

# TOWARDS AUTONOMOUS PAYMENTS FOR INTERNET OF THINGS

Kok-Seng Wong and Myung Ho Kim  
School of Software, Soongsil University  
{kswong, kmh}@ssu.ac.kr

## Abstract

The maturation of Internet of Things (IoT) combined with proliferation of smart devices has disrupted the payment industry. Most enterprises across various industries have recognized a need for the convergence of online payments, mobile payments and point of sale payments in retail locations. The revolution of payment systems creates opportunities and new way in how consumer making a payment in the future. For example, an autonomous payment system could allow consumers to pay for gas, food or parking without leaving their connected car or automates the process of in-store payments. However, security is a big obstacle in this payment revolution. From the consumer's perspective, all autonomous payment systems should be secure and transparent. Some of the concerns are related to issues such as which device is making a payment, who are the parties involved, and how to authorize the payment. Hence, user authentication is one of the core requirements to answer those concerns. In this paper, we will explore the user authentication challenge for autonomous payment in IoT environment and propose an enhanced user authentication solution that utilizes user biometrics as an authentication factor.

**Keywords:** Internet of Things (IoT), IoT Payments, Autonomous Payment Systems, Biometrics-based authentication

## 1. INTRODUCTION

The proliferation of smart devices such as mobile devices and wearables has created a new way we communicate with people, work, and carry out daily tasks. Mobile computing devices are now a key-computing platform for individuals and business professionals. For example, many consumers have started to use smartphones for mobile banking (e.g., to check their account balance and transfer funds), mobile payments (e.g., as a digital wallet) and mobile commerce (e.g., buying products using mobile applications).

Despite the ubiquity of mobile devices, wearable technology has also started to make inroads into our daily lives. Wearable devices, such as smart watches, smart bands and other devices, can be worn on users' bodies, and these wearables are usually equipped with multiple sensors to provide sensory and scanning features, including biofeedback and tracking of physiological functions (Brule, 2013). Smartphone vendors such as Apple, Samsung and LG are working on further developing wearable devices (or wearables). Apple Watch allows users to turn their wearable into a payment device by adding their credit or debit card information to a secure chip. The development of smart devices give opportunities across industries, particularly in the payments industry (Winston, 2014).

### 1.1 The Revolution of Payment Systems

The maturation of Internet of Things (IoT) combined with proliferation of smart devices has disrupted the payment industry. Before this, many consumers rely on credit cards as the best alternative to cash due to the convenience and ease of making payments. Over the last few years, credit card payments have undergone tremendous changes. Instead of using cash or credit cards in brick and

mortar stores or online channels, consumers are now using mobile devices to conduct payments. Mobile payment services have recently received a significant amount of attention and are gaining popularity among consumers due to the convenience, usability and security when compared to conventional payment methods. The market associated with the IoT has been growth tremendously over the past few years. As estimated by Gartner (Gartner, 2013), the incremental revenue generated by the IoT can reach \$309 billion per year by 2020. A Bloomberg report also projected that there will be a huge increase in the mobile-transaction market, with payments projected to reach \$90 billion in 2017 (Soper, 2014).

The revolution of payment systems is driven by technology, and experts foresee a welcoming acceptance by consumers toward the use of digital wallets. A local newspaper in South Korea recently reported that the number of Samsung Pay users crossed 500,000 in just one month (Cavoukian, 2009). The ability to pay using mobile devices provides greater convenience to consumer and also producing new source of revenue for many companies. For instance, corporations such as MasterCard, Visa, and American make major gains through increased non-cash transactions and greater access to customer data.

In a study conducted by Google-BCG(BCG, 2016), they identified four major shifts in the global payments landscape:

1. The ongoing digital and technology revolution, led by the ever-increasing penetration of smartphones and internet on mobile, has revolutionized digital payments.
2. The payments space has witnessed the entry of several non-banking institutions offering payment services and solutions.
3. Customers are becoming more demanding and expect instantaneous and one-touch payment solutions.

4. There have been several progressive changes in the regulatory framework.

The revolution of payment systems creates opportunities and new way in how consumer making a payment in the future. An autonomous payment system could allow consumers to pay for gas, food or parking without leaving their connected car. Furthermore, it can be used to automate the process of in-store payments where the customer can shop and buy from a physical store without going through the payment counter. The total amounts of the walked out items will be charged automatically once the customer leaves the store.

In this paper, we discuss about the user authentication for smart devices and related work (Section 2), the IoT payment challenges (Section 3) and propose a solution to incorporate biometrics-based authentication into existing payment system (Section 4).



## 2. BACKGROUND AND RELATED WORK


### 2.1 User Authentication for Smart Devices

In a generic sense, security is the prevention of an unauthorized party from gaining access to confidential information and system resources. A secure authentication system needs to ensure only authorized users can access the system. When performing authentication over the Internet, credentials will be submitted by the principal (the user, machine, or service requesting access) (Convery, 2007). If the credentials match, the user is allowed to access the services subscribed to the service provider.

Security is a big obstacle in the revolution of payment systems. In particular, autonomous payment solutions should first authorize the users before they can use the system to make any payment. Subsequently, the system needs to verify the identity of the users (i.e., user authentication).

IoT smart devices are intended for frequent and fast access, so the common authentication methods consist of PINs, simple passwords or pattern locks. However, these authentication methods are neither convenient nor secure because they are hard to remember and leave the device vulnerable to malware and phishing attacks. Therefore, the following devices are used in conjunction with authentication schemes to authenticate users on smart devices:

-  Security token, a small hardware device that can provide authentication information (e.g., one-time passwords) for the user.
-  Smart cards, a device that includes an embedded integrated circuit chip (ICC) that enables it to store data (e.g., cryptographic keys) and carry out on-card functions.

-  Biometrics, the user's unique biological characteristics (e.g., iris and fingerprints) for identity verification.

The combination of two or more factors (e.g., smart card and biometrics (Wong, Kang, Lee, & Ho Kim, 2015)) forms a multi-factor authentication solution that can improve the security of these devices. For instance, a combination of password with biometrics has become one of the more popular authentication schemes for mobile payment systems (Wong & Kim, 2016).

### 2.2 Visa Ready Program

The Visa Ready Program is a commercial program designed by Visa to provide IoT device manufacturers with a path to embed secure payments into their connected devices. It also provides a framework for collaboration with Visa, guidance and access to Visa network (Wire, 2016). Some mobile point-of-sale acceptance providers are now looking for benefits they can gain by enabling the Visa Ready Program.

A brief summary of the Visa Ready Program is described as follows:

1. Consumer loads a Visa card to their connected device.
2. Device sends card load request to token requestor.
3. Token requestor requests payment credential from Visa Token Service.
4. Visa Risk Manager makes a decision based on approval rules established by Visa card issuer.
5. Token requestor provisions token to the device and activates for payments.
6. Visa Token Service generates and delivers secure token to the device.

### 2.3 Related Work

Continuous (or periodic) authentication is now commonplace for user authentication on mobile devices (e.g., ePet (Waller, Johnson, & Davis, 1999), SilentSense (Drath & Horsch, 2014) and TapPrints (Hermann, Pentek, & Otto, 2016)). The main idea of continuous authentication is to silently and transparently authenticate users based on user touch behavior biometrics. For instance, implicit authentication (IA) schemes authenticate users on smartphones by profiling their behavior using touchscreens and accelerometers (Poarch, Grahn, Park, & Martin, 2015). Since the IA scheme can recognize differences in user behavior, it can prevent other users (i.e., non-owners or attackers) from using or accessing sensitive data stored on the device. For example, a previous study proposed a continuous authentication solution to observe user's activities on a mobile file system and network access (ENISA, 2015), and another study investigated whether a classifier can continuously authenticate users by means of touchscreen features on a smartphone (Papp, Ma, & Buttyan, 2015).

Although continuous authentication schemes can improve the user experience and device usability, they are

also susceptible to security issues. For instance, continuous authentication is only useful to provide frequent access to non-sensitive applications but is not suitable for sensitive applications, such as banking and payment systems. Continuous authentication is often bound to a latency that leaves the device unsecured for a certain period of time. For example, when a mobile device is unlocked, it will remain unlocked for a period of time until it is actively locked again (either by the user or the system if no active interaction is detected). Hence, the attacker has a timeframe within which to steal the unlocked device and access private data stored on the device.

Biometrics authentication has become a common feature in mobile and wearable devices. Goode Intelligence forecasted that there will be 604 million users of wearable biometrics technology worldwide (Winston, 2014).

### 3. THE IOT PAYMENTS CHALLENGES

Most enterprises across various industries have recognized a need for the convergence of online payments, mobile payments and point of sale payments in retail locations. However, due to the proliferation of mobile devices, there is a need to secure user's private data and to prevent unauthorized access and data leakage in mobile payment systems. The growth of mobile payment could inhibit due to factors such as limited interoperability among systems, inadequate security, and a lack of standards in the existing payment systems.

In 2013, the Payment Card Industry Security Standards Council (PCI SSC) released their security guidance for mobile payment transactions (Bartezzaghi, Cagliano, Caniato, & Ronchi, 2016). The guidance addresses the following three main risks associated with mobile payment transactions:

1. **Account data entering the device:** how to prevent account data from being intercepted when entered into a mobile device.
2. **Account data residing in the device:** how to prevent account data from being compromised when processed or stored within the mobile device.
3. **Account data leaving the device:** how to prevent account data from being intercepted upon transmission out of the mobile device.

Due to the above risk issues, security is now a key concern for consumers when selecting mobile payment service providers including security in mobile applications that deliver payment transactions secure identification. From the consumer's perspective, all autonomous payment systems should be secure and transparent. Some of the concerns are related to issue such as which device is making a payment, who are the parties involved, and how to authorize the payment. Other concerns may include liability issue such as payments error, failure, and disputes between shared owners. From a merchant perspective, it needs to understand what payment channels the owner has and how

to deal with a consumer with multiple devices and different payment options (i.e., bank accounts and credit cards).

## 4. PROPOSED SOLUTION

Smart devices and biometrics can be combined for user authentication to provide increased security to users. Users' biometrics templates can be used for one-to-one verification and for strong authentication of the device owner's identity. In our solution, we separate the user's sensitive information into two devices. The biometrics matching operation will be performed inside a wearable device. This approach can prevent leakage of the biometrics template and can improve security for payment systems. In this section, we will explain the details of our idea to enhance the existing payment solution (e.g., Visa Ready Program) with the biometrics-based authentication scheme.

### 4.1 System Components

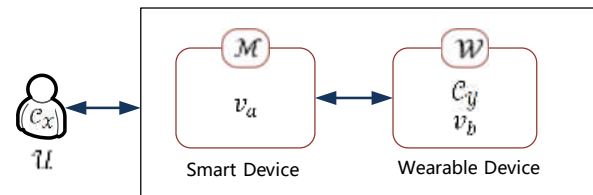


Figure 1. System Components in the Proposed Solution

The system components used in our solution are shown in Figure 1. The feature of each component is described as follows:

- [F1] Smart device  $\mathcal{M}$ ,** an electronic device (e.g., tablets, smartphones, mobile devices, and smart cars) used by the user to make the payment. This device is equipped with a biometrics scanner or sensor that can provide sensory and scanning features.
- [F2] Wearable device  $\mathcal{W}$ ,** an electronic device, such as a smart watch or fitness tracker that is capable of perform lightweight computations.
- [F3] User  $\mathcal{U}$ ,** an individual who owns both devices (i.e.,  $\mathcal{M}$  and  $\mathcal{W}$ ) and is concerned with security vulnerabilities in existing mobile payment solutions.
- [F4] Private data  $\mathcal{V}$ ,** information such as credit card information and bank account details. These information will be separated into partial private information,  $\mathcal{V}_a$  and highly sensitive information,  $\mathcal{V}_b$  such that  $\mathcal{V} = (\mathcal{V}_a \cup \mathcal{V}_b)$ . During the enrollment process,  $\mathcal{U}$  stores  $\mathcal{V}_a$  and  $\mathcal{V}_b$  in  $\mathcal{W}$  and  $\mathcal{M}$ , respectively.
- [F5] Biometrics template  $\mathcal{C}_y$ ,** biometrics features from  $\mathcal{U}$ 's physiological characteristics (e.g., fingerprint). This template will be stored in the wearable device and is used to verify if  $\mathcal{U}$  is a legitimate device owner.

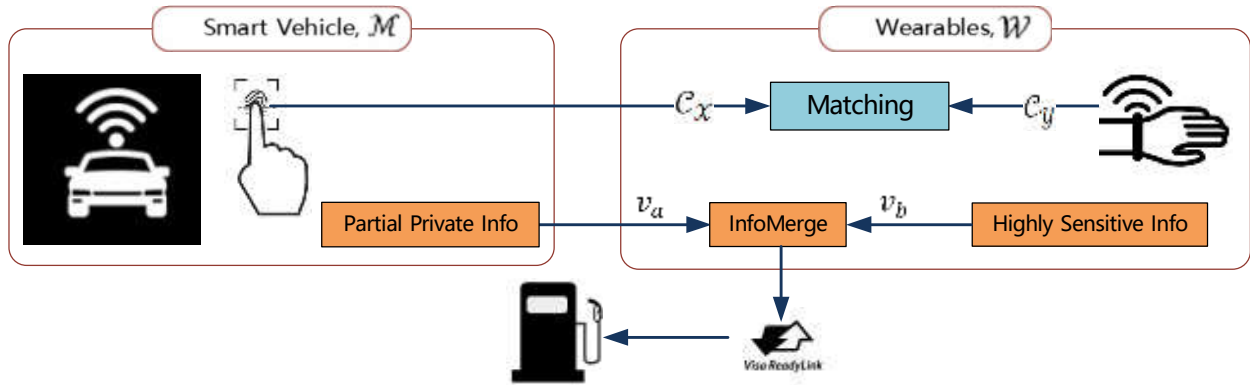


Figure 2. System Overview of Autonomous Payment by using Biometrics.

Biometrics query  $\mathcal{P}_{\text{query}}$ , biometrics features from  $\mathcal{P}_{\text{user}}$ 's physiological characteristics (e.g., fingerprint) during verification phase.

## 4.2 Secret Splitting

In existing mobile payment systems, the user's credit card information and bank account details are stored in a single device (e.g., a smartphone or security token). However, this approach poses some security vulnerabilities because an adversary can recover the full secret message when the device has been compromised. As a result of this issue, we propose to split and store the user's private data in two separate devices. For example, bank can split the credit card details  $\mathcal{P}_{\text{cc}}$  into  $\mathcal{P}_{\text{cc1}}$  (i.e., credit card numbers and credit card type) and  $\mathcal{P}_{\text{cc2}}$  (i.e., expiration date, pins and CVV number) such that  $\mathcal{P}_{\text{cc}} = (\mathcal{P}_{\text{cc1}} \cup \mathcal{P}_{\text{cc2}})$ .

## 4.3 System Overview

Let assume Alice wants to pay for gas at a petro station without leaving her connected car. In order to do so, she first scans her fingerprint by using the biometric scanner integrated in her car. Then the car will submit her biometric query  $\mathcal{P}_{\text{query}}$  to her connected wearable device (e.g., smart watch) for matching. If the matching is successful, the wearable device will automatically receive Alice's partial private info  $\mathcal{P}_{\text{cc1}}$  stored in the car. Next, the wearable device combines Alice's highly sensitive info  $\mathcal{P}_{\text{cc2}}$  with  $\mathcal{P}_{\text{cc1}}$  and submits the card load request to Visa Ready Program. The subsequence process will be the same as those described in Section 2.2. The system overview of our solution is shown in Figure 2.

In our solution, we assume that both  $\mathcal{M}$  and  $\mathcal{W}$  are tamper-proof devices. Hence, they can provide a strong guarantee that the information that is stored cannot be exported outside the device. In addition, the tamper-proof device can provide assurance that the data stored inside has

not been maliciously read or modified by an unauthorized party.

## 4.4 Discussions

Biometrics-based authentication systems provide a higher degree of security when compared to conventional authentication systems. Furthermore, they allow the system to keep track of the user's activities because individual biometrics characteristics cannot be shared with others. Although biometrics can provide many benefits when compared to conventional authentication methods, they also pose serious security and privacy concerns for the system's resources and the owner's biometrics features. This is of particular importance because biometric characteristics in humans are limited in number and cannot be reissued or changed. The risks associated with the use of smart devices and wearable devices are constantly growing due to their heavy use. In particular, user authentication is now an emerging problem that has attracted attention from researchers and vendors.

To protect the user's biometrics feature, we can transform the biometrics template by using some chaff features (Wong & Kim, 2012). It is also possible to split the biometrics feature by using secret splitting idea, such as in Shamir's secret sharing (Shamir, 1979).

## 5. CONCLUSION

Wearable devices are now becoming popular, so we propose their use to store partial private data of the user to participate in the authentication process. The combination of mobile and wearable devices provides a significant potential for applications where both security and privacy are important. From a security perspective, the key challenge is to prevent an adversary from impersonating a legitimate user during authentication. From a privacy perspective, we need to ensure that the user's private data and the biometrics template are not compromised. In this paper, our aim is to propose an idea to incorporate biometrics-based

authentication into existing payment system such as Visa Ready Program. Our solution can be used to enhance the security of the existing payment systems and to increase the confidence of consumers in using autonomous payment. Furthermore, our solution can be applied into other application domains such as Industrial IoT.

## 6. ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2014R1A1A2058695).

## 7. REFERENCES

Bartezzaghi, E., Cagliano, R., Caniato, F., & Ronchi, S. (2016). *A Journey through Manufacturing and Supply Chain Strategy Research*, Springer International Publishing, Switzerland.

BCG, G. (2016). Digital Payments 2020 The Making of a \$500 Billion Ecosystem in India. Retrieved October 2, 2016, from <https://www.bcg.com/en-in/d/press/25July2016-digital-payments-2020-making-500-billion-ecosystem-in-india-39417>.

Brule, M. R. (2013). Big data in exploration and production: Real-time adaptive analytics and data-flow architecture. *Proceedings of SPE Digital Energy Conference*, March 5-7, The Woodlands, Texas, USA, pp. 1-7.

Cavoukian, A. (2009). Privacy by Design-The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. Retrieved October 10, 2016, from [https://www.iab.org/wp-content/IAB-uploads/2011/03/fred\\_carter.pdf](https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf).

Convery, S. (2007). Network Authentication, Authorization, and Accounting Part One: Concepts, Elements, and Approaches. *The Internet Protocol Journal*, 10(1), pp. 2-11.

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or hype?[industry forum]. *IEEE industrial electronics magazine*, 8(2), pp. 56-58.

ENISA. (2015). Privacy and Data Protection by Design. Retrieved October 12, 2016, from <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

Gartner. (2013). Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets. Retrieved September, 7, 2016 from <http://www.gartner.com/newsroom/id/2621015>.

Hermann, M., Pentek, T., & Otto, B. (2016). Design Principles for Industrie 4.0 Scenarios. *Proceedings of 49<sup>th</sup> Hawaii International Conference on System Sciences (HICSS)*, Jan 5-8, Koloa, HI, pp. 3928-3937.

Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. *Proceedings of 13<sup>th</sup> Annual Conference on Privacy, Security and Trust (PST)*, Izmir, Turkey, July 21-23, pp. 145-152.

Poarch, D., Grahm, A., Park, D., & Martin, G. (2015). 10 Reasons Why Your Organization Needs Data Loss Prevention. *IT FOCUS AREA: SECURITY*. Retrieved September 17, 2016, from <http://focus.forsythe.com/articles/19/10-Reasons-Why-Your-Organization-Needs-Data-Loss-Prevention>

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11), pp. 612-613.

Soper, S. (2014). Apple Pay Leaps Ahead of Mobile-Payments Providers: Bloomberg Technology. Retrieved September 25, 2016, from <https://www.bloomberg.com/news/articles/2014-09-09/apple-s-payments-push-seen-as-challenge-to-paypal-square>.

Waller, M., Johnson, M. E., & Davis, T. (1999). Vendor-managed inventory in the retail supply chain. *Journal of business logistics*, 20(1), p. 183.

Winston, H. (2014). The Internet of Things will Revolutionize the Payment Industry. Retrieved September 7, 2016, from <http://www.yaleeconomicreview.org/archives/2204>.

Wire, B. (2016). Visa Brings Secure Payments to the Internet of Things Makers of Wearables and Cars Can Now Easily Embed Secure Visa Payments. Retrieved October 20, 2016 from <http://www.businesswire.com/news/home/20160220005021/en/Visa-Brings-Secure-Payments-Internet>.

Wong, K.-S., Kang, M., Lee, S., & Ho Kim, M. (2015). Practical Biometrics On-Card Matching for Remote User Authentication Using Smart Cards. In J. J. Park, I. Stojmenovic, H. Y. Jeong & G. Yi (Eds.), *Computer Science and its Applications*, Springer Berlin Heidelberg, 330, pp. 505-510.

Wong, K.-S., & Kim, M. H. (2012). A Privacy Preserving Biometric Authentication Protocol. *Advanced Science Letters*, 9, pp. 683-688.

Wong, K.-S., & Kim, M. H. (2016). An enhanced user authentication solution for mobile payment systems using wearables. *Security and Communication Networks*, 9(17), pp. 4639-4649.

## Authors



Kok-Seng Wong obtained his Ph.D. in Computer Science (major in information Security) from Soongsil University, South Korea in 2012. He is currently working as an Associate Professor in the School of Software at Soongsil University. His research interests include security and data privacy, secure computation, cryptographic protocols, cloud computing and IoT related topics.



Myung Ho Kim received his Ph.D. in Computer Science from POSTECH in 1995. He has been a professor in the School of Software at Soongsil University since September 1995. He is now the Chair of the School of Software. He specialises in business intelligence, internet security, and distributed computing.