NFC Based Services

**NFC-**

NFC is a set of communication protocols that enables two electronic devices to exchange data, one of which will be a portable device like a mobile phone or smart card. The range between the devices would be few centimeters. It operates at the frequency of 13.56 MHz. The maximum data transfer rate is 424kbit/s. There are three modes of operation-

* Reader/writer mode
* Card emulation mode
* Peer to Peer mode

**System Architecture-**

We are using a peer-peer architecture. The data relating to the user will be in a file in the smart phone. The desk/table will be connected to the database. The user data will be read from the file in the user’s phone the moment it comes to the proximity of the desk/table. Then this data is exported to the database. The time in the in the desk/table will also be exported to the database. This will make sure the time is not from the user device but from the verifier system.

Database

Desk/Table

(initiator)

User mobile device

Data from Data+TimeStamp

the device

This is the basic idea of the data insertion into database when the user taps their phone to NFC reader.

**Intern Timecard Punch-**

The idea of digitalizing the timecard punch for the employees is to improve deal with the proxies and to automate the salary accruing, leave details without the need of human intervention. All the smart phones are equipped with the NFC service. So, using the active mobile device is better than using the proximity cards and some other hardware tags. The system is a mix of hardware and software. It reader will be attached to the web server that is hosting the application. This will be an internet connected system onto which the application is hosted. There will be a database connected to the system.

When a new employee is being signed into the company, he must download and install an application that will collect the employee details and stores in the server. The data including the user’s device ID is sent to the server. The moment the employee brings his mobile phone to the NFC enables desk it reads the URL of the web based application. It will then read the employee’s device ID and match with the one that is stored in the database. The time at which employee’s device touches the NFC reader will also be noted and sent to the server. This will log into the new table the employee\_id, device\_id and the timestamp as in time. The use of device\_id will make sure that the employee is registering just one id from his mobile.

**Security Challenges-**

To make sure that the employee doesn’t bring in his colleague’s phone for sign-in, the employee will be encountered with a random challenge from the pool of challenges that the employee must provide during the registration process. There is a chance that the employee might have shared the answer for the challenges. So, to make the system more secure we can introduce a two-factor authentication including biometrics which can’t be duplicated. Being a punch-in system it is considered that network based attacks on the system are not present. When the phone is lost the user have to again register with the new phone, when there is a new registration the old registration with the same employee\_id must be deleted in the database.

**Dispatch-Subhaulers-**

We use the same web based application, except that the NFC enabled device is in the truck. All the process is the same except we need to add additional functionalities. The geotag of the location of the truck must be taken into consideration. This will be used for managing routes, pickups and reschedules. The [GoToTags NFC Encoder software](https://gototags.com/encoder/) can encode Geo Location records onto NFC tags by providing the encoding data on the “Custom Tags” worksheet in the [NFC tags encoding file](https://gototags.com/encoder/docs/nfc-tags-encoding-file/). Once the user is authenticated into the system, a new application that was already installed in the user’s phone pops open where he can send and receive messages. The messages are in the NFC Data Exchange Format(NDEF). The locations obtained can be mapped onto a graph after which we can apply various graph algorithms to manage the routes and pickups.

**Security Challenges-**

Being an internet based application, this system is prone to network based attacks where the data exchanged between the system might be changed in the transit. To prevent this NFC has Signature Record Type Definition protocol which is used to protect the integrity and authenticity of the NFC messages. Signing the NDEF record protects the integrity of the contents and allows the user to identify the signer if they wish. Signing certificates are obtained from third party [Certificate Authorities](https://en.wikipedia.org/wiki/Certificate_Authorities) and are governed by the NFC Forum Signature RTD Certificate Policy. Hence this public key authentication is used to introduce the integrity and authenticity.