# Authentication Protocol for Anti-Counterfeiting System using NFC

Fahmeeda Roohi
fahmeedaroohi@gmail.com
RV College of Engineering, Bangalore, Karnataka

B. K. Srinivas
bksrinivas@rvce.edu.in
RV College of Engineering, Bangalore, Karnataka

## ABSTRACT

*Counterfeit medicines are the medicines that were fabricated with the end goal of misleadingly addressing as valid, powerful and unique on the lookout. Such prescriptions cause extreme medical problems for patients. Fake medications inimically affect the human wellbeing. The companies which are genuine dangers to their income misfortune because of these fake medications. In this project we have developed an authentication protocol for counterfeit medications frameworks which relies on Internet of Things (IoT) to provide help in checking the genuineness of medications per "unit dose". Our convention utilizes the Near Field Communication (NFC) as it is helpful for portable environments. The protocol provides solid update stage for NFC. Besides, the strategy is complicated with evaluation of performance with the model for formal security examination.*

*Keywords*— *Counterfeit Medicines, Pharmaceuticals, Admin*

## 1. INTRODUCTION

The vast majority of businesses make substantial use of the cutting-edge Internet of Things technology. WHO defines counterfeit medicines as those that are fraud and purposefully labelled with identifiable information? Various counterfeit products, such as automobile components, cosmetics, food and beverage, and so on, cause challenges for various manufacturing companies. It poses a major hazard to pharmaceutical products. Counterfeit drugs don't come with a countermeasure.

According to the WHO, the use of counterfeit products has resulted in about 100,000 fatalities in Africa each year. In accordance with British "International Policy Network," tuberculosis and malarial drug use resulted in about 700,000 deaths per year. Counterfeiting is possible for both local and branded products. The salinity is high in several parts of Latin America, Africa, and Asia.

## 2. EXISTING SYSTEM

Legal medication manufacturing businesses adopt the systems where some pharmaceutical businesses use encrypted code labels on their packaging[1]. The user who wishes to buy a drug need to scratch the package label and send code to one of the systems of company , which validates the legitimacy of the medicine packet for free. The syringe is inserted after the drug packaging has been verified.

## 3. PROPOSED SYSTEM

### 3.1 Admin Web App
The admin is the super user and he is also called trusted authority (TA). Admin must have a separate login page and he can able to login into the home page using an authorized password. Once the admin login he can add product details. For each product, Hash code is generated and stored in the database.

### 3.2 Admin Android App
Admin can login to the android app with his credentials. Admin Can get the hash value of the product using product code. Once he gets a hash code, he can tap the NFC card and write hash code into the NFC card, while writing hash code is encrypted using XOR operation.

### 3.3 User Android App
Data users can able to register and login into their home page with an authorized password. The data user can tap the NFC card to check whether the product is genuine or not. Once the user taps the NFC card the hash code value is decrypted using XOR operation and sent to the server.

The server-side hash code is matched with the database hash value for the particular product. If it is matching the user will be notified as the product is genuine, if not, notified with a not genuine product.

## 4. SYSTEM ARCHITECTURE
The main focus of content architecture is on the way in which the content objects are structured and presented. The web architecture focuses on user interaction, navigation of web pages and presentation of the content. The web architecture describes the context of the environment in which the application has to be implemented.
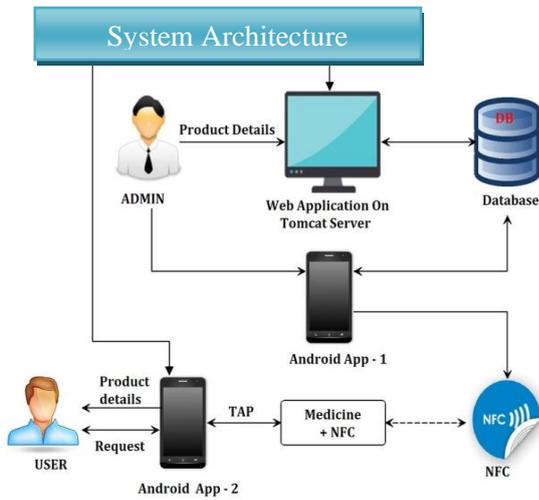
**Figure 1: System architecture for authentication protocol for Anti-Counterfeiting system using NFC**

## 5. DETAILED DESIGN

Detailed design focuses on each and every component of the application and interaction between each and every component. The sequence diagram describes about how and in what order the system objects are functioned. Detailed design of this application describes that when the user taps the NFC card on the NFC enabled mobile the data is fetched and hash code is generated then the product ID and hash code will be sent to the server and both the hash codes are compared and the result is sent to the users android phone which consists of android application.
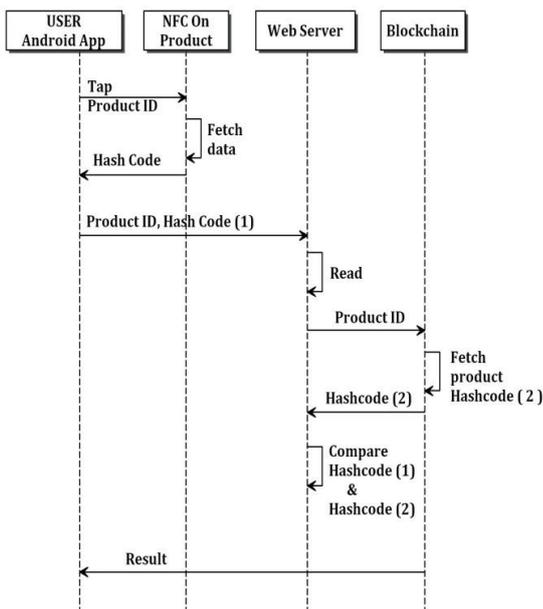


**Figure 2: Detailed Design**

## 6. METHODOLOGY

### 6.1 NFC Writing

NFC extends RFID frameworks which allows two-way communication between two end points, whereas previous frameworks, such as contactless smart cards, only allowed one-way communication. Because of the NFC tags that are unpowered may be read by NFC devices, it can also be used to replace older programs.

### 6.2 NFC Reading

When the user taps the card to the ATM, the XOR data is converted into original data before reading NDEF data from an NFC tag using the English language convention and sending the original data to the server. User data is loaded into the tag, but before it is stored into the card, it is declared an expectation channel, which tells the framework that it is authorized to use NFC. When NFC is recognized, Android should call a technique. Create a mechanism for putting together an NDEF message.

### 6.3 System Protection

A log file contains incredibly vital information that is delivered by the server, and it is used to examine any misuse of the service or any web application assault. Events and activities that occur when the service or application in runtime are also recorded in log files. Log files give you a clear picture of the operation of server as well as crucial information which includes about when the server was visited, how the server was visited, and "by whom" the server was visited. Because the application runs on the Apache Tomcat server, There are 2 log files generated by Apache HTTP server: the first one is access.log and second one is error.log. The entire file requests are recorded in access.log. If any of the user tries to access the below entry will be added to the log.

{88.54.124.17 - - [30/May/2021:06:35:10 +0110] "GET /result.php HTTP/1.1" 200 225 "-" "Chrome/5.0 (Windows NT 7.0; Ver64; rv:38.0) user/2010111001 Mozilla/45.0"}

The above log states that a file has been requested by the visitor of the server with an IP address of 85.34.127.167 on May 30th, 2021 07:44 and the request was successfully processed.

## 7. ANALYSIS

In the below table some of the features are mapped and compared with the existing systems.

| Various System available | Cost | Efficiency | Reliability | Security |
|---|---|---|---|---|
| Lightweight authentication protocol using NFC based Anti-Counterfeiting system | Less | High | High | High |
| counterfeit (fake) drugs & new technologies to identify it in India | High | High | High | Less |
| Counterfeit drugs and the online pharmaceutical trade, a threat to public safety | Less | High | High | High |

## 8. RESULTS

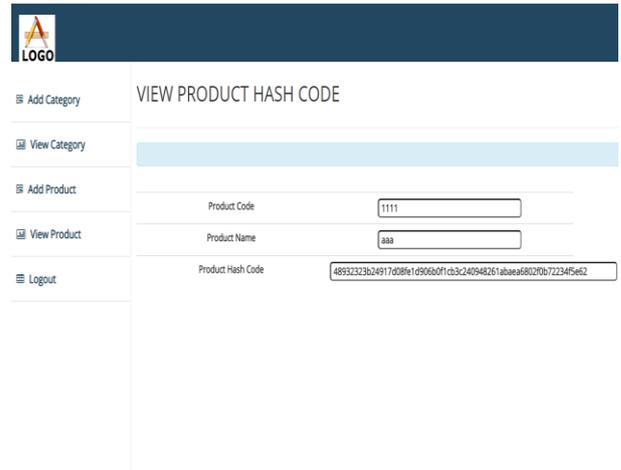Below screen shots are of web application which is handled by admin
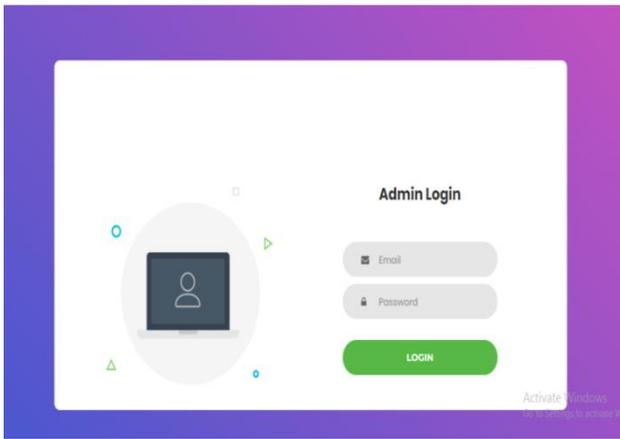
**Screenshot for admin login page**
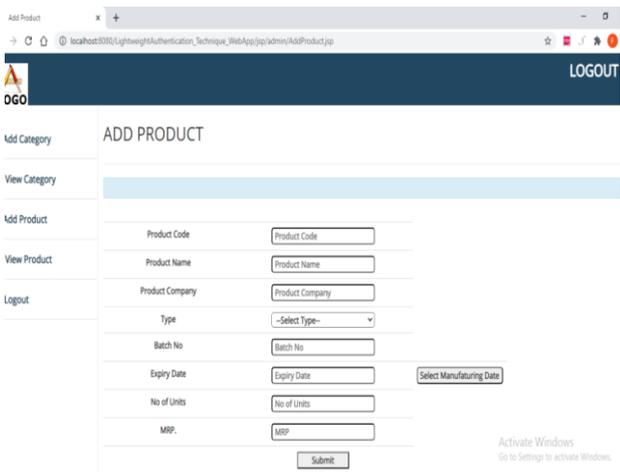


**Screenshot of admin web application**
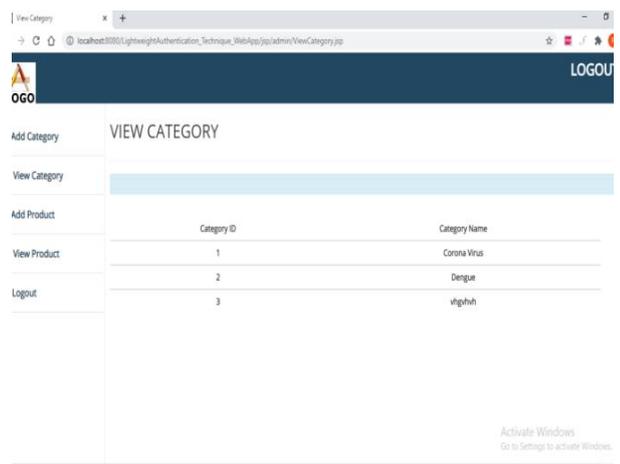


**Screenshot of admin web page for viewing product category**



**Screenshot of hash code generated in the web application**

## 9. CONCLUSION

The project's major goal was to develop an authentication process for anti-counterfeiting drug systems that would aid in determining the validity of pharmaceuticals per "unit dosage." The system aids in the verification of drug validity. Because of its wireless connection, NFC has emerged as a promising anti-counterfeiting technology. The proposed protocol has been shown to be capable of withstanding all attacks while retaining its own approaches and functionality.

## 10. REFERENCES

[1]   S. Choi, C. Poon, "An rfid-based anti-counterfeiting system", IAENG International Journal of Computer Science (2008).

[2]   M. Wang, Z. Yan, "A survey on security in d2d communications", Mobile Networks and Applications 22 (2) (2017) 195–208.

[3]   D. He, S. Zeadally , "Authentication protocol for an ambient assisted living system", IEEE Communications Magazine 53 (1) (2015) 71–77.

[4]  D. He, S. Zeadally , N. Kumar, J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security", IEEE Systems Journal 11 (4) (2016) 2590–2601

[5]  D. He, N. Kumar, N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks", Information Sciences 321 (2015) 263–277.