An Access Control System for Intelligent Buildings

Nian Xue[†, ‡], Lulu Liang[§], Jie Zhang[†, ‡], Xin Huang[†]
[†]Department of Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University, China
Nian.Xue15@student.xjtlu.edu.cn, Xin.Huang@xjtlu.edu.cn
[‡]School of Electrical Engineering and Electronics and Computer Science,
University of Liverpool, UK
Jie.Zhang3@liverpool.ac.uk
[§]China Information Technology Security Evaluation Center
lianglulu@secemail.cn

ABSTRACT
Accompanied with accelerated development of the Internet of Things (IoT) and smart home industry, smart access control systems, e.g. smart locks, are getting popular in recent years. In this paper, we propose a smart access control system that allows users to enter buildings via mobile phones. Also, a protocol is designed to secure communications in the system. In addition, some investigation results regarding security and usability are found: (1) most people pay more attention to security in the access control system; (2) most people prefer using fingerprint as the primary unlocking mechanism.

Keywords
Access control; Security; Intelligent building.

1. INTRODUCTION
A lock worked as an access control mechanism is one of the greatest inventions of human being. The earliest known key-operated lock has such a long history of approximate 4,000 years old and dates back to ancient Egypt [12]. Traditional metal locks have been used for centuries [17]. However, with the continuous and rapid changing of modern life styles, more features are expected from the access control systems, especially in the intelligent buildings [5, 21, 22, 23, 24]. The smart lock [9, 10, 14] is emerging to improve life quality [15], while also reducing the security risks and costs effectively [16].

A significant body of research has been done in this field for the past few years. For example, in year 2009, Park et al. [1] proposed a smart digital door lock system for home automation. Padmapriya and KalaJames [8] put forward an improved face detection and recognition method for smart lock security system used on vehicles. Moreover, Chang and Jiang study binary single-key-lock system [6], and Wu researches matrix-based lock system [7] for smart locks.

In the era of mobile internet, smart devices including smart locks can be controlled through mobile devices conveniently [18, 20]. For instance, Bo et al. [3] present a smart power system for intelligent buildings, enabling smart phones to control smart sockets remotely. Iftode et al. [2] design a system architecture that allows users to interact with embedded systems using smart phones. In [4], Ping et al. introduce a remote monitoring intelligent system based on fingerprint through wireless transmitting and receiving. Paper [11] develops and implements a remote lock system utilizing wireless communication on a smart phone by a dedicated Android application. In 2007, Bauer et al. deployed a trial smartphone-based system in university building, aiming to replacing existing access control technologies [13].

In this paper, a smart phone based access control system for intelligent buildings is proposed:

1) An experimental system based on smart locks and mobile phones is designed and developed, which is named as "*Smart-Phone-Controlled-Lock*" (SPCL).
2) A lightweight security protocol is proposed and implemented. Security features of the protocol are discussed. Its performance is also evaluated in the experimental system.
3) Survey methods including questionnaire and focus group are used in order to study the attitude of candidates towards access control systems and several unlocking mechanisms, such as biometric identification, password pad and sliding card. It can be a starting point of future studies.

This rest of this paper is organized as follows. The SPCL is briefly introduced and its security mechanism is provided in Section 2. In section 3, a prototype of SPCL is implemented and performance of the proposed security protocol is measured. Section 4 describes the research methodology used in our survey. In section 5, we present the survey results and discussion. We compare our system with related work in section 6. Finally, some conclusions are made in section 7.

2. SPCL
In this section, SPCL, a smart lock- and smart phone-based access control prototype system is introduced. It is designed to provide a convenient and secure way to realize access control for intelligent buildings. The security mechanism in the system is also studied.

2.1 SPCL Architecture
SPCL is a demo system for controlling smart locks through mobile APPs. It is comprised of five main components: cloud server, mobile client, desktop/laptop client, switch and smart devices. The architecture of the project is shown in Figure 1.

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264493

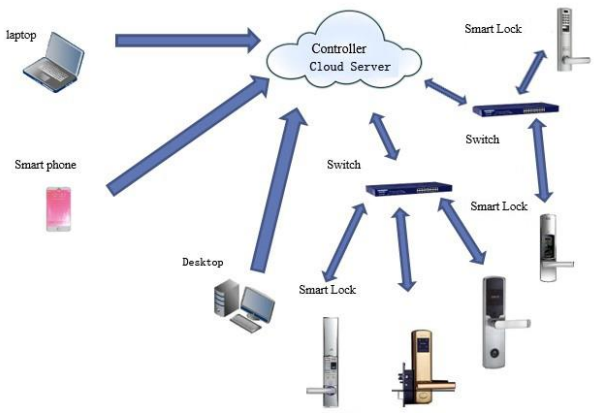


Figure 1. Composition and structure of SPCL

Cloud server is the central controller. It communicates with both client-side devices and smart devices. It can also store and process user's information, verify user's identity, and transfer control message from the mobile client to specified smart devices.

Mobile client usually is a smart phone or tablet PC. It can send user's instructions to the central controller (cloud server).

Desktop/laptop client is another auxiliary client-side device for controlling smart devices through the central controller.

Switch transfers messages. It works as a bridge between cloud server and smart devices.

Smart devices refer to devices such as locks, sockets and lights. It can connect to the cloud server or other devices via Blurtooth, WiFi, 3G/4G, Zigbee, etc., and execute instructions from the controller autonomously.

2.2 Security Mechanism

In order to provide secure communications between the smart lock and the cloud server, we propose the following security protocol.

Assume *k* is a key pre-shared by the server and the lock. The protocol can be roughly divided into four steps.

1. The Server sends an "*OPEN*" request to the lock.
2. After receiving the request from the server, the lock firstly generates a nonce *N*. Then the lock sends a nonce *N* to the server and calculates the MACl=HMAC (*k, N*);
3. Server calculates MACs=HMAC (*k, N*), and sends it back to the lock.
4. The lock checks whether MACs equals MACl. If the two values equal, then it executes the request. Besides, the lock should receive MACs in 5 seconds after step 2.

The detailed processing workflow is illustrated in Figure 2 below.

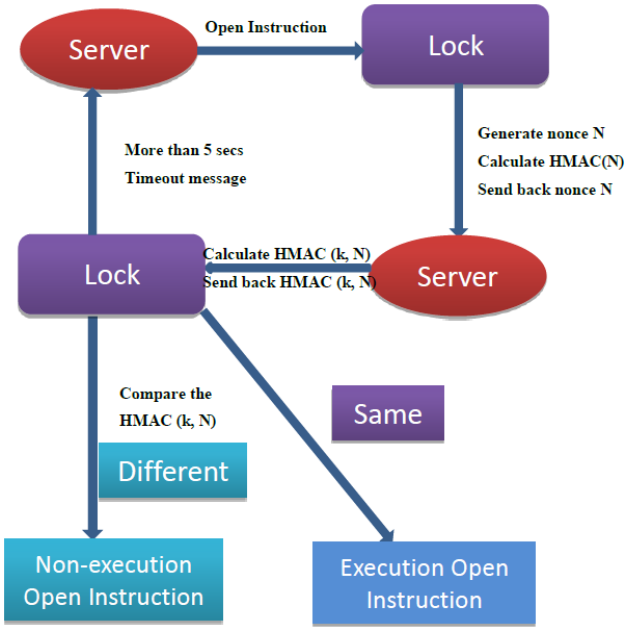


Figure 2. Instruction workflow diagram

2.3 Security Analysis

Impersonation attacks are the most serious security attack to access control system. If an attacker successfully impersonates the server without being detected by the client side (i.e. the smart lock in the demo system), then the client will execute any request of the attacker. More specifically, the lock may unlock according to the "*OPEN*" request from an attacker.

The proposed security mechanism can resist impersonation attacks due to the authentication between the server and the lock. The protocol also can resist other attacks such as replay attacks. The reasons are explained as follows:

Resist replay attacks: Attackers cannot reuse old values of MACs to pass the verification of the lock. This is because the computation of MACs takes a nonce *N* as input from the lock. Since the value of the nonce chances in each run of the protocol, the value of HMAC (*k, N*) also changes.

Authentication: Authentication between the server and the lock is guaranteed by the MACs. From the above analysis we can see that the MACs cannot be reused in different runs of the protocol. Additionally, it is difficult for the attackers to compute the value of MACs for the new generated nonce in the new run of the protocol. This is because in order to acquire the value of HMAC (*k, N*), the attacker has to know *k*. Since *k* is kept secretly by the server and the lock, the attackers have no better method than guessing the value.

3. IMPLEMENTATION AND PERFORMANCE

In this section, the performance of security protocol in our demo SPCL system is evaluated. During our experiment, we used Arduino Uno R3 as the controller of the smart lock. It could receive instructions from the cloud server. Table 1 summarized the features of our experimental system.

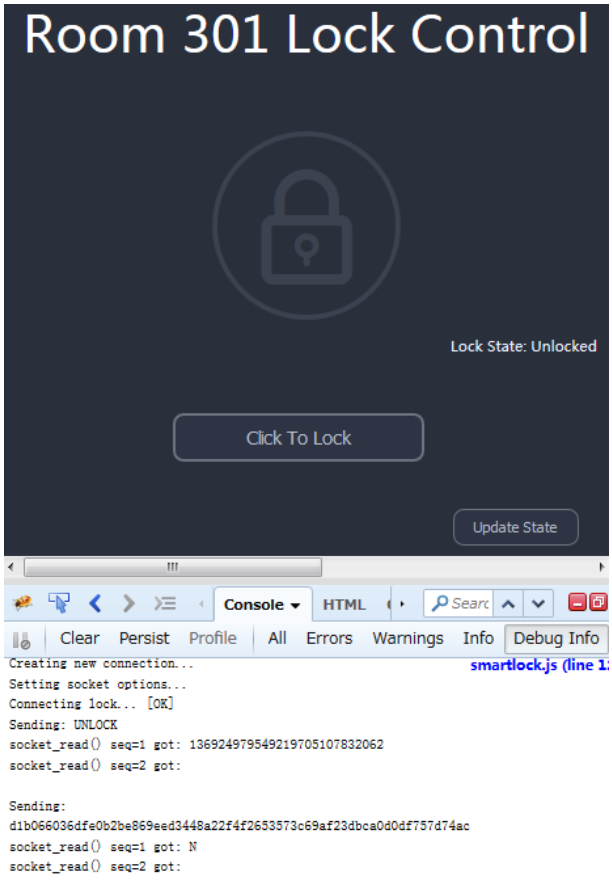
Table 1. Features of SPCL system

Public Cloud Server Remote Controller (Aliyun)	CPU	2.6 GHz (Intel Xeon E5-2650)
	Memory	8G
	Hard Disk	120G
	OS	Windows Server 2008 R2 (64 bit)
	Location	Hangzhou (Internet)
Private Cloud Server Local Controller	CPU	2.67 GHz (Intel i5 M560)
	Memory	4 G
	Hard Disk	500 G
	OS	Windows 7 Professional 32 bit
	Location	Suzhou (local network)
Smart Device (Arduino Uno R3)	Microcontroller	16 MHz, 8 bit (ATmega328)
	SRAM	2 KB
	EEPROM	1 KB
	Flash Memory	32 KB (bootloader 0.5 K)
Router	Feixun Router (FWR-706)	
Switch	TP-link Switch	

3.1 System Setup

We set up an online hotel reservation system using WAMP (Windows + Apache + MySQL + PHP). Guests can control corresponding locks by using mobile phones.

The HMAC algorithm in the security protocol is implemented using SHA-256. A successful running procedure of the protocol described in Section 2.2 is shown in Figure 3 below.



(a)

(b)

Figure 3. a) Implementation of security protocol on cloud server. b) Implementation of security protocol on smart locks

From Figure 3 a) we can find that the cloud server received a nonce *N* from the smart lock, and sent a calculated MACs back. Figure 3 b) shows that the smart lock reveived the MACs from the cloud server, and the value was equal to the MACl calculated by itself. Since the two calculated MAC values were matched, the door would be unlocked.

3.2 Performance Evaluation

In order to evaluate the system performance, a timer is set in the program to calculate the precise time consumption of each instruction cycle. The results of experiments are summarized in Table 2 and Figure 4，5，6 and 7. The results indicate that 68% of the local server TTL falls in the range of [0.5, 0.540375] and 86% of the remote cloud server TTL falls in the range of [0.596125, 0.620875].

Table 2. Experiment results on local and remote cloud server

Parameters	Local Cloud Server	Remote Cloud Server
Average time	0.5578s	0.6072s
Average ping time	<1ms	14.2ms
Number of rounds	50	50

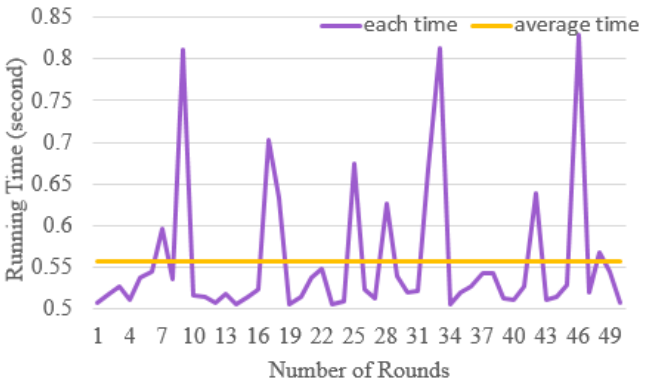


Figure 4. Running time of security protocol on local cloud server

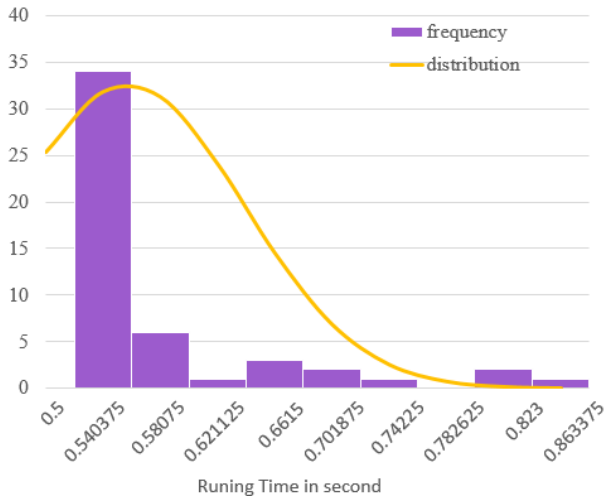


Figure 5. Distribution of running time on local cloud server

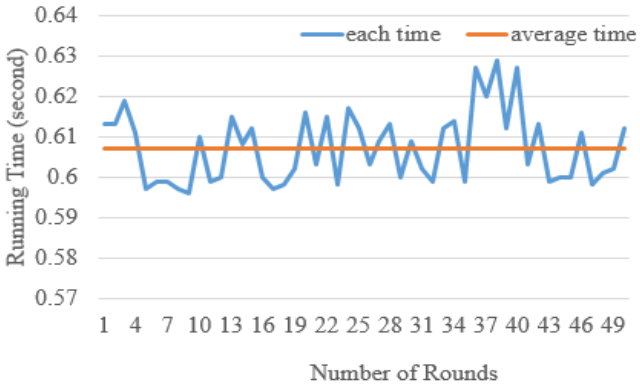


Figure 6. Running time of security protocol on remote cloud server

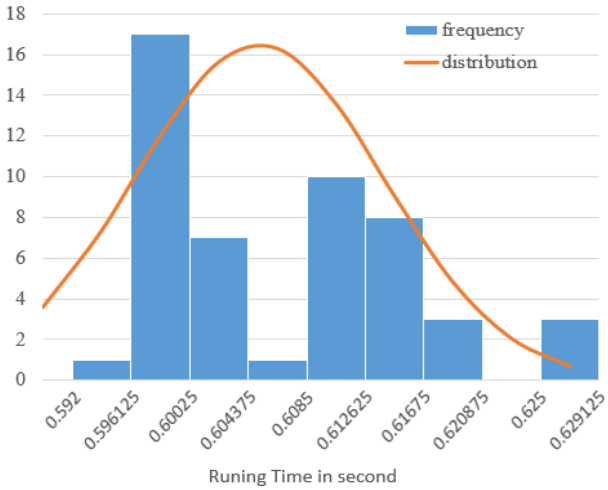


Figure 7. Distribution of running time on remote cloud server

4. SURVEY

The survey focuses on the following research questions:

RQ1: What are the important features of smart locks?

RQ2: Which unlocking method is preferred?

It is hypothesized that:

1) Security is the most important feature.

2) The fingerprint-based unlocking method is the most desirable unlocking method.

4.1 Quantitative Methodology

In order to examine the hypotheses, questionnaire was chosen as the main research approach. The questionnaire used in the survey is an online one with eighteen questions. The types of questions include demographic, multiple choice, dichotomous and Likert-scale questions. Because the subjects are mainly Chinese, in order to avoid the language barrier, the questionnaire was translated into Chinese. These voluntary participants answered the questions in approximately two minutes on average. In order to protect the privacy, all the respondents remained anonymous.

These samples consisted of 77 males (63%) and 45 (37%) females, having diverse backgrounds, such as education levels, occupation. The pie chart below (Figure 8) elucidates the occupation composition among the samples. Table 3 below shows if they know smart locks, and if they accept smart locks.

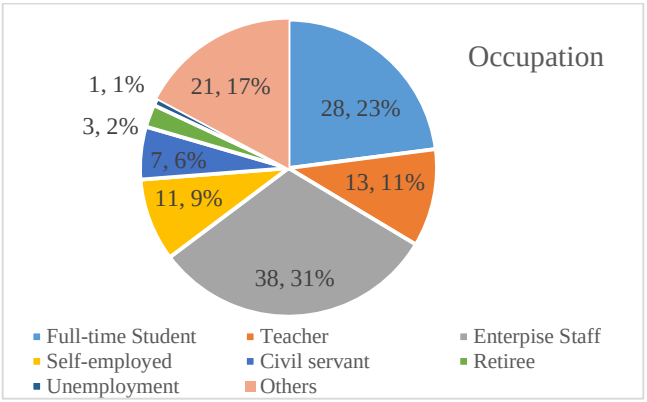


Figure 8. Composition of occupation

Table 3. Acceptance of Smart Locks from Different Age Groups

Group No.	Age Group	Percentage of Considering Using Smart Locks	Number of Respondents
G1	Under 18 years	1 (50%)	2
G2	18~25 years	15 (62.5%)	24
G3	26~30 years	17 (70.83%)	24
G4	31~40 years	30 (66.67%)	45

G5	41~50 years	19 (90.48%)	21
G6	51~60 years	3 (60%)	5
G7	Over 60 yeas	1 (100%)	1

4.2 Qualitative Methodology

We utilize focus group as an auxiliary research approach. Focus group is regarded as an effective qualitative research method, which enables researchers to determine cause and effect, to explore how individuals perceive their own experience.

8 people (one teacher, seven students) participated in the focus group for about 45 minutes. Descriptive characteristics of the eight individuals in the focus group are presented in Table 4. Author's role was leading the discussion and developing questions focusing on the three questions mentioned previously. The whole meeting conversation content was recorded using a smart phone.

Table 4. Focus Group Individual Background

Participant ID	Age	Gender	Occupation
I1	33	Male	Teacher
I2	34	Male	student
I3	27	Male	student
I4	22	Male	student
I5	22	Male	student
I6	28	Female	student
I7	22	Female	student
I8	22	Female	student

5. RESULTS AND DISCUSSION

5.1 Questionnaire

It is hypothesized that security is the most significant concern while choosing between traditional and smart locks. Figure 9 shows a histogram of the factors that will affect informants' choice when they buy locks. The result clearly indicates that security (86.89%) is the most important factor.

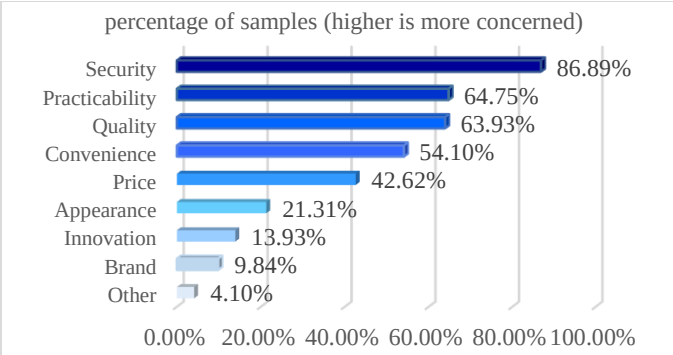


Figure 9. Factors affect people choosing smart locks

In the following grading questions, informants were asked to give marks (1 lowest, 5 highest) to both smart locks and traditional locks. The average mark of each aspect can be distinctly seen from Figure 10. As expected, smart locks acquire a better mark in the aspects of security.

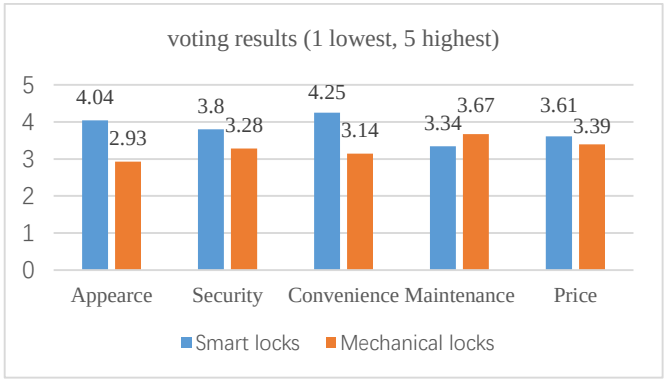


Figure 10. Comparison of smart locks and mechanical locks

Next, we let participants give a mark for a series of unlocking styles. Figure 11 provides the average marks for each method. Fingerprint is the only one whose value is over 4. Facial recognition obtains 3.8 which is the 2nd, followed by smart mobile devices.

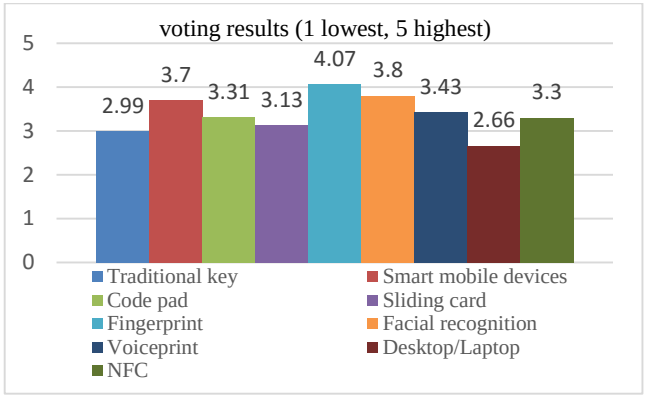


Figure 11. Comparison of various unlock styles

Finally, from the data in Figure 12, the biometric unlocking is the favorite method. Comparing another two means, people are more inclined to employ patterns to unlock door rather than using passwords.

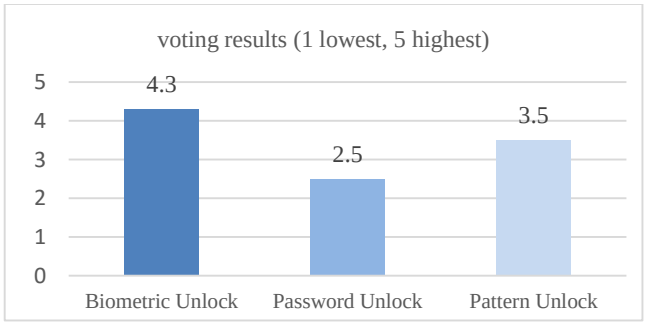


Figure 12. Comparison of different unlocking styles by using smart phone

5.2 Focus Group and Discussion

The participants' responses to smart locks were very positive and enthusiastic. A fierce debate on the two topics above was conducted. The advantages and disadvantages of security mechanisms used in smart locks are also analyzed.

The first purpose of this study is to find out whether security is important. All the participants agreed that security is the most important factor, and believed that the smart lock has a high level of security.

The second aim is to find the favorite unlock style. The results indicate that fingerprint is the best one. Also, the focus group member expressed their worries of losing fingerprints. Losing personal finger information might incur worse damages rather than losing key. Moreover, one member presented a problem that fingerprint can be stolen and duplicated easily.

The third goal is to investigate people's attitude towards "*smart-phone-controlled-lock*". Most of them were inclined to use their own smart phones to control the smart locks due to its convenience and expandability.

Additionally, participants of focus group elucidated some detailed examples of security mechanisms on smart locks. For instance, if the password of the smart lock was changed, the smart lock will send a message to the host as a reminder; some smart locks has a monitor and could take photos or record video. These functions that traditional locks do not have could improve security significantly.

6. RELATED WORK

In this section, the authors have compared and summarized a few differences among some similar smart phone-based systems mentioned previously.

Nowadays, smart phones are increasingly becoming popular and ubiquitous in our daily life [19], and almost everyone has one. With the widespread popularity of smart phones, the application based on smart phone has also gained a growing attention. The authors in this paper have built a prototype of SPCL, using smart phone and cloud server. SPCL can be applied to access control in intelligent buildings to enhance security and convenience.

In Bo et al.'s [3] system, the mobile phone is the central controller. However, this system cannot deal with massive requests in a short period due to the limited processing capability. In contrast, the central controller of SPCL is a cloud server that is more powerful.

In the architecture presented by Jeong et al. [11], the mobile phone connects the smart devices directly. However, security mechanisms rely on the security of Bluetooth.

Another phone-based access control system proposed by Huang et al. uses Raspberry Pi as the smart device, and the mobile phone communicates with the smart device through WiFi [10]. In contrast, SPCL uses Arduino Uno R3 which is a low-energy smart terminal device. Additionally, not only WiFi, but also Blurtooth, Zigbee, and Ethernet can be used in SPCL.

7. CONCLUSION

The presence of mobile technology together with cloud computing has dramatically changed the way modern people connect with the world. The proliferation of mobile devices has led to a bright new stage in which people's focus is also shifting from the desktop to the cloud. In this paper, the authors combine mobile device with cloud computing, providing a smart access control system for intelligent buildings. Consequently, the administrator can use the mobile phone to control smart locks remotely.

The authors suggest that the SPCL is a useful and practicable solution for intelligent building access control. Also, the authors designed and built a security mechanism implemented for SPCL. The performance of the security protocol was measured. Last, the authors discussed and summarized survey results.

Additional features and extensions can be applied to the proposed system, for example, NFC and fingerprint recognition integrated into smart phones, to improve the security and usability in the future.

8. ACKNOWLEDGMENTS

This work has been supported by the XJTLU research development fund projects RDF140243, as well as by the Suzhou Science and Technology Development Plan under grant SYG201516, and Jiangsu Province National Science Foundation under grant BK20150376.

This work has been supported in part by the Natural Science Foundation of China under Grant No. 61401517, in part by the National High Technology Research and Development Program ("863"Program) of China under Grant No. 2015AA016001.

9. REFERENCES

[1] Y. T. Park, P. Sthapit and J. Y. Pyun. Smart digital door lock for the home automation. In *TENCON 2009-2009 IEEE Region 10 Conference*, pp. 1-6, 2009.

[2] L. Iftode, C. Borcea, N. Ravi, P. Kang and P. Zhou. Smart phone: An embedded system for universal interactions. In *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*, pp. 88-94, 2004.

[3] W. Bo, M. Li, X. Peng, X. Li and X. Huang. A Smart Power System. In *the 3rd International Conference on Mechanical Engineering and Intelligent Systems*, Yinchuan, China, August 2015.

[4] P. Wu, G. Wu, W. Xie, J. Lu and P. Li. Remote Monitoring Intelligent System Based on Fingerprint Door Lock. In *2010 International Conference on Intelligent Computation Technology and Automation*, pp. 1012-1014, 2010.

[5] R. Xu et al. Software defined intelligent building. In *International Journal of Information Security and Privacy (IJISP)*, vol. 9(3), pp. 84-99, 2015.

[6] C. K. Chang and T. M. Jiang. A binary single-key-lock system for access control. In *Computers, IEEE Transactions on*, 38(10), pp. 1462-1466, 1989.

[7] T. Wu. A refined key-lock access control system. In *Aerospace and Electronics Conference, 1993. AECON 1993., Proceeding of the IEEE 1993 National*, pp. 583-587, 1993.

[8] S. Padmapriya and E. A. KalaJames. Real time smart car lock security system using face detection and recognition. In *Computer Communication and Informatics (ICCI), 2012 International Conference on*, pp. 1-6, 2012.

[9] W. Bo, Y. Zhang, X. Hong, H. Sun and X. Huang. Usable security mechanisms in smart building. In *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on, IEEE*, pp. 748–753, 2014.

[10] X. Huang, W. Bo, Y. Zhang and N. Gong. I-lock: A phone-based access control system. In *International Conference on Computing and Technology Innovation (CTI 2015)*, 2015.

[11] H. D. J. Jeong, W. Lee, J. Lim and W. S. Hyun. Utilizing a bluetooth remote lock system for a smartphone. In *Pervasive & Mobile Computing*, vol. 24, pp. 150-165, 2015.

[12] S. Ashley. Under lock and key, In *Mechanical engineering*, vol. 115, p. 62, 1993.

[13] L. Bauer, L. F. Cranor, M. K. Reiter and K. Vaniea. Lessons learned from the deployment of a smartphone-based access-control system. In *Symposium on Usable Privacy and Security, SOUPS 2007*, Pittsburgh, Pennsylvania, USA, pp. 64-75, July, 2007.

[14] H. Collinson. Help: working smarter lock, stock and password. In *Computers & Security*, vol. 14, pp. 39, 1995.

[15] A. Kaklauskas, E. K. Zavadskas, J. Naimavicienė, M. Krutinis, V. Plakys and D. Venskus. Model for a complex analysis of intelligent built environment. *Automation in construction*, vol. 19, pp. 326-340, 2010.

[16] C. Ulusoy. Android Library Design and Implementation for Smart Lock Access Control Systems. M.A. thesis, School of Elect. Eng., Aalto University, Finland, 2015.

[17] R. D. McCrie. A history of security, *The handbook of security*, pp. 21-44, 2006.

[18] X. Huang. Sensor application privacy and security. Mid Sweden University, 2010.

[19] R. Ballagas, J. Borchers, M. Rohs and J. G. Sheridan. The smart phone: a ubiquitous input device, *IEEE Pervasive Computing*, vol. 5, pp. 70-77, 2006.

[20] X. Huang, P. Craig, H. Lin and Z. Yan. SecIoT: a security framework for the Internet of Things. In *Security and Communication Networks*, 2015.

[21] N. Xue, X. Huang and J. Zhang. S^2Net: A Security Framework for Software Defined Intelligent Building Networks. In *The IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2016.

[22] J. Y. Son, J. H. Park, K. D. Moon and Y. H. Lee. Resource-aware smart home management system by constructing resource relation graph. *IEEE Transactions on Consumer Electronics*, vol. 57(3), pp. 1112-1119, 2011.

[23] L. Zhang, B. Liu, Q. Tang and L. Wu. The development and technological research of intelligent electrical building. In *China International Conference on Electricity Distribution, IEEE*, pp. 88-92, 2014.

[24] H. Shao and H. Fu. Design and implementation of intelligent building engineering information management system. In *Intelligent Computation Technology and Automation (ICICTA), 2014 7th International Conference on, IEEE*, pp. 158-161. 2014.