Send Orders for Reprints to reprints@benthamscience.ae

The Open Automation and Control Systems Journal, **2015,** *7,* **805-808**

Research on Information Security Interaction Mode of Mobile Devices Based on Ubiquitous Computing

Xianquan Zeng*

School of Information Engineering of Xuchang University 461000, China

Abstract: With the development of the communication technology and the network technology, the mobile network has gradually become the necessary application platform for people's work and life. So, the mobile device experiences a huge reform in communication mode and technologies. 3G and 4G technologies are closely associated with our life. Development of communication technologies brings more diversified exchange modes and more extensive information channels to us. However, the security problems caused by the technology reform are increasing dramatically. When the mobile devices conduct information interaction, how can the personal information be protected well? This problem is studied in this paper. This paper proposes the information security interaction design to enhance security when users interact with information *via* mobile devices based on the ubiquitous computing theory by combining the security mechanism of mobile devices.

Keywords: Information security, Interaction mode, Mobile device, Ubiquitous computing.

INTRODUCTION

This paper studies the information security interaction mode of mobile devices based on the ubiquitous computing, starting with the analysis of free connection and information transfer brought by ubiquitous computing to the mobile Internet devices. The ubiquitous computing becomes a new research field in the mobile Internet applications due to its continuous transfer and light computing feature. The ubiquitous computing is the network service system consisting of users, micro sensors, system services and information resource, and it integrates network, wireless communication, built-in computing system and sensing system to make users freely share information resources.

1. OVERVIEW OF UBIQUITOUS COMPUTING

1.1. Features of Ubiquitous Computing

The ubiquitous computing aims to realize natural interaction between mobile devices and human being and can be embedded in mobile devices in the surrounding or the wearing mobile devices. The ubiquitous computing can closely interlink persons, computers, sensors and Internet. The main features of the ubiquitous computing are described as follows:

First, the ubiquitous computing features information interaction. When persons are under the environment with plentiful computing devices, persons can be provided with different services accurately and quickly *via* information interaction. For example, when you accommodate at a hotel with ubiquitous computing devices, your personal habits, interests and hobbies can be transferred to the service persons at the hotel quickly, so the service persons can provide you with considerable services [1].

Secondly, the environment of the ubiquitous computing is transparent. The computing process of the ubiquitous computing is invisible, so the ubiquitous computing can be completed without disturbing the normal work and life of users [2].

Thirdly, the ubiquitous computing can dynamically change. The mobile devices will have certain mobile effectiveness in specific space, so when the device information is interacted, the structure of the ubiquitous computing system will not dynamically change [3].

Fourthly, the ubiquitous computing is self-adaptive. The ubiquitous computing features automated sensing, reasoning, and adaptation to user habits, work and life mode, so users can enjoy the service provided by the ubiquitous computing system even under unconscious state [4].

Fifthly, the ubiquitous computing can proactively repair errors. When the ubiquitous computing system fails, the computing module can automatically repair or upgrade according to the system error feedback [5].

1.2. Environment of Ubiquitous Computing

The ubiquitous computing can sense user behaviors and environment contexts by using sensors. The micro-processor can memorize and use the sensed and memorized information for user interaction and exchange *via* mobile devices. The remote servers store the user model database and

*Address correspondence to this author at the School of Information Engineering of Xuchang University 461000, China; Tel: 15836583827;
E-mail: xianquanzeng@hotmail.com

1874-4443/15

different resource information and can proactively provide dynamic help information according to the user's environment or demand. The wireless communication network is the important infrastructure for ubiquitous computing. Now the well-known Bluetooth and WI-FI is the main mode of network connection for mobile devices.

1.3. Association Between Ubiquitous Computing and Mobile Network

With the advent of big data age, the information resource sharing, proactive information acquisition and information interaction and exchange will be focused in the development of the mobile network. The mobile network can make the users acquire the required information at any time and place. For interaction between mobile devices and between persons and mobile devices under the ubiquitous computing environment, the perfect network information protection mode is required to protect interactive or sharing information and privacy. The Internet technology is fused with the mobile communication technology under the ubiquitous computing to form the interactive network environment, so the mobile network devices become diversified and humanistic under the ubiquitous computing environment.

2. INFORMATION SECURITY INTERACTION MODE UNDER UBIQUITOUS COMPUTING ENVIRONMENT

2.1. Interaction Mode of Information Security in Mobile Devices

The information security of the mobile devices under ubiquitous computing environment mainly includes unlocking password, voice recognition and biological recognition interaction mode. Now, generally the mobile device information is secured by using the unlock password, *e.g.* Sudoku pattern on the slipping screen of smart mobile phone and number password. For the Sudoku pattern, when a finger slips on the Sudoku pattern on the capacitance screen by certain numerical sequence, the device will match the slipping sequence with the set password. For the number password, the device will match the input number string with the set password to protect the mobile devices. The voice recognition technology can encrypt the mobile devices by recognizing the person's voice. The effect of such technology is not ideal due to the influence from external factors. The biological recognition can protect the system *via* differences of the user individuals, *e.g.* fingerprint recognition technology, face feature recognition technology and eyeball iris recognition technology.

2.2. Protection Mode of Information Security in Mobile Devices

The information security of mobile devices is more complicated than the traditional Internet information security. Recently, the personal information and asset theft based on the Internet frequently happened. Illegal persons induce users to use the mobile network *via* providing free WI-FI and phishing 2D code, so they can quickly get users' personal information and threaten information security. To ensure and strengthen security and protection of the information contained in the mobile devices, the technical security and protection measures should be provided for users at the software and hardware level and a sound security mechanism should be established. For the information security, the mobile devices can be protected *via* the software application security, network interface security and terminal device security. The software security indicates the security authentication of the application programs on the mobile devices. The network interface security indicates communication protocols, password algorithms and keys between the mobile devices and mobile network interfaces. The terminal device security indicates to provide sound security and protection measures for the devices and avoid virus intrusion. Generally, the protection modes include encrypted storage, software signature and system firewall.

2.3. Secure Interaction Mode of Mobile Devices Under Ubiquitous Computing Environment

The mobile devices provide the ubiquitous information service under the ubiquitous computing environment, and the information interaction is under the tangible and seamless state. Different devices can form the flow communication channels *via* different transport channels and protocols under the ubiquitous computing environment. The invisible computing scenarios can be established between users and environments. The information security will face huge challenges in this process. A perfect information security protection mechanism should be established for security interaction between mobile devices under the ubiquitous computing environment. First, the dynamic trust mode should be designed because the mobile network breaks through the traditional network boundary and transforms the traditional static trust relation to the dynamic trust relation, so an anonymous identity information mechanism should be established. Secondly, the access control privilege should be set. The user and information interaction modes are diversified under the ubiquitous computing environment. The entity mode and virtual modes are permitted. The ubiquitous computing network environment is a tangible space, so a proper access control strategy is required to prevent non-authorized resources or users from access to the network.

3. INTERACTION DESIGN INSTANCES OF MOBILE DEVICES BASED ON UBIQUITOUS COMPUTING

3.1. Design Conception

This paper designs an interactive system with the user behaviors as the mining object based on the interaction design idea of mobile devices under the ubiquitous computing environment. This system collects and analyzes the user work and living habits, behavior mode and interests and hobbies, establishes the user behavior diagram, provides purposeful user services according to the user habits, improves satisfaction of the user requirements, and secures information by combining the existing technologies in design of the interaction system.

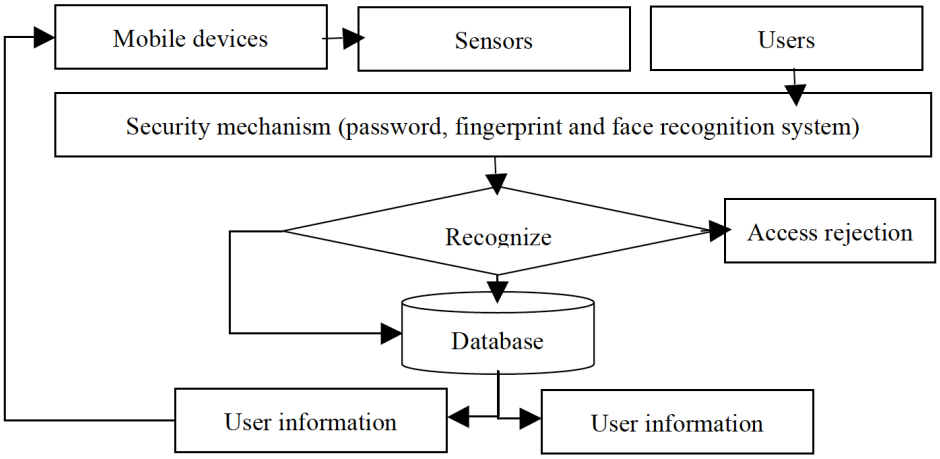

Fig. (1). Design flowchart of user behavior collection interaction system.

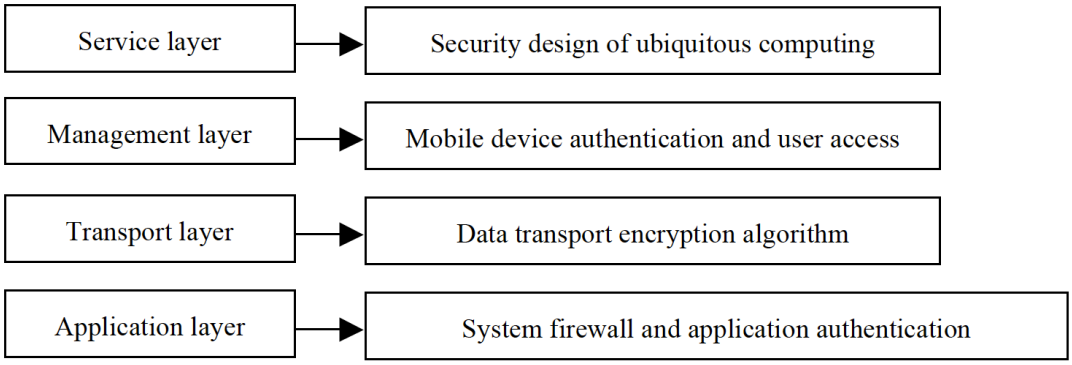

Fig. (2). Security architecture of ubiquitous computing.

3.2. Design Flow

The design flowchart of the user behavior collection and interaction system based on the ubiquitous computing is shown as the Fig. (**1**).

A user can log into the ubiquitous computing system *via* the environmental mobile devices and wearing mobile devices under the ubiquitous computing which can be authenticated *via* passwords, fingerprints and face recognition. The authenticated users can access the user database and user information is stored in the database. As the sensing device of user behaviors, sensors can collect the user behavior data and set the collection data object in an intangible manner in this process, *e.g.* user break time, time of visiting a brand store, consumption habit and emotion change trend.

3.3. Security Design

The security architecture of the ubiquitous computing is shown in Fig. (**2**): The user's identity information recognition and user's personal information database should be protected in the security design of the personal behavior information security interaction system of the mobile devices based on ubiquitous computing. The user identity information recognition is protected *via* the face recognition technology. When a user enters the ubiquitous computing environment, the sensors will track and detect the user's face, automatically adjust the user's face image area, generate the face image, or video stream, confirm the user's identity features *via* facial features, and compare the features with the user's face data in the database. When the user's identity is confirmed, the directional information will be collected. The user's personal information database is protected based on the server information security. The collected user information will be transferred to the server terminal *via* the mobile network. The transport protocols, network interfaces and servers will be encrypted. The mobile device terminal security involves service level, management level, application level and transport level. The service level security indicates the application system security operation environment for user business interaction. The management level security includes mobile device authentication and user access control. The application level security includes application security of mobile devices, *e.g.* mobile system and mobile APP certification. The transport level security indicates to encrypt the transported data by using encryption algorithms such as RSA, SM1, SM2 and SM3 when the user information is transported between the mobile devices and database for secure data interaction.

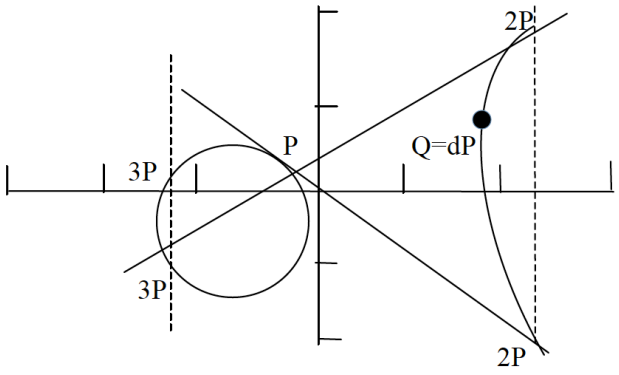

Fig. (3). Principle of SM2 algorithm.

The user behavior collection interaction system based on the ubiquitous computing designed in this paper encrypts data by using SM2 encryption algorithm. The SM2 algorithm is ellipse curve public key password algorithm and its equation is y2=x3+ax+b, where a and b are unique for specified standard curve. The principle of SM2 algorithm is shown in Fig. (**3**).

The SM2 algorithm uses the time d as the private key and Q as the public key. The tangent line passing the point P intersects with the curve at the point 2P. A line is drawn between the points P and 2P which intersects with the curve at the point 3P, so the point 2P is two times of the point P. The point 3P is three times of the point P. Similarly, four-time, five-time and six-time values of the point P can be calculated. The SM2 algorithm encrypts data by using 256-bit key and is extensively used as the commercial password algorithm.

CONCLUSION

The ubiquitous computing is a brand-new information service pattern used in the development of the mobile network and will change the traditional interaction mode between users and mobile devices. The ubiquitous computing highly integrates persons, devices and objects, constructs an intangible space *via* the sensor devices, wireless network equipment, mobile terminal equipment and servers, and lets users get different information more quickly and enjoy special service. Now, it is very difficult to tackle the information security of the mobile devices under the ubiquitous computing environment. This paper studies how to effectively secure the information on the mobile devices without influencing work and life of users. The information security interaction mode of the mobile devices based on the ubiquitous computing is protected by using existing technologies such as password technology, biological recognition technology and encryption algorithm in order to provide references for application and development of the mobile network under the ubiquitous computing environment in future.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Q. Peng. Ubiquitous computing. *Information Communication*, vol. 07, pp. 22-23, 2014.

[2] T. Lei, Z. Xingshe, Y. Zhiwen. Quick design and evaluation technology of ubiquitous computing applications. *Computer Science*, vol. 41, no. 8, pp. 30-37, 2014.

[3] Y. Qingjin. One position information interaction mode for mobile devices based on simple implementation mode of information security. *China Technology Information*, vol. 22, pp. 111-113, 2013.

[4] Y. Xiang, Z. Yuanyi, L. Qingzhou. Research and design of ubiquitous computing models based on mobile agents. *Computer engineering and design*, vol. 29, no. 21, pp. 5457-5460, 2018.

[5] L. Xufeng, Z. Shu. Information security protection system and method of mobile devices. *Information Security and Communication Security*, vol. 12, pp. 106-108, 2012.

Received: June 02, 2015 Revised: August 02, 2015 Accepted: September 05, 2015