HIGH SECURITY IN AUTOMATED FARE COLLECTION FOR TOLL SYSTEM WITH NFC USING AES ALGORITHM

Shilpa. D[1], Jayasri. R[2], Sanjana. R[3], M. Abirami[4]

[1]*Shilpa. D, Anna University, Chennai*
[2]*Jayasri. R, Anna University, Chennai*
[3]*Sanjana. R, Anna University, Chennai*
[4]*M. Abirami, Department of Computer Science and Engineering, Panimalar Institute of Technology, Tamil Nadu, India*

---***---

Abstract - *AFC Automated Fare Collection is gaining popularity in terms of public transportation where the transportation fee is calculated based on the length of the trip time or based on the trip distance, AFC can read the NFC (Near Field Communication) tag from where AFC will gather all the relevant data about the trip. As Technology is growing, there will be security problem with the NFC card, as many Smartphone comes with the same frequency that are associated with the NFC card, so it became easy for any user to change the information that are stored in the NFC, information like the check in time or shorten the route they have travelled that cause a drastic change in the price calculation. Our proposed model will provide all the necessary security. This proposed project provides protection to the entrance data and to monitor the behaviour of an individual user. This project demonstrates a simple payment system using NFC tag and a smart phone for AFC in metro and toll.*

Key Words: *NFC card, AFC, AES Algorithm, Mobile Payment, Wallet creation*

1. INTRODUCTION

As we all know, a normal toll collection takes a lot of time and there are traffic jams and we won't get the transparency in toll amount collection. For this, the introduction to RFID was done. It was also used for tracing vehicles. The drawback of RFID was that, it doesn't work properly in the cloudy climate. To overcome this drawback, we introduced NFC i.e. Near Field Communication. Also, AFC (Automated Fare Collection) is gaining popularity in terms of public transportation where the transportation fees is calculated based on the length of the trip time or based on the trip distance. AFC can read the NFC (Near Field Communication) tag from where AFC will gather all the relevant data about the trip. As Technology is growing there will a security problem with the NFC card, as many Smartphone comes with the same frequency that are associated with the NFC card, so it became easy for any user to change the information that are stored in the NFC, information like the check in time or shorten the route they travel that cause the drastic change in the price calculation. Our proposed model will provide all the necessary security.

1.1 Contactless Payment

Contactless payment systems are the credit cards and debit cards, or other devices, including smartphones, that use radio-frequency identification or near field communication for making secure payments.

1.2 Mobile payment

Mobile payment the payment services operated for financial regulation and performed using a mobile device. Instead of paying with cheque, cash or credit cards, a consumer can use a mobile to pay. Although the concept of using currency systems has a long history, it is only in this century that the technology to support such systems has become widely available.

Mobile payment is been used all over the world in different ways.

2. EXISTING SYSTEM

Automated Fare Collection (AFC) systems have been globally deployed for decades to automate manual ticketing and charging systems likes metros and toll, where the trip charge can be calculated based on the information that is stored in the NFC Card, provided in the station. While the card is displayed, AFC will reduce the amount based on the trip distance (trip time) and data is stored in the NFC in plain text format, and these would became a security problem as many smart phones are provided with inbuilt NFC. More over the frequency that the smart phones are provided is same as that is contained in the card so it became easy for any user for tampering the data in the card.

The trip information are sent to sever only at the time of completion of the trip since it became hard to cross check the information that are associated in the card while calculating the fair.

3. PROPOSED SYSTEM

The proposed system has two different methodology for providing security in AFC system. Protection for Entrance data and Fair collection. Protecting the Entrance Data is the process in which, whenever the user enters the toll then that entrance information will be encrypted and transmit the encrypted information to the server. If user changes any information in the card, that information will not be changed in the server. At the fair calculating unit, the card information is read and decrypted and also the information is cross verified in the server. Based on the result, the fair will be calculated and each log is maintained in the server, to easily track the particular user.

A complete environment for monitoring the behaviour of an individual user is done by means of driving licence info, insurance info .etc. And all this information is attached with the NFC card. While providing the card to the toll System, it automatically checks all the necessary parameter as it is.

4. METHODOLOGY

Fig 1: Working module

Every individual can register their vehicle for a NFC tag. This tag will be given a unique ID, feasible to use with that vehicle only. And an account is created for the use of that particular smart tag and maintain transaction history in the database. The user needs to deposit some minimum amount to this account.

Every time a vehicle approaches the toll booth, first the presence of the vehicle is detected. It will in turn activate the NFC circuit to read the NFC enabled smart phone. The transaction will begin, depending upon the balance available, toll amount will be deducted directly. The information like the insurance and driving licence info is checked at the same time as the payment. The software updates the details in the Centralized database server. A mechanism to generate the bill and will be sent to user as a text message.

5. IMPLEMENTATION

Fig 2: Hardware assembly

5.1 Near Field Communication

NFC allows devices that are closely placed, to wirelessly transfer data back and forth. The technology is almost like Bluetooth, but NFC uses far less power and works over much shorter distances.

In the world of consumers, producers, use of NFC technology to initiate contactless payments via credit cards or mobile devices. Rather than physically swiping the plastic, consumers simply move their smartphone or card across an NFC reader to automate transactions.

NFC payment technology already comes with most Android and iOS devices and a growing number of credit and debit cards. Now contactless payments are turning to be mainstream, with a growing number of stores and restaurants adding their own in-store NFC readers — including McDonald's etc.

Fig 3: NFC chip

5.2 How does it work?

For NFC, a user should either touch or show his phone to an enabled device and he or she will be able to share data without physically building up a connection. Nowadays, this innovation has been set in many Android, Windows and iOS phones. Hence, NFC has turned out to be more necessary than any other technology in recent times, especially when it's about mobile payments.

After installing the payment app on the phone, one needs to tap the phone on the credit card terminal and a connection will be made using NFC.

Presently, there are some NFC compatible cell phones like Samsung's Galaxy Series, Google's Nexus Series, and the iPhone. These are the following NFC applications that can provide a layer of security to the transactions:

1. Google pay
2. Samsung pay
3. Apple pay
4. Android pay

5.3 Advantages of NFC

NFC technology comes with various security features that help to protect financial data from prying eyes, including:

5.3.1 Proximity Protection

Contactless payment solutions work over short distances. This proximity protection represents the first level of defence in NFC.

5.3.2 User Initiation

To begin each transaction, the customer must initiate the contactless payment process. This usually requires a NFC application to be launched within the phone in order to create a connection between the device and the reader. So even if a thief gets closer, no transactions can happen in standby mode.

5.3.3 Secure Element Validation

Whenever a connection has been made, the mobile device has to be validated, this process assigns a unique digital signature to every payment rather than transferring credit card numbers between the device and the reader.

Working Arena

Fig 4: Implementation of NFC based toll collection system

6. ARCHITECTURE OF NFC BASED TOLL SYSTEM

The components of the NFC based toll collection system technology work as follows:

6.1 User Registration & Wallet Creation

Initially user needs to register into bank application as fair reduction would be based on the user account detail, then the user needs to register their name in the server then the server will generate the particular unique id to the user. Based on that id sever can able to track the particular user. Once the user logins, he or she needs to add the particular amount to the server wallet or add the corresponding account information in the server so that the AFC will automatically reduce the amount from the user account.

6.2 Vehicle Insurance Checking

Whenever a vehicle passes through a toll gate user uses NFC tag to swipe through toll gate so that amount will be deducted automatically. At the same time the automated fair collection machine also checks for the vehicle insurance to check whether it is valid or expired. If toll machine finds that the insurance is expired it automatically updates the database. Once vehicle insurance expiry is found, vehicle will be blocked and it cannot pass through the toll gate till the insurance amount is reduced from the user account.

6.3 Track the particular User

Based upon the User ID we can track the particular user and the amount of fair he paid when he passes through the toll gate. If a vehicle is theft it becomes easy to track vehicle and find it by law enforcement agencies.

6.4 Protecting User Entrance Data

Another way to avoid the data tampering by using NFC is make that Process online and protect the entrance data. Whenever the user enters into the station then the information will be recorded into the NFC card as an cipher text and as well as that information will be loaded into the server with the time of entrance and the way that user enter so that if any user try to change any information in NFC card by using mobile phone, that information will not be changed into the server, if user place the card in the exit end then the AFC will cross verify the data into the server and reduce the accurate amount from the user account or wallet.

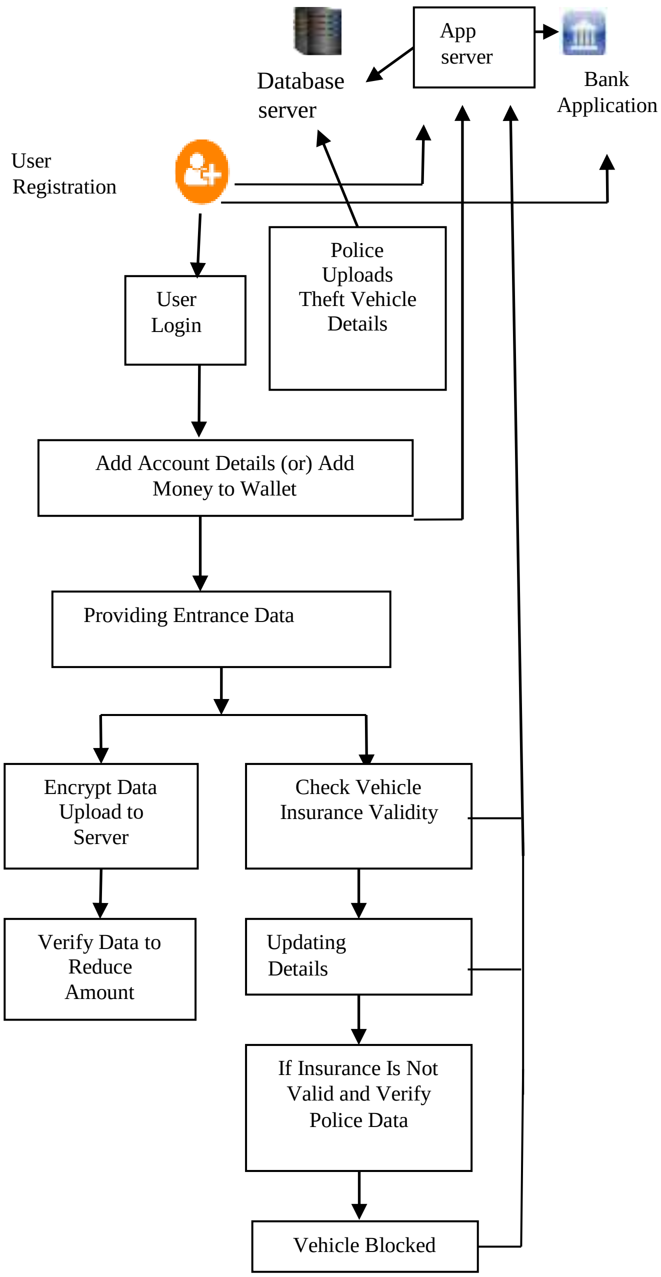
Database server
App server
Bank Application
User Registration
User Login
Police Uploads Theft Vehicle Details
Add Account Details (or) Add Money to Wallet
Providing Entrance Data
Encrypt Data Upload to Server
Check Vehicle Insurance Validity
Verify Data to Reduce Amount
Updating Details
If Insurance Is Not Valid and Verify Police Data
Vehicle Blocked

Fig 5: NFC based toll collection system

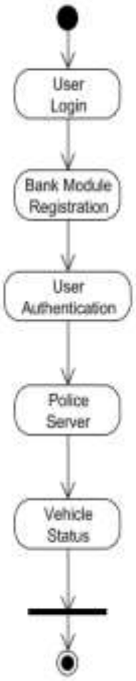

Fig 6: Working of system

7. CONCLUSION

A new security system, named Near Field Communication, for automatic fare collection in toll system is proposed. Digital transformations has changed the world and every startup has embraced the contactless payment frameworks. In the future, we will pay with our phones and NFC applications are the ticket to that wonderful future ahead. Because of the numerous current Smartcard information breaches, now is a great time to use a solution that protects our wallets from robbery and fraud. An alternative security algorithm is proposed, called AES algorithm and additionally insurance and driving license details are added to the system.

REFERENCES

[1] F. Dang, P. Zhou, Z. Li, E. Zhai, A. Mohaisen, Q. Wen, M. Li, "Large scale invisible attack on AFC systems with NFC-equipped smartphones", Proc. IEEE INFOCOM, pp. 1-9, 2017.

[2] F. Dang, P. Zhou, Z. Li, Y. Liu, "NFC-enabled attack on cyber physical systems: A practical case study", Proc. IEEE INFOCOM workshop, pp. 289-294, 2017.

[3] C. J. Mitchell, "On the security of 2-key triple DES", IEEE Trans. Inf. Theory, vol. 62, no. 11, pp. 6260-6267, Nov. 2016.

[4] Xi Chen, X. Wu, X. Li, X. Ji, Y. He, Y. Liu "Privacy-aware high-quality map generation with participatory sensing", IEEE Trans. Mobile comput, vol. 15, no. 3, Mar. 2016.

[5] M. Roland, J. Langer, J. Scharinger, "Relay attacks on secure element-enabled mobile devices", Proc. IFIP Int. Inf. Secur. Conf., pp. 1-12, 2012.

[6] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, B.-Y. Yang, "High-speed high-security signatures", J. Cryptographic Eng., vol. 2, no. 2, pp. 77-89, Sep. 2012.

[7] R. Verdult, F. Kooman, "Practical attacks on NFC enabled cell phones", Proc. Int. Workshop Near Field Commun., pp. 77-82, Feb. 2011.

[8] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones", Proc. Int. Workshop Radio Freq. Identification: Secur. Privacy Issues, pp. 35-49, 2010.

[9] G. de Koning Gans, J.H. Hoepman, F. D. Garcia, "A practical attack on the MIFARE classic", Proc. Int. Conf. Smart Card Res. Adv. Appl., pp. 267-282, 2008.

[10] E. Haselsteiner, K. Breitfu"Security in near field communication (NFC): Strengths and weaknesses", Proc. Int. Workshop Radio Freq. Identification: Secur. Privacy Issues, pp. 12-14, 2006.