2nd International Conference on Current Research Trends in Engineering and Technology
IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Bluetooth Low Energy based Fingerprinting

Kartik K Gajaria*[1], Bhavesh Bhanushali[2], Akshay Jani[3], Priyanka Puvar[4], Bhagirath Prajapati[5]
Department of Computer Engineering, A.D. Patel Institute of Technology, Anand, Gujarat, India

ABSTRACT

Since 2010, Bluetooth Low Energy (BLE) has been widely accepted as a most viable Bluetooth solution to projects having a power efficient architecture. The system makes use of Bluetooth Low Energy (BLE) Beacons installed on a specific subject of interest in addition with mobile devices on the client side doing all the required computation. In this case under a close proximity with the beacon, the mobile device shall compute and communicate with the server side services to verify the user fingerprint. Systems and methods are demonstrated for user authentication.

Keywords: Beacon, Bluetooth Low Energy (BLE), Close Proximity Communication, Fingerprinting

I. INTRODUCTION

In the recent years, Bluetooth low energy based beacons are being adopted for various places such as in super markets, etc. Different technologies have been tested for the close proximity applications such as the iBeacon protocol for the BLE beacons developed by the Apple Inc. Radio Frequency Identification (RFID) technology is another such example where transmission is triggered over a close proximity contact between the tag and mobile device.

In this paper, we will discuss the Bluetooth Low Energy to derive and demonstrate our solution. The key advantage with BLE is the minimal power consumption compare to the other technologies, which allow the transmission of beacons and power them continuously via batteries, in some cases until months and years. This opens an opportunity space to install these beacons at locations where the other technologies like IEEE 802.11 based WiFi access points and RFID would not have been possible.

In our solution, as illustrated in figure 1, we propose the use of such BLE beacons for the purpose of client authentication to private networks via data broadcasting. The beacon contains data which will be transmitted through an open channel, which will be captured by any BLE supported handset under a close proximity. In case of advertisement it is can be preferred to keep the data in plain text unencrypted format, which has been adopted widely. The use of BLE beacons in client authentication to private network is the key subject here where the data in the

beacon shall be encrypted and can only be decoded by the mobile application if and only if it generates a required hash output. This technique reduces the auto decryption overhead for each and every BLE beacon on the mobile handset and filters out the targeted beacons.

One such place where such technology can be utilized is to authenticate a target user group to a WiFi network where the authentication occurs from the beacon data but the targeted clients can be managed directly through the mobile application.

This way there is no human input required and only the authorised clients would be authenticated.

II. METHODS AND MATERIAL

Our goal is to evaluate and improve the close proximity advertisements and authentication techniques. We developed systematic processes for both advertisements and client authentication. Both involve an application on the client handset which shall support BLE scanning as a prerequisite. The application will run as a service on the client's handset and scan for any available BLE beacons nearby.

A. *User Authentication*

Here Authentication is done using a technique called "Fingerprinting". Fingerprinting assumes that each client has a unique identification which authorizes it to connect with the system. In our case the identification system is provided by the client side application, working alongside the server side services.

B. *Client side Phase*

When the client comes under close proximity with the BLE beacon, the application would fetch the data from the beacon and generate a hash value for it. The hash value is checked over a set of pre-defined acceptable hash values. If the output is valid then the beacon data is passed to our pattern check algorithm, which would pass the result over a comparator to check if it matches the required pattern. If the pattern check is successful, then an internal intent is sent to the data decryption module, based on our authentication algorithm, which will in turn return the key to the nearby private Wi-Fi network, hence, automatically connected to by the app itself.

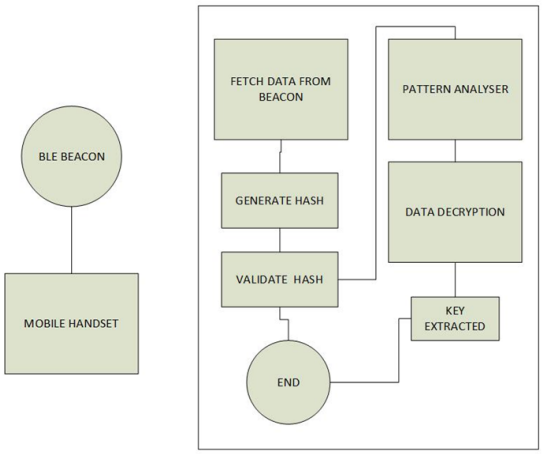

Figure 1: A workflow of how the beacon data is processed inside the mobile application.

III. RESULTS AND DISCUSSIONS

We have been using RFID tags for similar applications. In this section, we compared our proposed solution with the RFID based system.

A. Adaption and Compatibility

Beacons are designed to communicate with smartphones over a distance range of 1m to 70m, while the active RFID tags can go as long as 100m with an exception of higher power supply requirements. But while the RFID technology has its advantages, the adoption rate of RFID detection support in smartphones (Near Field Communication) is two in three, while generally all the smartphones in the market today support BLE.

B. Greater accuracy and convenience

While a RFID based communication will occur only when a tap occurs, a Beacon can be communicated with across a space. This brings added user convenience to the system over the RFID based systems. With that, consider a scenario where multiple users are to use this system at once. In the case of RFID communication, users would have to interface with the RFID tag in serial order. In case of a Beacon, the data is openly broadcasted to all the nearby users hence adding convenience with accuracy.

C. Overall Cost

Beacons typically cost around $10 to $50, which come battery powered and are flexible in terms of deployment and relocation. On the contrary, RFID technology costs $100 on average which is not designed for relocation.

D. Security

Since beacons are simply proximity detection devices which are used for broadcasting signals, there are no inherit security risks associated with them. With beacons, the vulnerability lies on the application, over how the application handles the data. On the contrary, when it comes to the RFID technology, which is tightly developed with IP network security solutions making it very secure in terms of transmission, the threat lies in the communication that happens between readers and tags. Because unlike the beacons which simply broadcast some data, RFID also transmits data related to the product itself such as the Electronic Product Code(EPC) which makes it vulnerable to threats like, clone tags, unauthorized readers, etc.

IV. CONCLUSION

In this paper, we have introduced a new technique to automate the user authenticate process using the BLE technology. This authentication process can be used with any services, for example – Airport check-in, Hotel check-in, Home security, etc.

We have tested our solution with the similar solutions in the market powered by different technology – RFID. In the tests our system not only overcomes the limitations of the RFID technology based systems but also adds additional advantages such as relocation support, low energy consumption, comparatively low cost and user convenience.

In the future, we will be testing the additional factors influencing the system such as the broadcasting parameters, the Transmission (TX) power, transmission interferences.

V. REFERENCES

1. Jae Hyung An and Lynn Choi, 2016, IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), (Dec 2016), ISSN No: 2166-9589, DOI: 10.1109/PIMRC.2016.7794891
2. Pavel Kriz, Filip Maly, and Tomas Kozel, “Improving Indoor Localization Using Bluetooth Low Energy Beacons”, Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2083094
3. Faragher, R., Harle, R., "An Analysis of the Accuracy of Bluetooth Low Energy for Indoor Positioning Applications," Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, September 2014, pp. 201-210.