

Figure 4 shows communication and utilization through personal information data and data protection between companies using it in the telematics environment. Personal information data that is created in vehicles with telematics technology can be protected and managed. This protected and managed personal information is communicated with devices, other communication devices and sensors associated with the vehicle. When communicating using personal information data, the data management framework transmits the personal information through encryption. The devices and sensors receiving this personal information decrypt and use it in accordance with need.

Furthermore, the personal information received from the vehicle through the data management framework should be decrypted or stored and managed as it is in companies and public organizations that use telematics technology and should be used limitedly by the relevant authority users as needed. In addition, personal

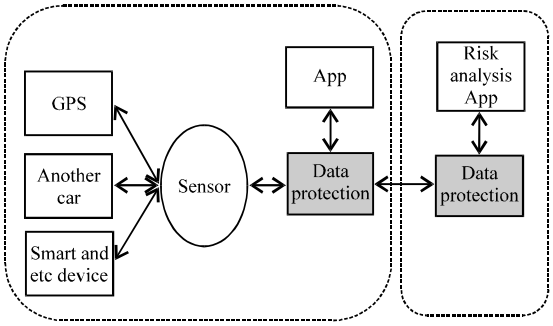

Fig. 4: Data Protection of telematics

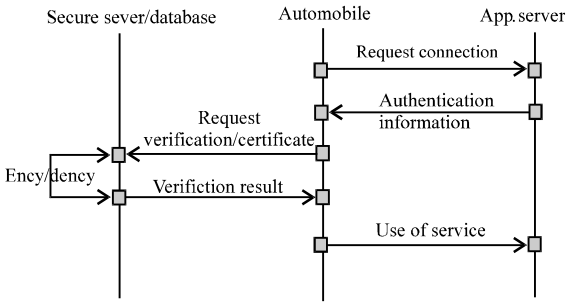

Fig. 5: Operation process flowchart of data management framework

information may be used in the vehicle with telematics technology. Companies and public organizations that provide related technology encrypt and transmit the requested personal information using the data management framework and also use the decrypted data in the vehicle.

The data management framework for protecting personal information in the telematics environment stores the data after encryption according to whether or not encryption is required for the generated data and transmits it to the requested device and sensor. After receiving the data again through this work and deciding whether or not the encryption is necessary again, the storage activity is performed.

In addition, the data management framework verifies whether the information requested by the device and the sensor is the information in the data management framework. If the external request for data is needed, the request is delivered to the company or the public institution. The company or the public institution transmits the requested data with encryption. Figure 5 shows the operation process flowchart of data management framework in the telematics environment.

CONCLUSION

The development of both IT technology and IoT technology would accelerate the application of telematics technology. Trust to telematics technology should be supported to generalize and develop the application as well as use of telematics technology.

In the telematics environment, drivers and passengers may be generating and providing personal information without being aware of it. The variously exposed threat elements may exist in the process of generating and providing personal information. In particular, in the telematics environment, personal information in real time is created and the type of personal information that is generated may change in accordance with the given type of time. The protection and management of personal information data should be performed, so as to eliminate the damage caused by leakage and exposure of personal information, including increasing the reliability of telematics technology. For this purpose, the data management framework is necessary to manage and protect data in vehicles with telematics technology. Data would be encrypted, decrypted and managed by data management framework.

ACKNOWLEDGEMENT

This study was supported by the research program funded by the Han-Sung University.

REFERENCES

Daniel, B., 2014. Identifying telematics threats. IQT. Quartery Summer, 6: 17-21.

Duri, S., M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.M. Tang, 2002. Framework for security and privacy in automotive telematics. Proceedings of the 2nd International Workshop on Mobile Commerce, September 28, 2002, Atlanta, GA, USA, pp: 25-32.

Eichler, S., J. Billion, R. Maier, H.J. Vogel and R. Kroh *et al*., 2005. On providing security for an open telematics platform. Proceedings of the 5th International Conference on ITS Telecommunications, June 27-29, 2005, Technical University of Munich, Munich, Germany, pp: 1-4.

Foster, I.D., A. Prudhomme, K. Koscher and S. Savage, 2015. Fast and vulnerable: A story of telematic failures. Proceedings of the 9th USENIX Workshop on Offensive Technologies, August 20, 2015, Woot Carrollton, Texas, USA., pp: 1-9.

Francois, T., I. Toshiya and P. Christopher, 2009. Automotive Telematics: Driving Toward the Wireless World. Booz Allen Hamilton, McLean, Virginia, USA.,.

Kaminski, T., M. Kruszewski, M. Niezgoda and J. Gacparska-Stolek, 2011. Telematic security system for cash transport vehicle. J. KONES., 18: 149-154.

Koscher, K., A. Czeskis, F. Roesner, S. Patel and T. Kohno *et al*., 2010. Experimental security analysis of a modern automobile. Proceedings of the 2010 IEEE International Symposium on Security and Privacy (SP), May 16-19, 2010, IEEE, Berkeley, California, USA., ISBN:978-1-4244-6895-9, pp: 447-462.

Nobuhiro, K. and M. Manabu, 2014. Telematics-compatible information security technology. Tech. Rep., 145: 16-18.

Prabu, A.V., B. Kodavati, T.A. Rao, E. Rambabu and S.S. Tripathy, 2011. Telematics based security system. Intl. J. Wireless Mobile Networks, 3: 138-147.