ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

NFC Based Access Control System Using Image Hiding

Prof. L.J. Sankpal[1], Sachin Mundhe[2], Manoj Kotwal[3], Pratik Machale[4], Shubham Malshikare[5]

Assistant Professor, Dept. of Computer, Sinhgad Academy of Engg, Pune University, India[1]

BE Student, Dept. of Computer, Sinhgad Academy of Engg, Pune University, India[2,3,4,5]

ABSTRACT:Near-field communication (NFC) is a set of communication protocols that enable two electronic devices to connect and one of which is usually a portable device such as a smartphone. An Access control system is simply defined as any technique used to control passage in or out of any area or any premise, such as residential areas, offices and others. It serves as a prevention technique to reduce the number of building break-in's and provides a safer alternative in security systems. A Conventional access control system allows users to access a premise using an access card. It has been introduced as an alternative system to the most common access control system using physical keys and mechanical locks to increase the level of convenience to access a premise. However, in conventional Security systems an intruder is able to gain access to the premise if they possess the access card or the physical keys.Proposed system utilizes Near-field communication (NFC) smartphone and information hiding technique.

I. INTRODUCTION

Near Field Communication (NFC) is a standards-based, wireless communication model that allows NFC enabled devices to establish communication by simply coming into close proximity with each other. NFC devices can be used in arbitrary applications. Current applications for NFC include contactless transactions in retail, and ticketing systems, data exchange, and simplified setups for more complex communications such as Bluetooth and Wi-Fi.

Nowadays, the number of building break-in cases are increased and it has been a major problem in recent years. An Access control system can be used to reduce the number of building break-ins and it also provides a safer alternative in security systems. An Access control system is simply defined as a technique used to control access in or out of any area or any premise, such as residential areas or offices.

The evolution of Science and Technology creates a new generation of the access control systems, known as digital access control system. A digital access control system allows users to access a premise using an access card. It is introduced as an alternative system to the most common access control system using keys and conventional locks to increase the level of convenience to access a premise. However, an intruder is able to gain access to the premise if they possess the access card or the physical keys. Hence, in proposed access control system it utilizes near field communication (NFC) smartphone and information hiding technique to overcome the disadvantages mentioned on the existing systems. The first protection level is NFC smartphone and NFC reader or tag to initiate the access control to the premise. In the second level steganography technique is used to embed access pass-code into the user's photo to obtain an encoded photo, which is also known as stego-photo. The access pass-code in the stego-photo is later extracted using information hiding technique during the door access stage for verification of the authorized user. An automated door is developed and NFC reader or tag is located near the door. The interaction between NFC smartphone and NFC reader or tag enables prompting of the correct stego-photo to be selected using the smartphone to perform the user authentication process. The door is unlocked if the access pass-code extracted from the stego-photo matches with the access pass-code.

II. LITERATURE REVIEW

The evolution in science and technology has created a new generation of the access control system known as a digital access control system. Users gain access to the premise by just entering numeric password on the keypad. Thus, the level of convenience increases tremendously as compared with the system that utilizes physical keys as users do not

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

need to carry larger and heavier bunch of keys around. However, this system possesses weakness in the security perspective. AA Hossain et al. mentioned in [1] about potential drawback of using keypad system is that it is more susceptible to shoulder surfing attack. In shoulder surfing attack, a spy from a distance might observeor record the overall process of the user keying the numeric password.

In [10] biometric access control system uses physical part of the user, such as fingerprint and iris as a method of authentication. The biometric systems basically implement the same working principle where unique user's thumb (or user's eye) is utilized to identify and verify the correct user in the fingerprint (or iris) access control system. For example, an authorized user has his fingerprint (or eye) physically scanned to the fingerprint reader (or iris's camera). In [4], The physical characteristic of his fingerprint (or eye) has to be recognized by the reader (or iris's camera) before access is granted. There is a high possibility that the fingerprint reader does not recognize the user if there is a scar on the user's finger. Besides that, dirt on the fingerprint reader or iris's camera may cause the systems to be malfunctioned.

Sufian Hameed, in [3], The advance of NFC technology has also increased the threats like security vulnerabilities. NFC alone does not ensure secure communications. Due to lack of security, attackers can easily use the NFC technology for proximity hijacking attacks and eavesdropping. With gaining unauthorized access, an attacker can listen into NFC transactions and access victim's credentials such as his financial and personal information. It can be used against him with malicious intent.

Many NFC based applications are potentially vulnerable to different types of attacks without proper protection and normal user will not be able to differentiate malicious/forged tags from genuine tags [2]. In [7], Haselsteiner et al. highlights different threats like instance eavesdropping, data corruption, man-in the middle attack, data insertion and data modification, which can compromise NFC interactions. Collin Mulliner [8] was among the first researchers who analysed a number of previously unknown types of attacks. These vulnerabilities can easily be exploited by attacker to spoof the tag content. After that Milliner [7] published the tag spoofing attack, the NFC-Forum issued a specification of Signature Record Type Definition (SRTD). The specification adds digital signatures to provide authenticity and integrity to the NFC Data Exchange Format (NDEF) messages [9].

In [6] steganography a pass-code is hidden in an image. According to the technique, an image is stored in a memory which can be encrypted using different encryption algorithms like AES, ECC and SHA etc. Encrypting message contains flow of bytes which is converted in form of bits, so that insert it in color pattern of pixel. A byte of encrypted message will carry eight bits which is divided into 12 possible sequence of bits.

III. OBJECTIVE

A. EXISTING SYSTEMS

A.1. LEGAL ENTRIES USING PHYSICAL KEYS AND MECHANICAL LOCK

Mostly used type of access control system utilizes metallic keys and locks. In this system, physical are used by users to simply lock or unlock the door with a physical key.

A.2. ACCESS CONTROL SYSTEM USING DIGITAL KEYPAD

The recent progress in science and technology has been used to develop a new generation of the access control system known as a digital access control system. Users gain access by just entering numeric password on the keypad.

A.3. ACCESS CONTROL SYSTEM USING DIGITAL KEYPAD

Biometric access control system utilizes physical part of the user, such as fingerprint and iris as a method of authentication. The biometric systems basically work on the principle where unique fingerprint is utilized to identify and verify the correct user in the fingerprint access control system [10].

B. PROPOSED SYSTEM

In proposed system the first protection level is NFC smartphone and NFC reader or tag to initiate the access control to the premise. The second protection level is the information hiding technique to embed access passcode into the user's photo to obtain an encoded photo, which is also known as stego-photo. The extracted access passcode is then compared with the access passcode that is stored in the server previously. The door will only be unlocked if both access passcode is matched. Otherwise, the door is re-locked. In order to gain access to the house, user can re-scan his phone to the reader or tag and re-select the correct

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

stego-photo to the reader or tag and re-select the correct stego-photo for the whole decoding and verification process is repeated.

IV. ARCHITECTURE

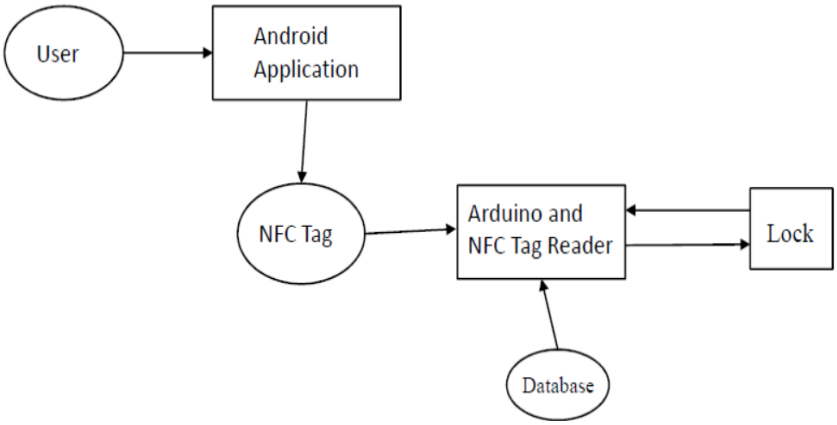

Fig.: Architecture

This system that utilizes near field communication (NFC) smartphone and information hiding technique to overcome the disadvantage mentioned previously on the existing systems.
The system consists of following multiple modules:

1. NFC reader (connected to controller)
2. Arduino
3. Smartphone application which emulates NFC cards

The main working of the system is divided into two phases

A. Registration Phase:

- User will have number of images to select and to stenograph their entered password.
- Image will be steganographed with entered password (encrypted) and get replaced by original image.
- User will have to enter correct password at the time of unlocking door and by selecting registered image.
- Selected image will be decrypted and registered password (decrypted) will be compared with entered password.

B. Door lock/unlock Phase:

- The device must be brought into closer proximity.
- Registered user will enter his password and select one image which they selected while registering.
- Keys will be matched and if match found NFC tag write screen will be opened.
- By pressing write button unlock code will be written on tag and will be checked with NFC reader kit at the door.
- Reset button is available to reset unlock codes on tag.

V. ADVANTAGES

1. It will benefit the many organization as they will get more secured.
2. It will reduce the risks of intrusion and unauthorized access.
3. This system introduced as a trade off balance between security and convenience.
4. NFC modules can be integrated on one chip device resulting in saving space on the device which can be utilized for other necessary functions and still keeping the size of the gadget small and handy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

VI. CONCLUSION

In this application we conclude an access control system based on the concept of two-factor authentication. The proposed system utilizes NFC smartphone (i.e. something that the user has) and stego-photo (i.e. something that the user knows) to overcome the disadvantage exhibited by the access control system using the access card. This is true as a secure system typically is a complex system and requires complex algorithms which will eventually sacrifice the convenience. An insecure system, on the other hand, performs simple algorithm, thus convenience is dominant.

VII. FUTURE SCOPE

The system is essential for today's generation as what type of security measures they should take to make their life more secure to outside world. A list of mobile phone which have NFC readers can be obtained from internet and many more phones will be launched soon.

All the locking system will be replaced by personalized NFC enabled devices and NFC tags as door locks. Thus NFC can be used as step towards the world of automatic devices. Even for the basic needs there will be the need for an NFC-enabled device like for subscribing for personal offers that will be made available to unique smart phone users. The switches for using domestic appliances like tube lights, fans etc. will be replaced by remote controls that further can be operated using NFC-enabled devices used as Home Automation appliances. Also a record can be maintained by the user in their smart phones of the usage of these appliances.

REFERENCES

1. AA Hussein, and AA Mohammad, "Near Field Communication (NFC)," International Journal of Computer Science and Network Security, vol. 12(2), pp. 93-100, Feb. 2012.
2. J. Christian, J. Scharinger, and Gerald, "NFC Devices: Security and Privacy," in Proc. of the 2008 Third International Conference on Availability, Reliability and Security, pp. 642-647, 2008.
3. Sufian Hameed, Usman Murad Jamali and Adnan Samad, "Protecting NFC Data Exchange against Eavesdropping with Encryption Record Type Definition," IEEE/IFIP Network Operations and Management Symposium (NOMS 2016): Mini-Conference,2016.
4. A Kumar, and K. M. Pooja, "Steganography-A Data hiding Technique, "International Journal of Computer Applications, vol. 9, pp. 1-5, Nov.2010.
5. V. K. Sharma, and V. Srivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection," Journal of Theoretical and Applied Information Technology, vol. 36(1), pp. 1-8, Feb. 2012.
6. S. Narayana, and G. Prasad, 'Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions," International Journal of Signal and Image Processing, vol. 1(2), pp. 60-73, Dec. 2010.
7. Sebastian Dunnebeil, Felix Kobler, Philip Koene, Jan Marco Leimeister, and Helmut Krcmar," Encrypted nfc emergency tags based on the german telematics infrastructure." In Proceedings of the 2011 ThirdInternational Workshop on Near Field Communication, NFC '11, pages 50–55, Washington, DC, USA, 2011. IEEE Computer Society.
8. Collin Mulliner. Vulnerability analysis and attacks on nfc-enabled mobile phones. In ARES, pages 695–700, 2009.
9. NFC data exchange format (ndef), nfc forum technical specification, rev. 1.0, Jul. 2006. http://www.nfc-forum.org/specs/spec list/.
10. M. Lourde, and D. Khosla, "Fingerprint Identification in Biometric Security Systems," International Journal of Computer and Electrical Engineering, pp. 852-853, Oct. 2010.