**Abstract (150-300 Words) \*Very like original\***

Indoor localization has been widely studied due to the inability of GPS to function indoors. Numerous approaches have been proposed in the past and several these approaches are currently being used commercially. However, little attention was paid to the privacy of the users especially in the commercial products. Malicious individuals can determine a client's daily habits and activities by simply analyzing their Wi-Fi signals and tracking information. In this paper, we implemented a privacy-preserving indoor localization scheme that is based on a fingerprinting approach to analyze the performance issues in terms of accuracy, complexity, scalability and privacy. We developed an Android app and collected many data on the third floor of the FIU Engineering Center. The analysis of data provided excellent opportunities for performance improvement which have been incorporated to the privacy-preserving localization scheme.

Index terms: fingerprint, localization, privacy, homomorphic encryption, Paillier, DGK

**Introduction (300-500 Words)**

Discuss Problem of Location Accuracy and Privacy. Why is it bad for RSS (Signal Str.) and

MAC Address to be collected?

However, there are significant security threats to the individual is a malicious person were to collect data on someone’s phone location.

Potential Solutions & one solution some other person used

[Mention everything from previous article?]

Our Solution

In this paper, we will build upon the finger printing-based localization approach by implementing homomorphic encryption [CITE PREVIOUS REU]. Homomorphic encryption supports both addition and multiplication on encrypted data. The Android device will create a data entry consisting of the signal strength coming from the various access points. The device will send the data to a database which has been trained to localize a phone by computing the Euclidean distance based on the RSS strength on each fingerprint point. To preserve privacy, the data will be encrypted from the Android device and computed at the database. The problem that arises is akin to the Socialist Millionaire problem, where it is crucial that the database know from which AP is the Android app receiving the highest signal strength, but the values are encrypted for security purposes. Following a solution [CITE SAMET’S PAPER] a similar implementation has been completed using Java rather than C++.

What Objectives have been completed

Our contributions can be listed as follows

1) Creating an implementation of DGK using Java.

2) Extending the Socialist Millionaire’s problem and generating a solution to solve max/min for an array of encrypted integer values.

3) We study the performance tradeoffs in terms of computational complexity and location accuracy.

4)

Structure of this Paper (Very similar)

The structure of this paper is as follows. In next section, it will summarize related work in the topic of localization privacy. Section III describes the work flow. Section IV describes the implemented approach of fingerprinting and homomorphic encryption. Section V provides a detailed evaluation of the Android application. Section VI concludes the paper.

**Acknowledgement**

The student Andrew Quijano was supported by the US NSF REU Site at FIU. Program Grant No: REU-CNS-1461119.