Security Context Framework for Distributed Healthcare IoT Platform

Orathai Sangpetch(✉) and Akkarit Sangpetch

Faculty of Engineering, Department of Computer Engineering,
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
{orathai.sa,akkarit.sa}@kmitl.ac.th

Abstract. As Internet of Things (IoT) is entering mainstream, data privacy and security in information exchange becomes a major concern and a barrier for potential adopters, especially in healthcare regime. Information from health IoT devices and services is sensitive and confidential. While many existing works have proposed enhancements and security prospects for individual devices and components in IoT ecosystems, they still do not address the underlying challenge which is the lack of sufficient security within systems. Effective security has to be built-in, not patched upon. To efficaciously tackle the challenge in distributed IoT systems, we present a security context framework which applies adaptive security contexts to properly track data of interest. The proposed solution can achieve accountability and track information propagation, involving devices, services and parties who have responsibility and potential legal liability. This could help leverage not just technical but also policy and legal aspects to enable health IoT adoption.

Keywords: Security context · Security framework · Internet of things · Cloud computing · eHealth

1 Introduction

Health and wellness is a key factor to the foundation of human capital, building strong economy. According to the UN report on the World Population Ageing [1], older population has been increasing rapidly, especially in more developed countries. There will be approximately 1,000 million older people in 2020 and double in 2050. The issue becomes one of the world's big challenges. Integrating technology, such as Internet of Things (IoT), into our lives can alleviate this challenge.

As shown in Fig. 1 for an example, a user can utilize existing wearable devices to monitor health and vital signs, such as blood pressure, heart rate, ventilation, and ECG. The monitored data will be transferred and stored at a cloud-based platform where healthcare providers or professionals can analyze and provide recommendations for users subscribing to the service. As a result, the user can spend their life independently while still receives personalized and on-demand healthcare service.

This IoT and cloud-based system mostly deals with sensitive and personal information. Cybersecurity becomes a crucial factor to effectively utilize technologies without compromising privacy. Many current IoT [8] and cloud-based solutions are not

M.U. Ahmed et al. (Eds.): HealthyIoT 2016, LNICST 187, pp. 71–76, 2016.
DOI: 10.1007/978-3-319-51234-1_11

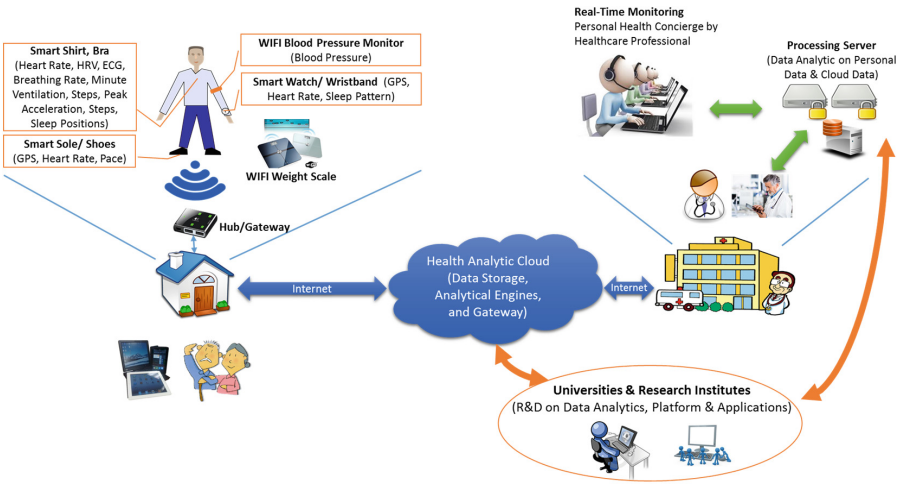

Fig. 1. An example of how to utilize internet of thing and cloud computing to provide remote and personalized healthcare service.

initially designed with security in mind. With existing threats and potential values of data, effective security cannot be just a surrounding fence like traditional security perimeter [9]; but it has to be designed within since the beginning.

In this paper, we propose a security context framework for healthcare information. The proposed framework serves as a security guideline to design the system and as a validator to evaluate security in existing systems of interest. The proposed security context should be integrated within the entire data flow since the security strength is equal to the weakest link of the flow. As illustrated in Fig. 2, if the link between the device and the gateway is compromised, the data becomes compromised even if the security in the cloud is strong. Traditional and existing data security models [4, 5] often concern with access or the implementation of individual device or software component level. This is insufficient since, if anything happens, we should be able to track the line of operations to the level of whom is responsible or at stake. Healthcare information system thus requires stronger security context than other types of system.

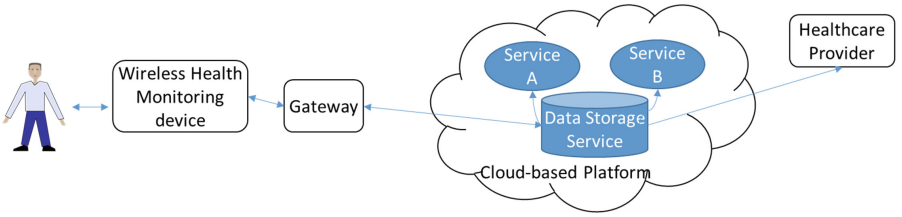

Fig. 2. A data flow example to show how personal health data gets transferred through the computing chain.

2 Security Objectives in Healthcare IoT

In order to reap the benefits of IoT technology with nominal security and privacy concern, a system that is built to manipulate healthcare information needs to satisfy at least the following security principles:

- **Authentication** is an act of verifying the truth of the credential or attributes provided.
- **Authorization** is a process to specify the access rights to resources. In this case, resources could be chunks of personal data.
- **Accountability** is an ability to trace what happens to resources of interest.
- **Confidentiality** is an act or rules to limit the access to resources of interest.
- **Integrity** is an assurance that resources of interest are accurate and trustworthy.
- **Availability** provides reliable access to resources of interest to authorized people.
- **Non-repudiation** is an implication of complete obligation to a particular contract or transaction.

3 Security Context Framework for Distributed Healthcare System

The main idea of our framework is the creation of security context associated with each resource which, in this case, is a piece of personal health information. When a piece of information is created, the associated security context should be generated automatically. The initial context is unchangeable after the creation, thereby yielding the non-repudiation property. However, at each information transfer, a device or a service can append additional context information in order to generate an audit trail, reflecting the data usage and path. We define a security context (SC) of a resource or a piece of information with an identifier X as follows.

Security Context: $SC_X = \{ACL\{\text{action}\}, Audit\{\text{action}\}\}$. The security context is essentially a pair of an access control list (*ACL*) and an audit list (*Audit*) of actions. An *ACL* specifies an action which can be acted upon the piece of information. An *Audit* list specifies the past actions that are performed on the information associated with the context, while an action is defined as follows.

Action: action = <*actor, operation*>, where an *actor* is a pair of <*PrincipalID, StakeholderID*>. *PrincipalID* is used to identified a security principal, which can be a user, an entity, a device, or a software component. This security principal is the one who initiates the operation on the information. *StakeHolderID* represents a legal entity who is responsible for the principal, such as healthcare providers, researchers, or end users. In other words, a stakeholder is the one who owns or is responsible for the piece of information. An *operation* suggests what process is performed on the information.

In practice, when information is propagated from the source through different devices and services, not only the information but also the associated security context will be coupled together and transferred. This couple is called a *propagation context*, which is formally described as follows.

Propagation Context: $D_X = \{SC_x, information\}$ where SC_x is the security context with identifier X and this security context belongs to the enclosed information.

With our approach, information transfer or exchange among different components will be in a form of propagation context. To facilitate information propagation and exchange at scale, both *ACL* and *Audit* lists should be immutable and can only be appended when the information is processed.

For example, when a piece of information is created, the initial security context will be created. This first security context is then composed of the ACL and audit trail of the first action, where the actor is a pair of the information owner and the device generating the information with the *creation* operation. Concisely, *PrincipalID* will be the device ID and *StakeholderID* will be the user ID. As the information travels through the system, each principal is authenticated and checked against the security context's *ACL* to authorize whether the principal has a sufficient right to access the information. In addition, the information regarding the devices or entities processing the information during the transit should be appended to the security context's *Audit* list for traceability purpose.

4 Practicality of Deploying Security Context for IoT Applications and Discussion

In this section, we apply the security context concept proposed in Sect. 3 to verify the desirable security principles in Sect. 2. Assume that we have a healthcare system presented in Fig. 3, where user Y uses device D to monitor his health whose data will be transferred to the cloud through the gateway. Then, user Y views his data through service B. At the data creation phase, the actor will be <D, Y> and the security context's audit list will be {<<D, Y>, *Creation*>}. When the data arrives at the gateway which only transfers the data through the cloud, the security context's audit list would become {<<D, Y>, *Creation*>, <<G, Y>, *Transfer*>}. When the data reaches the cloud storage service, the security context's audit list will be {<<D, Y>, *Creation*}, <<G, Y>, *Transfer*>, <<S, C>, *Store*>}. When the user views his information through service B, the security context's audit list will be {<<D, Y>, *Creation*>, <<G, Y>, *Transfer*>, <<S, C>, *Store*>, <<B, H>, *View*>}.

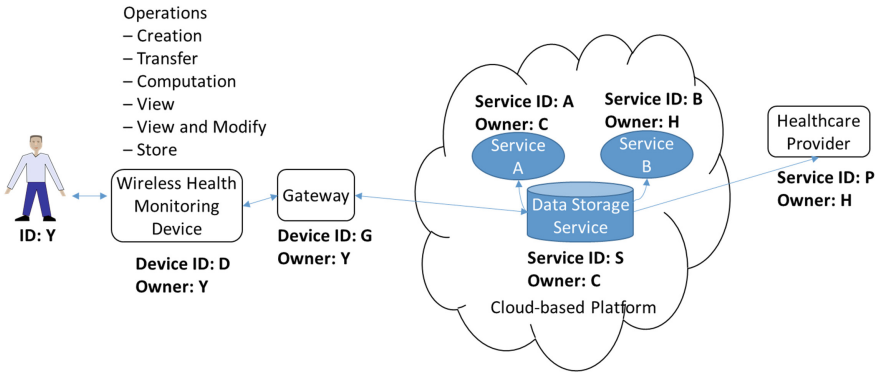

Fig. 3. An example of a security context application.

Once we construct the security context's audit list, we can consider it along with the selected technology deployed in the system in order to evaluate the security level of the given security. For example, we can use blockchain technology [7] as distributed online ledger in order to satisfy the accountability principle and the non-repudiation property as well as scalability. Currently, many financial institutions have considered to use the technology to keep track of online payment transactions.

The proposed security context can be difficult to apply to many current health monitoring devices since they are not equipped with an identification unit which can provide authorization to desired users. However, this is not an urgent concern yet. As long as the device is not sharable, we can associate a device with a user. However, it will be more secure if device providers incorporate an identification unit within the device. This can help alleviate an unauthorized use in the case of stolen devices or misusing devices to give false health data.

5 Related Works

Security and privacy issues have become a growing concern in the field of healthcare information systems and IoT. FTC report findings [2] suggest that IoT may lead to unauthorized usage of personal information by tapping into information exchange on insecure channels or through third party cloud service providers. In addition, a vulnerable device may be a potential source for staging attacks to other devices. Previous work suggests that distributed IoT approach presents unique challenges for access control due to the lack of certificate infrastructures and the need to balance the technical constraints on the range of medical devices [3]. Researchers have suggested an adaptive risk-based framework to be used to evaluate security model implementation and validate data from different IoT devices [4].

Our work has presented an extended security model for healthcare IoT. One could view IoT security framework as an extension of existing eHealth security model for exchanging EHR using cloud-based applications [5]. We propose a unified security context for medical IoT devices as well as a framework for storage and exchange of health information in the cloud. The devices also present an additional attack surface for IoT system as introduced in [6]. The security framework presented in previous works have largely focused on securing individual layers, devices, platforms, or applications independently. Our work argues that we should focus on a holistic view of security, centered on securing the pieces of information and how we should adaptively secure and track the information usage, while the information is propagating through various components and devices.

6 Conclusion

In this work, we propose an adaptive security context framework for exchanging health information in IoT ecosystem. We believe that in order to increase IoT adoption, we need to fundamentally address the challenge in data privacy and security concerning information exchange. This means we should be able to properly track and secure the

pieces of information generated from healthcare IoT devices, components and services, in addition to satisfy general security principles. To achieve this, we present an information-centric approach based on usage of the proposed security context framework. The proposed framework can help ease the privacy and security concern and increase adoption in healthcare IoT system. The framework also methodically assists how to design and implement or select appropriate technologies to ensure the desired level of security in the balance of usability, device limitations, resource constraints and supporting infrastructures.

References

1. United Nations: Department of Economic and Social Affairs, Population Division: World Population Ageing 2013. United Nations Publication, New York (2013)
2. FTC Staff Report: Internet of Things: Privacy and Security in a Connected World Federal Trade Commission, Washington, DC (2015)
3. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
4. Abie, H., Balasingham, I.: Risk-based adaptive security for smart IoT in eHealth. In: Proceedings of the 7th International Conference on Body Area Networks, pp. 269–275. Oslo, Norway (2012)
5. Zhang, R., Liu, L.: Security models and requirements for healthcare application clouds. In: IEEE 3rd International Conference on Cloud Computing, pp. 268–275, Miami (2010)
6. Lake, D., Milito, R., Morrow, M., Vargheese, R.: Internet of things: architectural framework for eHealth security. J. ICT Stand. **1**(3), 301–328 (2014)
7. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, 2009 (2012). http://www.bitcoin.org/bitcoin.pdf
8. ForeScout Technologies, Inc.: Survey Identifies Internet of Things (IoT) Security Challenges for the Connected Enterprise. Marketwired, 14 June 2016
9. Forrester: No more chewy centers: The zero trust model of information security. In: The security architecture and operations playbook for 2016