A Lightweight Private Internet of Things Remote System and its Micromixing Application

Hai Fu, Tianhang Yang, Weiliang Jia, Songjing Li*
Department of Fluid Control and Automation, Harbin Institute of Technology Harbin, 150001, China
*Corresponding author’s e-mail: lisongjing@hit.edu.cn

Abstract. Most current Internet of Things systems face many problems like privacy leakage, information island and low application value, because they are designed from the perspective of Internet of Things service providers. However, the practicality and privacy security of Internet of Things services are more important from the perspective of Internet of Things system users. Considering that there aren’t too many Internet of Things devices to use and manage for ordinary people and service, a more service-oriented architecture of the lightweight private IOT remote system is proposed in this paper. To verify this system, verifications like remote sensors, remote actuators, and a micromixing application are developed and illustrated. Owing to its distributed server architecture, this system has high flexibility, practicability, parallelism, and low coupling. This novel system architecture provides a new perspective to develop practical valuable private Internet of Things services.

1. Introduction
Most of the IOT(Internet of Things) systems are designed in top-down approaches from the perspective of IOT service providers and pay more attention to the scale of the IOT systems, network connection, data storage, data visualization, computation, analysis[1, 2]. The typical feature of those systems is with large scale IOT cloud platforms based on expensive cloud servers, they belong to centralized server architecture[3]. These IOT cloud platforms are used to conduct the identity authentications, IOT devices managements, data process and storage, etc.. However, if we switch to the perspective of IOT system users, the large scale expensive IOT cloud platforms don’t seem necessary for many private IOT services. Because there aren’t too many IOT devices to use and to manage for ordinary people or IOT services, these IOT service providers must create many individual accounts for every personal IOT user to manage IOT devices at present so that the personal IOT services looks like a safe private IOT system. But there are many potential risks like user privacy leakage, monitoring, and abuse in these IOT systems[4-7]. There is a serious asymmetry between IOT service providers and users on the control of IOT services information. That risk cannot be thoroughly eliminated by only relying on the IOT service providers’ commitments to the rational use and protection of users’ data. On the other hand, large IOT platforms are more likely to attracting attacks from hackers because of the huge capacity, valuable information, and privacy of IOT devices. And the publicity of the IOT service Website addresses and applications are easier to deeply analysed. Another issue of these IOT systems is information island. Usually, these IOT services can’t be shared between different IOT service users and providers because of business competition, system safety and privacy laws that leads to many huge information islands. The main work of this paper is aimed at attempting to solve above problems using a lightweight private IOT remote system from the perspective of IOT system users.
2. Architecture of the lightweight private Internet of Things remote system

From the perspective of IOT system users, a more service-oriented architecture of the lightweight private IOT system and its embedded intelligent sensing and control Web unit are proposed as shown in Fig. 1. This architecture is a distributed server architecture and developed in a bottom-up method. Before the practical basic functions of the IOT are designed and implemented, the practical needs should be analysed carefully. There are three layers in this architecture, namely, hardware perception and control layer, transport layer and application layer. The hardware perception and control layer is the foundation of IOT service. The implementations of hardware perception and control layer are typical Mechatronic systems, and their basic unit is embedded intelligent sensing and control Web unit. The hardware perception and control layer include sensor data parsing algorithms, digital signal processing algorithms, control algorithms and communication interface and so on. Like the concept of Edge Computing, most of the IOT service operations like identity authentication, IOT devices management and data storage, Mechatronic functions etc. are done in this layer which is the terminal edge of the lightweight private IOT system. Application layer is corresponded to specific IOT services.

Fig. 1 Architecture of the lightweight private IOT remote system and embedded intelligent sensing and control Web unit

To avoid the weak password security vulnerability, we proposed rules of password strength evaluation considering characteristics of embedded systems are as below. Rules of password strength evaluation are (1) the length of the password must be more than 8; (2) at least one element appears from lowercase letters (i.e. {a to z}); (3) at least one element appears from capital letters (i.e. {A to Z}); (4) at least one element appears from numbers (i.e. {0 to 9}); (5) at least one element appears from special characters satisfying certain restrictions (e.g. {! @ # $ % & * ( ) _ + = - }). However, a safety authentication password, not only the rules of password strength evaluation but also the easy memorization should be satisfied at the same time[8]. We proposed the sectional password generation method based on rules of password strength evaluation. The details of the method are (1) determine password length; (2) determine number and length of line segment based on principles of password strength evaluation; (3) determine the direction of line segment; (4) Password generation and memory. The generation of an easy to remember strong password is shown in Fig. 2. This method can be used to generate many easy to remember strong passwords. Usually in the development of Web servers, the names of Web pages are meaningful and certain naming rules. As shown in Fig. 2, in this lightweight private IOT remote system, a map between the names of functional Web pages and index Web page to strings generated by strong password rules is adopted to avoid illegal accesses by URL-guessing attacks. Based on this mapping, a simple method of information sharing is proposed by us. That’s the URLs of information sharing Web pages are shared with others directly. The people who got the URLs hardly guest the details of the embedded intelligent sensing and control Web server and its URLs of functional Web pages.
3. Verifications of this lightweight private Internet of Things remote system

3.1. Verification of lightweight private sensor Internet of Things remote systems

According to the output signal types, sensors can be divided into analog and digital sensors. The lightweight private IOT system proposed by us can be applied in the development of remote sensor. To verify this concept, private remote temperature sensor remote systems with analog and digital sensor are shown in Fig. 3 and Fig. 4. Mobile data network was used by the smart phone. And a wireless router with an education network IP address was used by the embedded Web servers. According to the experimental data curves, functions of lightweight private sensor Internet of Things remote systems are verified successfully.
3.2. Verification of lightweight private actuator Internet of Things remote systems

The lightweight private IOT system proposed by us can be applied in the development of remote actuators. To verify this concept, a private relay IOT system for remote control of an AC LED is shown in Fig. 5 and a private air conditioner IOT system for remote control of an air conditioner is shown in Fig. 6. Mobile data network was used by the smart phone. A wireless router with an education network IP address was used by the embedded Web servers. According to the experimental results shown in Fig. 5 and Fig. 6, functions of lightweight private actuator Internet of Things remote systems are verified successfully.

Fig. 4 Verification of the lightweight private digital humidity sensor IOT remote system

Fig. 5 Verification of the lightweight private relay IOT remote control system
4. A lightweight private Internet of Things micromixing remote system

Microfluidic is one of the important frontier research fields. Acoustofluidics is an important branch of microfluidics. Acoustofluidics has many valuable applications, such as acoustic tweezers, cancer cells separation, micromixing and so on. Sharp-edge micromixing device has been widely studied in recent years owing to its excellent mixing performance[9, 10]. For the operation of some toxic substances, sterile environment, and long-time multi batch experiments, remote operation of experimental system is very necessary. A lightweight private IOT micromixing remote system is developed as shown in Fig. 7. Mobile data network was used by the smart phone. A wireless router with an education network IP address was used by the embedded Web server.

A piezoelectric ceramics transducer with 4kHz working frequency is used to excite acoustic streaming around sharp-edge microstructures. The total flow rate is 1μL/min. The bright region of experimental pictures is fluorescent water, and its flow rate is 0.5μL/min. When the embedded portable
acoustic generator Web server does not receive control commands from the client subsystem (browsers), there is an obvious interface around sharp-edge microstructures because of laminar flow and weak diffusion in the micro channel of the sharp-edge micromixing device. When the embedded acoustic streaming generator Web server receives control commands from the client subsystem, it will generate a PWM wave with 4kHz and apply on the piezoelectric ceramic transducer after power amplifying. The obvious interface will disappear soon under acoustic streaming effect. Through experimental results, we validate successfully the private micromixing IOT system and it is a successful combination of Acoustofluidic and IOT.

5. Conclusion
From the perspective of IOT system users, a lightweight private IOT remote system is proposed. It has a more service-oriented architecture. Verifications like remote sensors, remote actuators and a micromixing application are developed and illustrated. All the verifications and the micromixing application successfully prove that this architecture has high practicality and privacy security. Finally, we believe this novel architecture will derive many practical valuable private IOT services in the future.

References
[1] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamtac. (2012) Internet of things: Vision, applications and research challenges. Ad hoc netw., 10(7): 1497-1516.
[2] Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, C. S. Hong. (2019) Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Gener. Comp. Sy., 92(MAR): 265-275.
[3] M. M. Othman, A. M. Mousa. (2020) Internet of Things & Cloud Computing Internet of Things as a Service Approach. In: 2020 11th Int. Conf. Inf. Commun. Sys. (ICICS), pp. 318-323.
[4] Y. Huang, X. Guan, H. Chen, Y. Liang, S. Yuan, T. Ohtsuki. (2020) Risk Assessment of Private Information Inference for Motion Sensor Embedded IOT Devices. IEEE T. Top. Com., 4, pp.265-275.
[5] O. P. Attanasio, N. Pavoni. (2011) Risk sharing in private information models with asset accumulation: Explaining the excess smoothness of consumption. Econometrica, 79(4): 1027-1068.
[6] A. Khan, B. Ravikumar. (2001) Growth and risk-sharing with private information. J. Monetary Econ., 47:3: 499-521.
[7] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama, J. Shah. (2019) IOT Security Risk Management Model for Healthcare Industry. Malays. J. Comput. Sci., 131-144.
[8] R. Morris, K. Thompson. (1979) Password security: A case history. Commun. ACM, 22(11): 594-597.
[9] H. Bachman, H. Fu, P. Huang, Z. Tian, J. E. Seckler, J. Rufo, Z. Xie, J. H. Hartman, S. Zhao, S. Yang, J. N. Meyer, T. J. Huang. (2019) Open source acoustofluidics. Lab Chip, 19(14): 2404-2414.
[10] H. Bachman, P. Huang, S. Zhao, S. Yang, P. Zhang H. Fu, T. J. Huang. (2018) Acoustofluidic devices controlled by cell phones. Lab Chip, 18(3): 433-441.