International Journal of Engineering & Technology, 7 (3.24) (2018) 232-236

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Design of Access Control and Positioning System based on Beacon

Eun-Shin Kwak[1], Eon-Gon Kim[*2]

[1]*Graduate School of Information & Communications Engineering,Hanbat National University,125 Dongseodaero, Yuseong-gu, Daejeon, 34158, Republic of Korea*

[*2]*Department of Information & Communications Engineering,Hanbat National University,125 Dongseodaero, Yuseong-gu, Daejeon, 34158, Republic of Korea*

**Corresponding author E-mail: egk8996@hanbat.ac.kr*

Abstract

Background/Objectives: Smart devices combine GPS (Global Positioning System) and Wi-Fi signals to precisely identify the user's location outdoors. Also, it is possible to provide a navigation function for displaying on a service such as a map by using this technology. However, it is impossible to precisely locate the user because service provision for indoor location confirmation is difficult to receive GPS. Therefore, it is necessary to study and design the system more accurately by applying various technologies.

Methods/Statistical analysis: Many infrastructure technologies are being researched and utilized to improve indoor location and accuracy. Typical existing services include Wireless Local Area Network, Bluetooth, Ultra-wide Band, Ultrasonic sound, and Beacon. Based on these technologies, users are located inside the building and provided services based on their location. However, it is pointed out that a precise positional measurement is not performed, an error rate is large, and an error occurs in the result due to the influence of the surrounding environment. Therefore, in this paper, we design a system for indoor location and access control by applying low power Bluetooth based beacon. Beacon is used in the proposed system design because it has less battery consumption of smartphone than the existing Bluetooth version.

Findings: In this paper, we have carried out a study to improve the accuracy and reliability of the indoor positioning system service which is rapidly activated. To do this, we designed a system for locating users in indoor space using low power Bluetooth based beacon and heterogeneous sensor. Also, we propose a security policy that can efficiently control access to facilities based on indoor location. As a result, Beacon, ultrasonic sensors, Wi-Fi, and motion sensors were designed as integrated modules, and access control was performed by locating the users in each zone. In addition, a system design methodology for user access control, behavior restriction, and user behavior pattern analysis is proposed by combining user room location information and security policy.

Improvements/Applications: Finally, we designed a protocol and software for communication between beacon and mobile, and implemented a smooth communication module. In addition, we conducted a study on indoor location using Beacon for precise location. To do this, hybrid positioning algorithms using Beacon and various devices (ultrasonic sensor, Wi-Fi, motion sensor) were studied. And, the algorithm was designed for the situation - based indoor location positioning technology using heterogeneous or various sensors. Based on the results of the study, we propose a system policy that improves the accuracy of indoor location and enhances the security of access control.

Keywords: *Beacon, Access control system, Positioning system, RSS, Security control.*

1. Introduction

In recent years, outsider visitors often leak data by using a camera or data communication function built into smart phones or smart devices. In particular, there are increasing accidents in which security data such as customer information, electricity, electronic and mechanical drawings, and production facilities of financial institutions are leaked to the outside. For many years, industrial espionage spill accidents have increased rapidly, and interest in access control has also increased.

Currently, various agencies and companies such as public institutions, research institutes, and corporations apply various control services to prevent accidents in which insider information is leaked due to access by outside visitors.In case of security sticker, security sticker is attached to the smartphone camera or connection terminal to prevent photo shooting or connection with the insider system. Security stickers are attached at the same time as entering and exiting. When a trace is found by sticker inspection at the time of exit, security procedures such as inspecting the memory of the device are performed[1].However, there is a disadvantage in that it is difficult to confirm whether the breakage of the security sticker is intentional or not.

In the case of MDM, it is a management tool to control insider mobile devices and manages various mobile terminals as well as smart phones. The MDM system allows insiders to initialize their mobile devices, lock them remotely, and track what they did on the device. And, when there is no possibility of recovering the lost or stolen device, the enterprise can initialize the terminal to prevent the loss of information in the device. However, in the case of MDM, centralized control based push method is used, so it is difficult to distribute and service in a batch. Therefore, research and development are necessary to overcome technical limitations and it is necessary to secure professional technical manpower. In

the case of device security, the smartphone is left in a separate storage room for outside visitors[2,3].This approach can fundamentally prevent information leakage through smartphones. However, the waiting time for accessing can't be avoided long, there is a possibility of loss, and even a basic call can't be made, so that a considerable inconvenience is required.

In the case of the RFID access control system, the access card must be carried separately. If you lose a card because you must have a separate card, it may cause problems of personal information leakage and security of access. In addition, there are inconveniences of the initial card purchase cost and the erroneous ejection of the card to the new user, and the problem of the security system becoming ineffective due to the illegal copy of the card occurs. RFID technology transmits data using communication between reader and tag.Therefore, there is a possibility that a malicious attacker between the reader and the tag may intercept the data exchanged between the reader and the tag.If there is no ability to protect the information between the reader and the tag, the malicious attacker can obtain the information[4,5].Thus, encryption between reader and tag should allow malicious attacker to obtain information, which is meaningless information.In addition, the structure of the RFID tag has a response to the command when the reader transmits an instruction.In such a case, the reader can identify the tag based on the information transmitted from the tag. Through this, an attacker can obtain various personal information[6,7].

Recently, it is application control method which is widely applied to access control system.In the case of smartphone control via an application, users can control the functions of camera, Wi-Fi, data communication, tethering, and Bluetooth by installing apps on smartphones of outside visitors.It can be installed and deleted without the central control of the visiting company, and it is quite convenient compared to other methods because the visitor applies and releases the security policy of the company through QR code at the entrance.Figure 1 shows the scale of the access control security market.

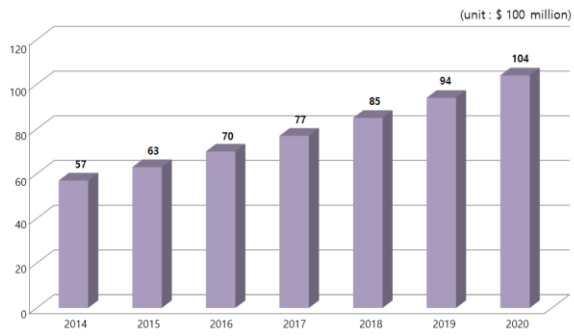

Figure 1:.Access control security market trend

Recently, Beacon has been widely used in the IoT market.Beacon is a transmitting and receiving device and equipment that has the characteristics to transmit the promised signal by shape, light, sound, color, radio wave, and to provide information such as position and direction.The current Beacon refers to the short-range wireless communication technology using Bluetooth.Find the location of a user in a certain range, and convey various information to the user.It is based on BLE (Bluetooth Low Energy) version 4.0 of Bluetooth and features low power consumption.BLE improves power consumption of existing Bluetooth, so it can be used for one year with one small battery.In addition, there is no limit to the number of simultaneous connections, so it is possible to connect multiple devices simultaneously in a limited space.The available distance is longer than NFC(Near Field Communication), which is a method of directly tagging a smartphone within 10cm [8].

The Beacon automatically detects and communicates when the user is within 50~70m(100m).In addition, it is possible to divide by 5~10cm units, so even if there are many users in a limited space, personalized information can be transmitted to each individual.It is suitable for utilizing the Internet of Things(IoT), which applies the Internet to all objects because of low power consumption and long range, and the O2O(Online To Offline) service, which connects online and offline[9,10].Beacons can use GPS technology to easily identify indoor location information without consuming a lot of smartphone battery.

Therefore, in this paper, we design Beacon based access control system.To do this, we design an integrated module that can improve the accuracy and reliability of user's location by using Beacon, acoustic sensor, Wi-Fi and motion sensor.In addition, we design a security-enhanced Beacon-based access control system by establishing insider / outsider rights management policies.

2. Access Control System and Positioning Security Service Status

2.1. Access Control System Status

In the case of domestic IT security business regulations, it is based on IT security related laws.The head of the administrative agency shall comply with the information and communication facility security law when he or she needs security measures for the designated protected area. According to the Act on Information and Communication Facilities, illegal shooting prevention measures using camera equipped mobile phones, etc. are taken, and it is stipulated that the unauthorized access and the carrying out of information assets should be controlled.Figure 2 shows the various access control system technologies.

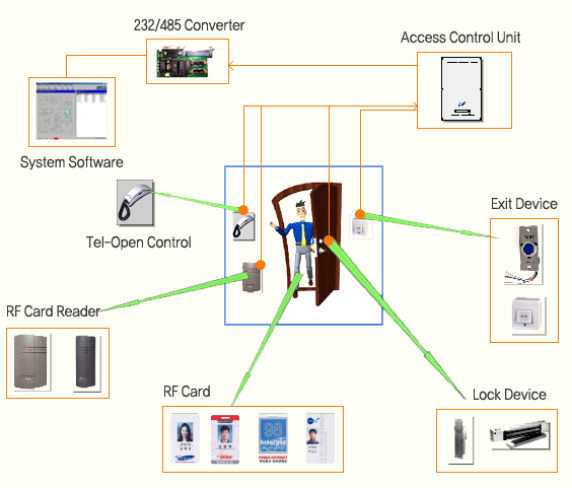

Figure 2:.Access control system technology

For this reason, CosoSys and theBoan are currently providing access control services using Beacon.In Europe, CosoSys is a provider of endpoint data security (DLP) and mobile device management solutions (MDM), which includes operating system-specific device control solutions and host-based data loss prevention (DLP) service.In case of Device Control, it supports all operating systems and provides various analysis tools for transmission log, trace, and audit log of shared files on the network through the latest peripherals.In the case of Mobile Device Management (MDM), it provides services such as security policy, remote program monitoring, remote deletion, locking, tracking lost device and location.

In the case of theBoan, insider security is strengthened by prohibiting the leakage of insider information by illegally using smart devices when visiting outsider visitors.To this end, we provide a Visitor Smart Device Management System (SDMS).The entrance and exit process of the SDMS enters the place of visit after the QR code is issued after confirming consent for the policy

adherence by the outside visitor.Check the user, group, and policy settings for the behavior when visiting, and record the entry and exit history management.After that, QR code is used to decide whether to comply with the policy and whether to exit according to the integrity verification.It controls smart devices and wireless communication devices of outsider visitors, manages the control of camera use, and provides services to block photographs and movie shooting[11].

In case of wireless, it manages Wi-Fi access control and permits access to authorized AP (Access Point).In addition, by managing Bluetooth usage control, it provides a service to prevent insider information leakage through 3G, LTE (4G), Wi-Fi Hotspot, and tethering blocking control through blocking and data communication control such as data communication through Bluetooth have.

Both of these services are BLE based services, but they have the following problems.First, the different levels of support between Android and iOS have not been resolved. In the case of iOS, since the OS itself supports ibeacon, it can receive signals and services even if the app does not work. On the other hand, in Android, the received signal strength indicator (RSSI) between beacons is unstable, This phenomenon appears to be extremely unstable in the background.Second, this use of RSSI values is limited because current BLE technology is not intended to be used to measure distance or position[12]. The Bluetooth Special Interest Group (BT-SIG), which manages and operates the bluetoothprotocol is currently developing a new protocol with consideration of distance and location, but it is expected to take several years.

As such, IPS has attracted a great deal of attention because of its ability to be able to locate indoor locations globally and its various applications and its application services. There are various applications that are used from shopping guide to access control. However, there is still a problem that technical problems such as accuracy of user location and personal information protection must be determined.

2.2. Positioning Security Service Status

BYOD (Bring your own device) caused by users' use of smart devices is causing a problem of leakage of insider information.As a result, the BYOD security issue is rapidly being discussed.In Korea, AMOLED technology outflow in May 2012 is the case.It is the case that the contents of development status and test results are leaked to the outside through smart phone messenger.In May 2012, there was a case where the illegal shooting of the company's private new car racing fair led to a sharp decline in sales of older models.An insider employee shot a spy shot using a camera on a smartphone and leaked it to the outside.In all of these cases, information is leaked due to smartphone shooting, which indicates that insiders and smartphones are the biggest threats to corporate information[13].

As an alternative, physical security technology and location-based interlocking services are provided as the first application services that should be preceded for prevention of outsider infringement and leakage of insider information.X-ray and metal detectors, security gates, access control and communication restrictions.It has the effect of minimizing information leakage and ensuring convenience through device control and monitoring work within the company.However, in terms of company characteristics and effectiveness, a service that coordinates unnecessary confusion is considered to be the most important key.

Card key systems using NFC and RFID provide a typical access control security service.Card type accounts for the highest percentage in the access control security service market.The access type number key system has been switched to a card key, which is evolving into a biometrics capable of dedicated encryption.This causes a variety of problems such as a serial number of a card key and a duplicate card, thereby serving as a supplement and an alternative[14].The security gate is a system that controls access to the building itself, not to the office or a specific space, because it is combined with a card key or biometrics technology.Fingerprint recognition, facial recognition, and smart phone recognition are combined with security gates, which is highly trusted in terms of security.It can be accessed and controlled through the administrator while being linked with alarm monitoring.

3. System Design

In this paper, we design Beacon based access control system.To do this, we design an integrated module that can improve the accuracy and reliability of user's location by using Beacon, acoustic sensor, Wi-Fi and motion sensor.In addition, we design a security-enhanced Beacon-based access control system by establishing insider / outsider rights management policies.

Figure 3 illustrates the access control situation to the inside / outside. The overall system configuration designed in this paper is designed to grasp user identity and accurate indoor location information by using mobile device, Beacon, Wi-Fi, motion sensor and ultrasonic sensor.In addition, IPS security service that proposes user access control and mobile device behavior and operation to indoor space restricted access by providing information to security policy server was designed.

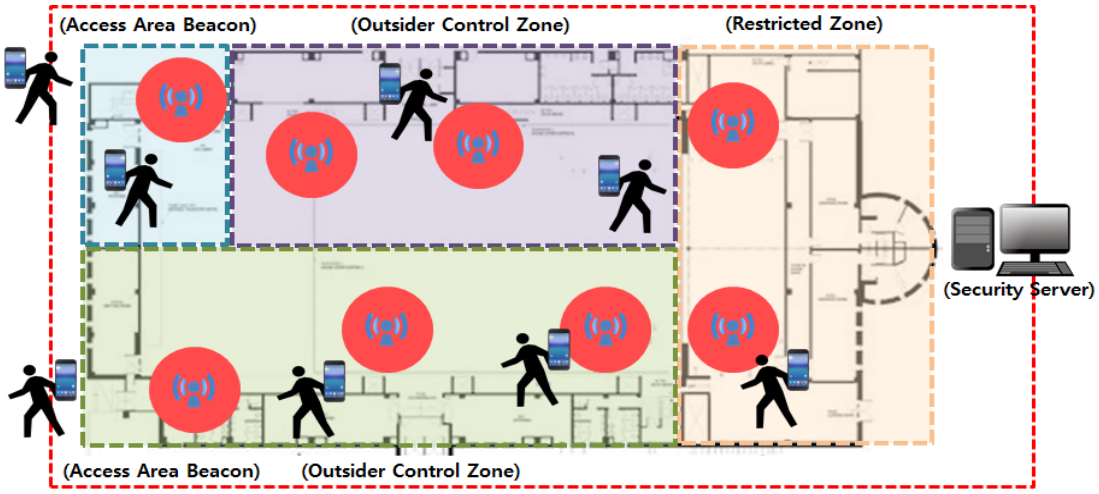

Figure 3:. Overall system configuration diagram

Figure 4 shows the outsider policy situation among the insider / outsider access control policy model.

① Outsider visitors are given a policy on user identification information and behavior restriction by installing a solution on their mobile device at the time of visit, and agree on the control procedures according to the solution.

② The camera and data transmission function of the mobile device is blocked by the control solution from the outside control area to the inside / outside control area.

③ For outside visitors, follow access control solutions for access areas and access to controlled areas.

④ The administrator monitors / controls the movement path provided by the control solution installed in the mobile device of the outsider party through the monitor.

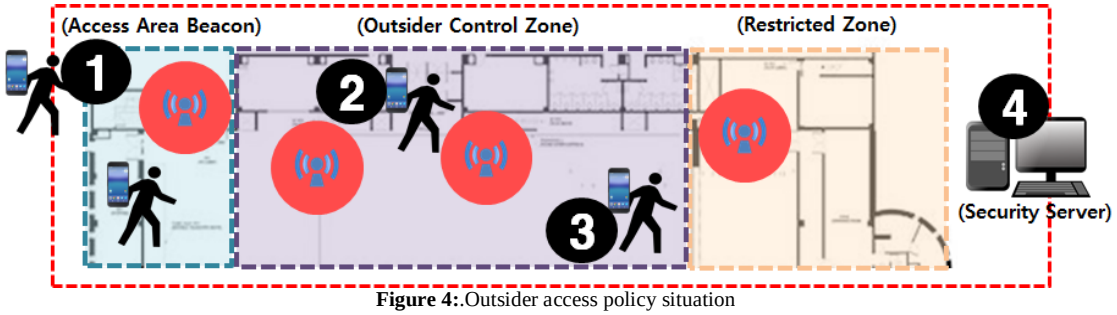

Figure 4:.Outsider access policy situation

Figure 5 shows the insider policy situation among the insider / outsider access control policy model.

① Policy insiders can pass through the access area through pre-installed solutions.

② In the case of insiders, it is possible to move without being affected by the outside control zone.

③ When accessing the inside / outside control area, the camera and data transmission function of the mobile device are blocked due to the control of the solution.

④ The administrator monitors / controls the movement path provided by the control solution installed in the mobile device of the outsider party through the monitor.

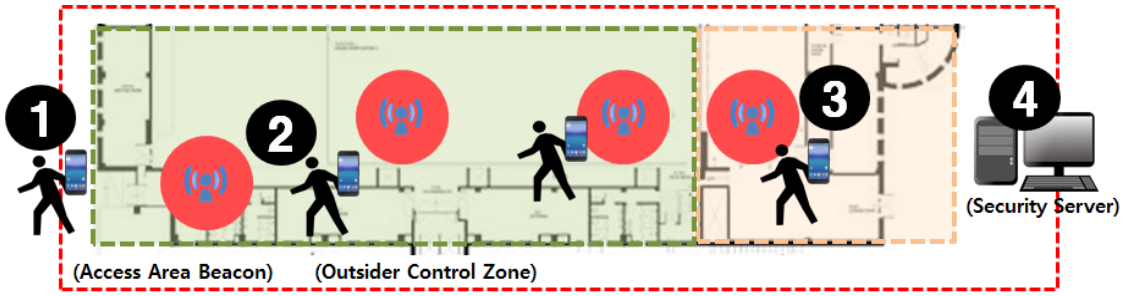

Figure 5:.Insider access policy situation

In addition, Beacon, ultrasonic sensor, and motion sensor were integrated and integrated to measure the position and motion information of insider / outsider inside the building. The indoor location measurement method using the integrated module proceeds to step 4.

In step 1, in the case of a visitor, a personal code unique to a user is generated using a coded sound wave signal, and position information is provided through coordinate confirmation of each sound wave signal. Also, the position of the visitor is obtained by triangulation through the RSSI value, which is a signal strength value between the mobile device and the beacon.

In step 2, the location and identity of the visitor are measured and monitored at every moment by the access control policy, insider/outsider authorization management policy, and control access.

In step 3, accuracy is important in a situation where a visitor approaches a certain area when moving in a building, and a precise position is measured by applying a hybrid positioning technique using heterogeneous sensors connected with Beacon. Based on this, we analyze the location-based behavioral pattern and accurately grasp the entry and exit lines and information.

The last 4 steps solve the problem of reflected wave processing by calculating the first time the electromagnetic waves reach the sensor when the visitor approaches the space between the layers in the building. When the positioning is completed, the information is used to limit the activities of inside and outside riches according to information access and space access authority.

4. Conclusion

So far, GPS is the core technology of positioning technology in outdoor location - based services.However, it is impossible to apply GPS in the shaded area such as the room, and a new technique for indoor positioning is needed.In order to solve this problem, existing services are based on the location of the user inside the building based on WLAN (Wireless Local Area Network), Bluetooth, Ultra Wide Band (UWB), Ultrasonic sound, Beacon And provided services based on user location.Especially, Beacon is the feature that battery consumption of smart phone is less than that of existing Bluetooth version. Also, even if the user does not take any action, he automatically detects the location of the user and provides related services.Due to this situation, research on new indoor positioning technology and network development for providing indoor location information service is underway in developed countries and global companies.Based on this, we are establishing an indoor location based business model that creates various added value.

Therefore, in this paper, we design Beacon based access control system.To do this, we design an integrated module that can

improve the accuracy and reliability of user's location by using Beacon, acoustic sensor, Wi-Fi and motion sensor.In addition, we design a security-enhanced Beacon-based access control system by establishing insider / outsider rights management policies.

To this end, we designed a system that can improve the accuracy and reliability of user positioning by using Beacon and heterogeneous sensors (ultrasonic sensor, Wi-Fi, motion sensor).In addition, we propose a security policy to establish access control policy by insider and outsider authority management policy.Finally, insider and outsider traceability system, authentication server, and visualization system are integrated into the overall access control system to analyze the behavior patterns of the passengers and propose an effective Beacon-based access security solution policy.

Acknowledgment

This research was supported by the research fund of Hanbat National University in 2017.

References

[1] Valentini GL, Lassonde W, Khan SU, et al. An overview of energy efficiency techniques in cluster computing systems. Cluster Comput. 2013;16(1):3–15.
[2] Wright J, Yang AY, Ganesh A, et al. Robust face recognition via sparse representation. IEEE Trans. Pattern Anal. Mach. Intell. 2009;31:210–27.
[3] Yang J, Zhang L, Xu Y, et al. Beyond sparsity: the role of L1-optimizerin pattern classification. Pattern Recognit. 2012;45(3):1104–18.
[4] Michahelles F, Thiesse F, Schmidt A, Williams JR. Pervasive RFID and near field communication technology. IEEE Pervasive Comput. 2007;6(3):94–6.
[5] Avoine G, Dysli E, Oechslin P. Reducing time complexity in RFID systems. International Conference on Selected Areas in Cryptography, LNCS. 2005;3897:291–306.
[6] Liu Y, Zhong Q, Chang L, Xia Z, He D, Cheng C. A secure data backup scheme using multi-factor authentication. IET Inf. Secur. 2017;11(5):250–55.
[7] Liu H, Darabi H, Banerjee P, Liu J. Survey of wireless indoor positioning techniques and systems. IEEE Trans. Syst. Man Cybern. 2007;37(6):1067–80.
[8] Lee HC, Lee DM. A study on localization system using 3D triangulation algorithm based on dynamic allocation of beacon node. J. Korea Inf. Commun. Soc. 2011;36(4):378–85.
[9] Lee D, Helal S, Sung Y, Anton S. Situation-based assess tree for user behavior assessment in persuasive Telehealth. IEEE Trans. Human-Mach. Syst. 2015;45(5):624–34.
[10] Chen Y, Kobayashi H. Signal strength based indoor geolocation. In: Proceedings of the IEEE International Conference on Communications (ICC '02). 2002; 1: 436 – 39.
[11] Park JH, Yang LT, Chen J. Research trends in cloud, cluster and grid computing. Clust. Comput. 2013;16(3):335–37.
[12] Pal A. Localization algorithms in wireless sensor networks: current approaches and future challenges. Netw. Protoc. Algorithms. 2010;2(1):45–73.
[13] Feng C, Au WSA, Valaee S, Tan Z. Received-signal-strength-based indoor positioning using compressive sensing. IEEE Trans. Mobile Comput. 2012;11(12):1983–93.
[14] Carretero J, Blas JG. Introduction to cloud computing: platforms and solutions. Clust. Comput. 2014;17(4):1225–29