International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I4P111

Volume 69 Issue 4, 63-65, April, 2021
© 2021 Seventh Sense Research Group®

Review Article

Survey on Automated Fare Collection and Document Verification

Bhuvaneswari S[1], Rishi S[2], Prathip Kumar K[3] , Vishnu Raj K[4]

[1] Computer Science and Engineering,Easwari Engineering College, Anna University, Chennai, India
[2,3,4] Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India

Received Date: 17 March 2021
Revised Date: 23 April 2021
Accepted Date: 26 April 2021

Abstract *- Near Field Communication (NFC) is an upcoming technology which offers a wide range of services, from access keys for offices and houses to payment and trusted applications. NFC devices have become the need of the hour for the data transmission that takes place within shorter ranges i.e. the distance of 4cm. It involves the usage of the Internet for the payment transmission to occur. Security is the important parameter to consider when the internet is involved because there is a high percentage of risk during money transfer and data breach can take place if no proper security mechanisms are implied. Hence the NFC devices should be employed with proper security protocols. This paper discusses various NFC applications and their security protocols.*

Keywords *– NFC Technology, AFC system.*

I. INTRODUCTION

Security is the biggest concern in the NFC based systems.In the toll, people prefer contactless payment over the physical payment because they are swifter and more convenient in terms of fare collection.The vehicle's document and the driver's license are not being checked at the highways. In recent years there has been an increase in the number of accidents which takes place at the highways specifically during the night time. The current system in the National Highways of India(NH) uses,

- Physical payment and contactless payment methods through RFID which are less secured and have lower data transfer data compared to NFC.
- The system does not maintain any geographical location of the vehicles.

II. LITERATURE SURVEY

Fan Dang at el [1] has implemented a lesspay attack on the existing AFC system to reduce the fare charged for the metro rides, considering 100 users are present in it and also has provided countermeasures such as Limiting Frame Waiting Time, Protecting the Entrance Data, Computing Fare via Online Data-Sharing, Using Dynamic QR Codes instead of AFC Cards to prevent lesspay attack. To begin the attack, we first collect entrance data using a lightweight app installed in the client's mobile. Secondly, the client's station information is collected by reversing the E-card tapper application using APKtool and the stored station information is extracted from the database. On the Client side, an emulated card (ISO/IEC 14443) is implemented for communicating to the terminal with false entrance data but same data structure as original and the location of the client is fetched by the use of Android API via Cell-ID and wifi. To deploy the debit command, a request is sent to the proxy card in the cloud side. On the Cloud side, which is built using AKKA, to get the nearest city from the client's location we use PostGis and Cartesian distance method. Once the request is received from the client, the proxy card which comprises ACR122u card reader and a physical card is activated. The physical card is dispatched using LRU dispatching algorithm and we set the card to a state INUSE for 2mins. After a successful transaction, the state is set to AVAILABLE. Among the 4 countermeasures the most effective ones are Online fare calculation and Dynamic QR code. Nowadays, the AFC system is operated in offline mode. Our system proposes the use of online transactions by which the trip details are updated twice, one at starting and other at end. The fare is deducted on a daily basis or monthly basis from the account which has been linked with the user's AFC card.

S.N. Akshay Uttama Nambi et al [2] has developed two applications, 1. NFC Smart Kiosk and 2. NFC smart web poster, based on Near Field Communications. The NFC reader is developed using JAVA and the data transfer between the mobile app and the NFC reader is done by peer-to-peer communication which is implemented using JSR-257 contactless communication API. In NFC smart web posters, the information is stored as a URL in the Mifare card(ISO/IEC 14443) and the URL is read using a NFC enabled smartphone in reader mode. The results show that the NFC can be integrated into mobile phones to develop a set of applications.

Nahar Sunny Suresh Shobha et al[3]proposed a new approach for the field of payments using Near Field Communications cards which has been derived from RFID and the concept of magnetic induction. Each and every NFC payment is done by taking and linking two points of data namely, NFC tag and an encrypted password. A special code is sent from the user's mobile phone using a secure NFC radio to the respective payment system and in return the system sends the transaction details. A PIN number is required to authorize any transaction. In order to stay protected against hackers, the NFC radio communicates with only one app on the mobile phone which is completely isolated from the rest of the Operating System. This system has the advantage of making a payment securely and also with a single tap.

Walter Austin Hufstetler at el[4] has designed a two step verification application/software for computers using Near Field Communication technology. The application is developed using C# with the help of pGina. In this system, the authentication involves two factors, 1) Passcode 2) Scanning of NFC card. To avoid data leakage, the NFC's Unique Identifier Number and the Passcode is stored as an encrypted text using Advanced Encryption Standard to the computer. User is authenticated into the system by entering the passcode, additionally NFC card is scanned and the UID of the card is verified with the UID stored in the computer. If the authentication fails, a text or e-mail is sent by Simple Mail Transfer Protocol(SMTP) to the account owner. And the login Activities are being recorded in the system. The success rate of this system is nearly 100 percent. One of the disadvantages is that only one user credentials can be stored to the system.

Vedat Coskun at el[5] discussed an alternative solution that suggested a prototype for Near Field Communication Technology using cloud computation method. Security Element (SE) which is used commonly are 1) Embedded Hardware based SE 2) SMC based SE 3) UICC based SE. The main restrictions in these are 1) Storage capacity is limited to the mobile phone. 2) The speed of retrieval and saving process is based on the processor of the mobile phone. 3) Accessibility to data stored is limited to the mobile phone unless there is a gateway or bridge to the data that is maintained. 4) Loss or theft of the mobile phone will result in high financial risks. These restrictions are resolved by the proposed prototype by integrating the SE to the Cloud System. The prototype has the advantage of 1) Unlimited data storage as the capacity isn't bound to a physical device. 2) Accessibility of the data is swift due to the current networking speed. As a result, this prototype proves that the SE integrated to the Cloud is more efficient than conventional techniques.

Anusha Mandalapu at el[6] resolves the problems such as Peeping attacks, Skimmers, Brute-Force attack, Retrieving passwords from the systems using Near Field Communication featured three level authentication system. This authentication system is constructed on the basis of following parameters: NFC reader, Dash Matrix Algorithm, Pattern Value Password, One Time Password, Negative Pattern Password and Quick response code. A website is created for the registration of NFC enabled transactions. At first the personal details of the user are collected. Furthermore, a pattern password has to be drawn in a single stroke by the user and it is stored to the system for authenticating the user. Finally, an acknowledgement is received by the user along with a Negative Pattern Password, created by the bank for card blocking. At the ATM when the user taps on to the tag installed, an URL is sent to the user's mobile phone. Pattern Value Password has to be entered by the user for the authentication process and it is carried out by using Dash Matrix Algorithm. At last, an OTP is generated on the screen and it must be entered by the user at the ATM to complete the process. For card blocking, the user must enter the Negative Pattern Password generated by the bank at the registration process. Afterwards, a QR code is displayed at the ATM screen, and has to be scanned and verified by the user.

Romeo L. Jorda Jr. at el[7] proposed a system for Door lock automation with an automated circuit breaker using Near Field Communication Technology. The Hardware components used for the construction of the system are : Raspberry pie, NFC tags/readers, NodeMCU ESP8266, Deadbolt Lock, Automated Circuit Breaker, WLAN Repeater, Servo Motor. The softwares used in the development of the system are: Arduino IDE for subsystems, Python for main system, and MySQL for the database. Initially, the NFC reader reads the user's NFC card for authentication. If the process is successful then the user is allowed to pass, If not read again until authenticated. Once the user passess, the respective user credentials is uploaded to the database and a record is maintained. After the completion of the job, the user once again taps on to the reader which triggers the circuit breaker to turn off the power. NFC is more secure than any other technique, when it comes to e-payments and door locks.

Jonghyun BAEK at el[8] discussed two secure and lightweight protocols such as hash function and XOR operation for the authentication of NFC based applications. This proposal suggests separate authentication techniques for NFC tag and NFC smartphone.At first, a random number is generated by the server for both the tag and smartphone, which are matched to them with respect to their unique ids. When the smartphone communicates with the tag, a random number is generated by the tag using a hash function and sent to the server via the smartphone, if the random number is matched with the data stored in the server the authentication of the tag is successful, else an error message is delivered to the smartphone. For the authentication of the smartphone, a random number is generated by the device using which a partial id of the tag is obtained and it is sent as a request to the tag itself. The tag computes the request using the hash function to a D-request format and the D-request is sent back to the device. Finally, the partial id, D-request and the random number are sent to the SP server, where the device is authenticated using XOR operation. If the authentication is successful, a new random number is generated for both the tag and smartphone, else the session is terminated.

Nurbek Saparkhojayev at el[9] designed a NFC enabled Access Control and Management System for locking / unlocking mechanism of doors. The mechanism by which the system functions is by the help of HCE Mode and Near Field Communication Technology. Firstly, the smartcard which is of ISO 7816-4 standard is fixed in place of door lock. When the user taps the mobile phone, communication occurs between mobile phone and NFC reader . The system functions in two phases namely: 1)Registration Phase 2)Locking/Unlocking Phase. In the phase of registration, the user raises a request to the server and the server generates an unique UID and public key. The public key is to encrypt the data transfer which is created using the RSA Algorithm. The generated UID and the public key are sent back to the user. The user in return sends the UID,public key,System ID to the server.Once the details are received successfully by the server the registration process is complete and the details are stored in the database. In the locking/unlocking phase,when the user taps the mobile phone against the smart lock,the System ID is sent to the server. The server verifies the ID with the stored ID, if a matching entry is found, it sends the release command and the door is unlocked. If the ID does not match with any entry in the database, the server sends an alert message to the user.

Maali Alabdulhafith at el[10] designed an application for multi-morbidity patients which is used to detect the drug allergy using the Near Field Communication Technology. The application involves two phases :1)Function 2)Update. The actors in the application are Patient,Nurse,Physician,Pharmacist. The application maps each drug to separate NFC tags and the patient wears a NFC tag which contains the details of his medical history and his drug allergy details. The first phase of the application is divided into three phases:1)Reading 2)Information Retrieval 3)Sending/Alerting Phase. In the reading phase, the nurse scans the patient's NFC tag from our application. The details are sent to the database which is maintained by the hospital server. The information about the patient's history is retrieved from the database and sent to the nurse. If the person is allergic to certain drugs, an alert is sent to a physician and pharmacist . The alert is sent via text message, which consists of only basic patient information and the drug which they are allergic to . A detailed report about the patient's medical history is sent via email to physician and pharmacist. If the nurse finds any new allergy the details are uploaded to the application in the updation phase. The nurse enters the drug information into the application against the patient's details. The details are saved and uploaded to the database.

III. CONCLUSION

Near Field Communication is a booming technology which is used in wireless communication for shorter distances. This survey lists different applications which employ NFC technology and their uses in several fields. The paper provides new approaches to increase security levels in the NFC based systems which are used for payments.

REFERENCES

[1] Fan Dang, Ennan Zhai, Zhenhua Li, Pengfei Zhou, Aziz Mohaisen, Kaigui Bian, Qingfu Wen, Mo Li,'Pricing Data Tampering in Automated Fare Collection with NFC-equipped Smartphones', IEEE Transaction on Mobile Computing,IEEE, 18(2019).

[2] Akshay Uttama Nambi S.N.,Prabhakar T.V ,.Jamadagni H.S. ,Kishan Ganapathi, Pramod B.K., Rakesh C.M., Sanjay Naik R. ,'Near Field Communication – Applications and Performance Studies, International Conference on Information Processing,SpringerLink,:292(2018).

[3] Nahar Sunny Suresh Shobha, Kajarekar Sunit Pravin Aruna, Manjrekar Devesh Parag Bhagyashree, Kotian Siddhanth Jagdish Sarita ,'NFC and NFC payments: A review',International Conference on ICT in Business Industry & Government (ICTBIG) (2016) 2-8

[4] Walter Austin Hufstetler; Maria Jose Hito Ramos; Shuangbao Wang, 'NFC Unlock: Secure Two-Factor Computer Authentication Using NFC', IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS),(2017)507-510,

[5] Vedat Coskun; Busra Ozdenizci; Kerem Ok; Mohammed Alsadi, ' NFC loyal system on the cloud',7th International Conference on Application of Information and Communication Technologies. (2014)21-25.

[6] Anusha Mandalapu,Daffney Deepa V,Anish Dev J,Laxman Deepak Raj, 'An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies,International Conference and Workshop on Computing and Communication (IEMCON),(2015)29-34.

[7] Romeo L. Jorda; Joshua Renz A. Coballes; Lejan Alfred C. Enriquez; Mark Lester S. Millan; Angelo J. Mora,Melbert Neil G. Teodoro,Nilo M. Arago,August C. Thio-ac,Lean Karlo S. Tolentino,'Comparative Evaluation of NFC Tags for the NFC-Controlled Door Lock with Automated Circuit Breaker',IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), (2018)260-265.

[8] Jonghyun Baek; Heung Youl Youm, Secure and Lightweight Authentication Protocol for NFC Tag Based Services,10th Asia Joint Conference on Information Security,(2015) 63-68.

[9] Nurbek Saparkhojayev, Aigul Dauitbayeva, Gulnaz Baimenshina, Aybek Nurtayev, NFC-enabled Access Control and Management System',International Conference on Web and Open Access to Learning, (2014) 208-212.

[10] Maali Alabdulhafith, Raghav V. Sampangi, Srinivas Sampalli, 'NFC-Enabled Smartphone Application for Drug Interaction and Drug Allergy Detection', 5th International Workshop on Near Field Communication (NFC), (2013)512-518.