iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3543

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Security Enhancement in ATM System Using NFC and QR Based Approach

S. Mary Rexcy Asha[1], P. Soma sundaram[2], S. Nanthakumar[3], A. Nalayiram[4], M. Madan[5]
[1, 2, 3, 4] *Department of Information Technology, Panimalar Engineering College, Anna University*

Abstract: ***In smart factories and smart homes, devices such as smart sensors are connected to the Internet. Independent of the context in which such a smart sensor is deployed, the possibility to change its configuration parameters in a secure way is essential. Existing solutions do provide only minimal security or do not allow transferring arbitrary configuration data. In this paper, we present an NFC- and QR-code based configuration interface for smart sensors which improves the security and practicability of the configuration altering process while introducing as little overhead as possible. We present a protocol for configuration as well as a hardware extension including a dedicated security controller (SC) for smart sensors. For customers, no additional hardware other than a commercially available smart phone will be necessary which makes the proposed approach highly applicable for smart factory and smart home contexts alike.***
Keywords: Internet of Things, Configuration, Near Field Communication, Radio Frequency Identification, Security Controller.

I. INTRODUCTION

This project is actually presents an secure config NFC and QR-Code based hybrid approach for smart sensor configuration. With the support of ATM, though banking becomes easier, it also became feeble. There has been countless gear of abuse that have in use in banking transactions. Thus there is a essential need to provide high security. This paper proposes the amalgamation of Face Recognition System in the identity verification process engaged in ATMs to enhance the security system. In smart factories it is essential to perform maintenance operations of sensors involved in the production prcoess. By introducing a secured and easy to use configuration interface, even untrained staff can perform firmware updates or configuration changes. However, it is very important to protect the confidentiality and authenticity of configuration data as employees applying the configuration updates could be potential adversaries. By enabling any employee or external person to perform configuration operations, the flexibility of the already deployed sensors will be increased while the associated maintenance costs will be decreased.

The approach presented in this paper not only is able to transfer cryptography keys but also arbitrary configuration data and firmware updates. To transfer data, NFC technology is chosen for three reasons. (i) NFC offers some security advantages compared to other wireless technologies [6]. Also, certain kinds of attacks such as man-in-the-middle are harder to conduct due to the limited communication range of NFC.

The update process can be performed without an internal power source, if the necessary hardware is powered by the NFC field. NFC is easy and intuitive to use. Humans easily understand the principle of bringing one device near to another to transfer data

II. METHODS AND RELATED WORK

A. Radio Frequency Identification

RFID tag is a small device which stores and sends data to RFID reader. They are categorized in two types – active tag and passive tag. Active tags are those which contain an internal battery and do not require power from the reader. Typically active tags have a longer distance range than passive tags. Passive tags are smaller and lighter in size than the active tags. They do not contain an internal battery and thus depend on RFID reader for operating power and certainly have a low range limited up to few meters. o recognize the identity of an RFID tag, RFID reader sends radio signals which is captured by the coil (working as antenna) for the tag. The coil receives these signals as alternating current and passes to the chip. The chip extracts both the power and the information from this alternating current. By communicating with the non volatile memory of the chip that stores unique id as well as other information, it sends back the required signal to the antenna which is then transmitted to the RFID reader.

B. Near Field Communication

NFC devices are compatible with many existing RFID devices and tags as the NFC standard comprises various RFID standards [8]. NFC is used in a diverse range of businesses. Today, the most well-known application of NFC is in the mobile payment sector [9]. Coskun et al. [10] note that NFC is also widely used in mobile ticketing applications. Another prominent field for NFC is the

Internet of Things (IoT). Atzori et al. [11] state that *NFC [...] together with RFID [...] will link the real world with the digital world.*

C. Quick Response Code

A QR code is a two-dimensional code that offers various advantages over traditional (linear) barcodes such as a much higher data density or the possibility to read QR codes from all directions. The higher density allows a maximum capacity of 2953 bytes. Although the encryption of a QR code's content is possible, encrypted QR codes can be rarely found [12]. Therefore, Conde-Lagoa et al. [13] suggest to encrypt the content using symmetric cryptography. Soon [14] lists sample applications such as ticketing or identification of all sorts of items. Christian Lesjak, Thomas Ruprechter, Holger Bock, Josef Haid, Eugen Brenner in [2] propose ESTADO, a system that enables smart services by providing the necessary connectivity from industrial equipment to service providers for device state tracking. Our system design focuses ont he migration of current devices and the security aspect. Using a non-permanent NFC based connection, connectivity is only established ad-hoc on customer demand, and any data transmission is fully transparent to a customer. To enable smart maintenance services fortoday's and future industrial equipment, regular status information must be transmitted from device customers to maintenance service providers over the Internet. Dr. Shyam Thangaraju in [3] proposed the NFC**.** . NFC can be a useful technology for data transfer between two devices in close proximity to one another. This technology is being increasingly adopted for use in wireless transactions, including money transfer, loyalty coupons, transit passes, tickets, etc. Mobile handset manufacturing companies are increasingly integrating NFC hardware in their phones. Not surprisingly, it is gaining traction in the field of medical devices and electronic health records. . This paper looks into the details of this technology, its advantages and disadvantages over existing solutions, and the feasibility of its usability in this highly-regulated area. Michel Abdalla ,David Pointcheval in [4] explained the Password-based encrypted key exchange are protocols that are designed to provide pair of users communicating over an unreliable channel with a secure session key even when the secret key or password shared between two users is drawn from a small set of values. In this paper, we present two simple password-based encrypted key exchange protocols based on that of Bellovin and Merritt. While one protocol is more suitable to scenarios in which the password is shared across several servers, the other enjoys better security properties. Both protocols are as efficient, if not better, as any of the existing encrypted key exchange protocols in the literature, and yet they only require a single random oracle instance. The proof of security for both protocols is in the random oracle model and based on hardness of the computational Diffie-Hellman problem

III. SYSTEM DESIGN

In the system architechture, 5V power supply is required for raspberry pi 3 to power up the device. The GSM Modem is connected in GPIO pins of a raspberry pi 3 which is used to pass the message to the respected user. The camera is connected in the USB port of the raspberry pi 3 which is used for a face recognition purpose. Smart card reader is used as like ATM card. Android app is used to scan the QR-Code. A 16GB SD card contains the raspbian OS which is used to boot the system.

Fig 1.Architechture Diagram

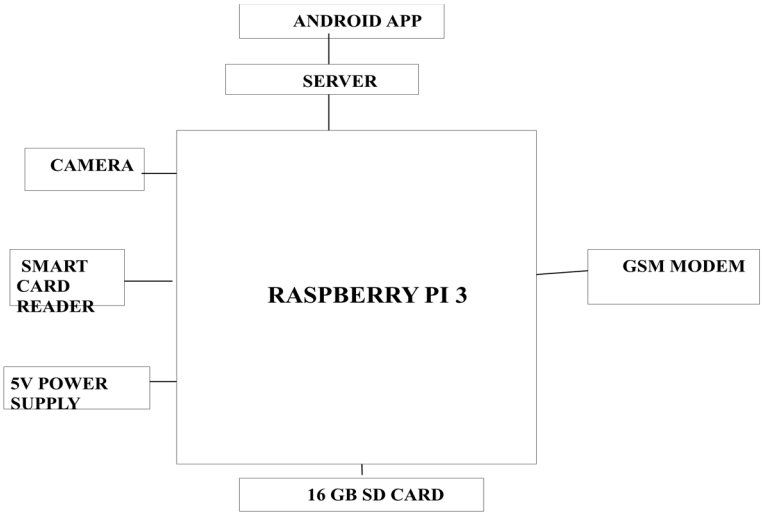


Fig 2.GSM SIM 900

Fig 3.RASPBERRY PI 3

A. Server Module

The server module is the backbone for interfacing the hardware kit with the user mobile application. We develop an http web server in order to communication with the kit and app simultaneously. The web server will be hosted in a public IOT domain. In this module we are going to do graphical user interface development as well as storing our data into a SQL Lite. For this first we have to design a basic web page which is related to our concept. After designing a web page we need to develop user registration form as well as user login form. In registration form we need to add basic user information like username, mail & password etc. After completion of web design we have to design the database to store all user information, to do this we are using SQL Lite database. In user login page we need to enter correct user name and password to login. If user name and password are correct it will goes to the home page, if not it will stays in that page only until we enter correct user name and password.

B. Mobile App Development

Nowadays everyone carry their Smartphone's anywhere. We use the existing available device to provide safety and security from unauthorized use of ATM card or to prevent from shoulder surfing attack. For this we use QR code technology to avoid such misuse. An application will be developed to scan the QR code and app will verify the OTP embedded in the QR code. Once verified a success message will be displayed.

C. Kit Design and integration With Server

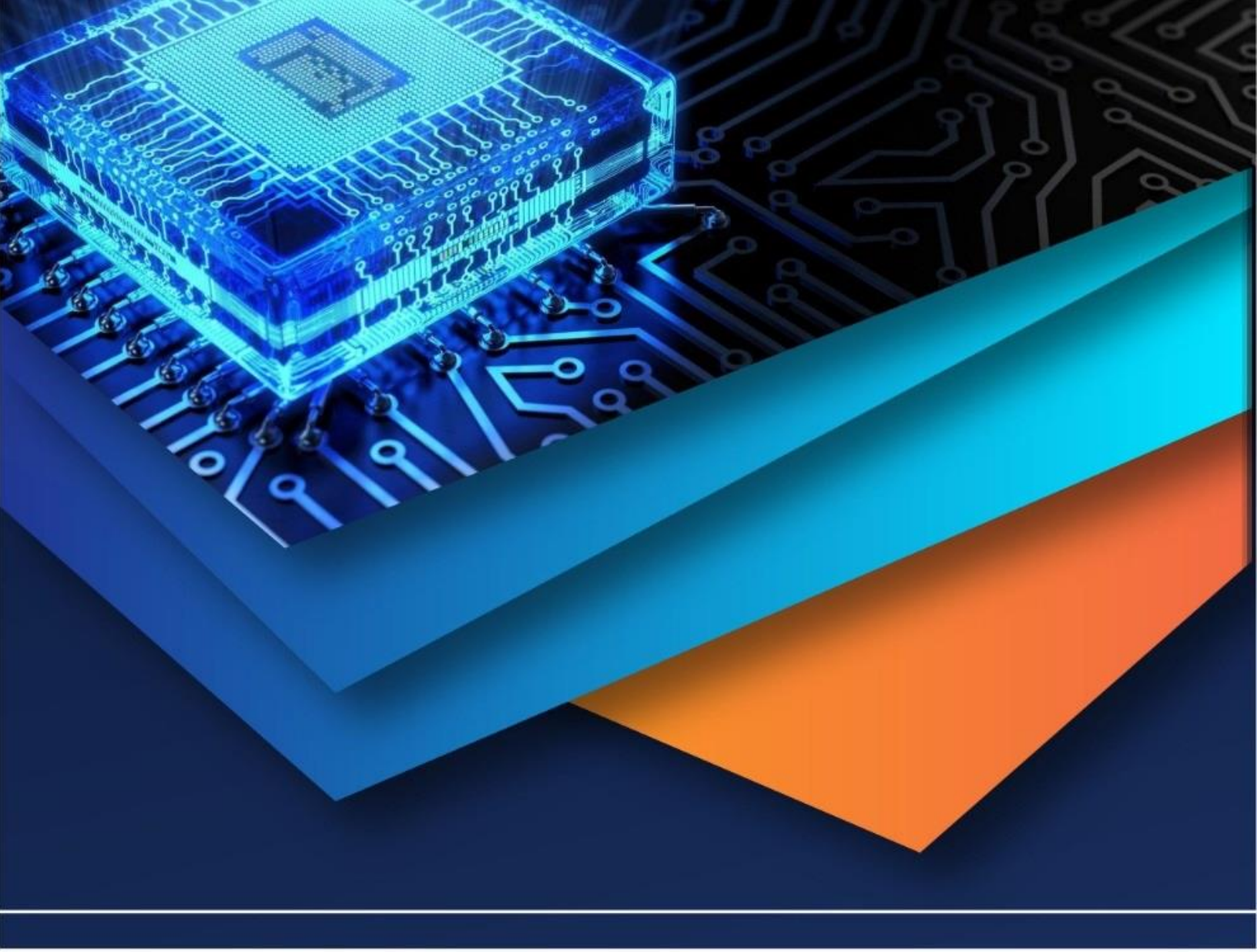
In this module the hardware kit will be integrated with the server end. When the user inserts their Smart Card in the ATM machine (Our hardware), our system will read the ID from the smartcard and captures the user's face. The face recognition algorithm compares the captured face with the registered face for that particular user. Once the user is verified by their Smart Card and Face Recognition, the actual transaction will take place. To complete the transaction, the third level authentication is done. The system will request the server for a unique OTP. The OTP will be converted to a QR Code and displayed in the ATM Screen. The user has to scan the QR code from their mobile app, which in turn sends the scanned code to the server for verification. The server compares the generated OTP and user send OTP. If both OTP matches; the server will authenticate the user.

V. CONCLUSION

By this approach the security of the ATM system has been improved. The customers will identified based on the face recognition system which will avoid forgery and theft taking place in the ATM. This system also allows the customers to access the ATM through special pin number by which customers other than face recorded can also able to access the ATM machine. For the future enhancement we are going to update the drawbacks of the face recognition system. This system can also be implemented in the smart homes and factories. This will improve the security of industries in the future.

REFERENCES

[1] Arjun.K,Kalaiselvan.R,Aruna Jayashree R," Smart ATM Access and Security System using RFID and GSM Technology" on ICEIET,2016.
[2] Christian Lesjak,Thomas Ruprechter,Holger Bock,Josef Haid and Eugen Brenner," Facilitating a Secured Status Data Acquisition from Industrial Equipment via NFC",on Journal of Internet Technology and Secured Transactions (JITST), Volume 3, Issue 3, September 2014
[3] Dr. Shyam Thangaraju," NFC in medical devices", in HCL Engineering and R&D Services practice team ,2013
[4] Michel Abdalla and David Pointcheval," Simple Password based Encrypted Key Exchange Protocol", in A. Menezes, editor, Topics in Cryptology , Vol 3376 , pg 191-208,2005
[5] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC)," in Workshop on RFID security, 2006, pp. 12–14.
[6] D. López-de Ipiña, J. I. Vazquez, and I. Jamardo, "Touch Computing: Simplifying Human to Environment Interaction through NFC Technol- ogy," 1as Jornadas Cient´ıficas sobre RFID, vol. 21, 2007.
[7] G. Van Damme, K. Wouters, and B. Preneel, "Practical Experiences with NFC Security on mobile Phones," Proceedings of the RFIDSec, vol. 9, 2009.
[8] J. Ondrus and Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems," in Management of Mobile Business, 2007. ICMB 2007. International Conference on the. IEEE, 2007.
[9] V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication (NFC) Technology," Wireless personal communications, vol. 71, no. 3, pp. 2259–2294, 2013.
[10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey,"Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[11] V. Sharma, "A Study of Malicious QR Codes," International Journal of Computational Intelligence and Information Security, vol. 3, no. 5, pp. 21–26, 2012.
[12] D. Conde-Lagoa, E. Costa-Montenegro, F. Gonzalez-Castao, and F. Gil- Castieira, "Secure eTickets Based on QR-Codes with User-Encrypted Content," in 2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE), 2010.
[13] T. J. Soon, "QR Code," Synthesis Journal, vol. 2008, pp. 59–78, 2008.
[14] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," in VLSI Design, 2004. Proceedings. 17th International Conference on. IEEE, 2004, pp. 605– 611.
[15] A. Vasudevan, E. Owusu, Z. Zhou, J. Newsome, and J. M. McCune, "Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me?" in International Conference on Trust and Trustworthy Computing. Springer, 2012, pp. 159–178.
[16] M. Sabt, M. Achemlal, and A. Bouabdallah, "The Dual-Execution- Environment Approach: Analysis and Comparative Evaluation," in IFIP International Information Security Conference. Springer, 2015, pp. 557–570.
[17] D. Wu, M. J. Hussain, S. Li, and L. Lu, "R2: Over-the-Air Repro- gramming on Computational RFIDs," in RFID (RFID), 2016 IEEE International Conference on. IEEE, 2016, pp. 1–8.
[18] J. Haase, D. Meyer, M. Eckert, and B. Klauer, "Wireless sensor/actuator device configuration by NFC," in 2016 IEEE International Conference on Industrial Technology (ICIT). IEEE, 2016, pp. 1336–1340.
[19] D. Serfass and K. Yoshigoe, "Wireless Sensor Networks Using Android Virtual Devices and Near Field Communication Peer-To-Peer Emula- tion," in Southeastcon, 2012 Proceedings of IEEE. IEEE, 2012, pp. 1–6.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY