NFC BASED ACCESS CONTROL SYSTEM USING IMAGE HIDING

AKSHAY KUMAR SINGH (akshaysingh2621995@gmail.com), NISHANT MANGRULKAR (nishantmangrulkar@gmail.com), SOURABH OSTWAL (sourabhoats@gmail.com), PRATIK SHUBHAM (Pratiksh2011@gmail.com)

Sinhgad Institute of Technology, Lonavala

ABSTRACT

In the elds of data security, access control is most important in avoiding unauthorized Access in premises. Digital Security access control systems are designed to avoid unauthorized entry. It will control one door in a single room or many arrivals in an entire building. An intruder is able to gain access to the premise if he possesses the access card or the physical keys. Instead of carrying all sort of keys(house key, garage key, car key, o ce keys), in addition to this people also carry smart phones which can be used for accessing. Today almost all phones are NFC supported. We propose an access control system that utilizes near eld communication (NFC) device information hiding technique using steganography which can be used to access instead of carrying bunch of keys.

I. INTRODUCTION

Nowadays, there are many number of house breaks which are increasing everyday. Person needs to carry a bunch of keys with him in order to secure his premise. These bunch of keys includes house keys, o ce keys, garage keys, car keys etc. this bunch of keys may act as burden for the user.

In todays date Science and technology is getting evolved rapidly. This made possible to use a smart phone which have several features which may help in secured access like Bluetooth, NFC, WiFi infrared etc. These all are wireless technologies which can be used for transmitting data from one device to another. Bluetooth technology operates over unlicensed, which is available at 2.4Ghz frequency, also can link one digital device to another within a range of 10m to 100m at the peak speed of 3mbps, but it depends upon the device class. Bluetooth and WiFi are di erent from NFC. NFC working is dependent on electro-magnetic eld which helps in faster transmission and short ranged.

For secured system access cards [1] can be used which works on NFC. This access card contains password hidden it. User needs to hold this access card near to NFC reader which is embedded on doors. NFC reader then reads the passcode from access card and user gains access. This has a drawback, in todays modern world people have many cards and to handle such cards is a challenging task. If the card is lost then any person in contact with the card may get access to premise illegaly. In this paper we propose a [2] two factor authentication access control system based on NFC enabled mobile device. User only needs to carry a single phone instead of carrying whole bunch of keys. In this system when needed access user simply needs to hold his phone near to NFC reader. NFC reader then reads the password and user gains access.

Password can be stored more secured by hiding it under image by the process of stegnography.

Stegnography is a process in which user can hide any textual informa-tion under any multimedia like image, audio, video etc. In order to realize NFC door lock user needs to achieve these goals

1] Connect Arduino board to the network.
2] Con gure the NFC reader according to user.
3] Embed NFC reader to Arduino board.
4] Save authenticating users.
5] connect sensors.

In the next section [II] we provide background about the system. Sec-tion [III] describes the proposed system. Section [IV] describes the conclusion and future works.

II. LITERATURE SURVEY

The evolution of science and technology creates 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 need to carry larger and heavier bunch of keys around. However, this system possesses weakness in the security perspective. A potential drawback of using keypad system is that it is more susceptible to shoulder sur ng attack. In shoulder sur ng attack, a spy from a distance might observe or record the overall process of the user keying the numeric password.

In biometric access control system uses physical part of the user, such as ngerprint 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 ngerprint (or iris) access control system. For example, an authorized user has his ngerprint (or eye) physically scanned to the ngerprint reader (or iris's camera). The physical characteristic of his ngerprint (or eye) has to be recognized by the reader (or iris's camera) before access is granted. There is a high possibility that the ngerprint reader does not recognize the user if there is a scar on the user's nger. Besides that, dirt on the ngerprint reader or iris's camera may cause the systems to be malfunctioned.

In proposed system the rst 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 are 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 stego-photo to the reader or tag and re-select the correct stego-photo for the whole decoding and veri cation process is repeated.

There were some research done in previous on authorized access control. Authors of [1] used smart accesss cards to gain access. These smart cards had passwords in it which were not able to be seen by direct eyes. In there proposed system user needs to hold the card near to NFC reader which is then read by NFC and access is granted. If the user is not authorized then no access is given. This had a drawback, if the card is lost by the user then
any person whonds it may gain illegal access to the premise.

The researchers of [3] proposed a security model where user needs to register his iris to the system. Iris is unique body part of every human. No two human can have same iris. This was a high level system where iris is recognized by person an access is gained only to authorized individual. There was disadvantage of using this, if user receives any damage to his eye then system won't recognize him.

Another concept used by the authors was [4] face recognition. Facial metrics rely on features such as eyes, nose, mouths and distance between features. The scanner completely scans all the features and store it. If any change occurs such as wearing optical glasses or change in hair or beard, then the scanner again needs to register.

The author of [5] used ngerprint identi cation for security. Fingerprint is an impression of all the ridges on the nger which are connected by many other ridges. These ridges are the most important part in scanning. These are scanned by sensors such as Ultrasonic User places his nger on the reader and sensor scans all ridges on it in order to get perfect impression. But any kind of injury like burned nger may lead to improper ridges which may not be accepted by the scanner.

In our proposed system out of two factors rst is NFC enabled device which is always present with user and another factor is password hidden under image. Stegnography is a method by which user can hide any text under any multimedia like image, audio, video etc. the user simply needs to hold mobile device near NFC reader, reader then reads the password if the user is authorized then access is granted or if the user is not authorized then access is not gained.

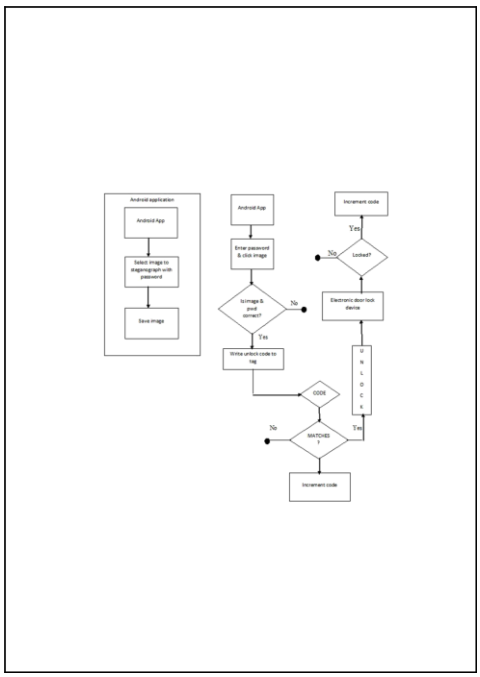

Fig: Architecture Diagram

III.WORKFLOW

In the Proposed System the Computer acts as a registration server where all the users availing this facility needs to register here. On successful registration the Server generates a unique passocde and encodes the password inthe user photo. The newly created photo which called as a stego photo is downloaded on the users smart phone/device.

The very rst step to do is to register the mobile phone to server.

After registering the user is then provided with a password.

The user then needs to select an image which is unpredictable. Unpredictable image and password helps user secure his premise.

The third step is to hide the password into image.

Stegnography is a method in which any data can be hidden under image. This data can be audio, video, text or any kind of Multimedia.

User then gets a stego-image.

When the user needs to enter the premise he is supposed to hold if mobile phone nea to the NFC reader, NFC reader then compares the password saved in image to the password saved in its server. Here there are two possibilities, the password may match or the password may not match.

If the password in the image does not match with the one password saved in server then user needs to register to the server to gain access.

If the password is correct then NFC screen is open with unlock tag written on it. The door is unlocked.

IV. ADVANTAGE AND DISADVANTAGE

Advantage

This system introduced as a trade of balance between security and convineince as user don't have to carry bunch of keys and it also provide high security.

Easy to use, user simply needs to hold device near to NFC reader.

Easy to learn and setup

Secure communication between NFC reader and NFC enabled device.

Disadvantage

NFC operating range is very less as compared to Bluetooth and Wi which is only 10cms.

Data transfer rate is very less as compared to Bluetooth and Wi as it works on electromagnetic eld.

This technology is very expensive as compared to other security techniques.

V. APPLICATIONS

Service initiation:-In this scenario functioning of NFC is the same as that of RFID. NFC device reads some data from NFC tag and uses the same information in several di erent ways. In this case tag serves as transmitter. NFC device can read the data even if the cell phone is powered o . Example of such scenario can be the advertisement or information poster.

Peer-to-Peer:- In this application, a direct link is formed between two devicesto transfer the data. Amount of data should not be too large. If user wants to transfer large amount of data, Wi-Fi or Bluetooth connection can be set up, but that is invisible to user.

VI. CONCLUSION AND FUTURE SCOPE

In this paper we have proposed an access control system based on two factor authentication. The proposed system utilizes NFC enabled mobile device and stego image(an image which has information hidden in it). This sytem is secured and convenient. This system is high in demand and is present everywhere. By reducing the number of keys and cards people needs to carry single smartphone in order to gain access. If the device is lost no need to remove o disable the device user can delete the device from the network. This system can help blind people and old people to unlock doors easily. Tags can be shared within family members to gain access In future this access system can be replaced by NFC rings which can also be used to unlock door and as well as unlock mobile devices and other smart phones.

VII. REFERENCES

[1] Philip S Lee \Smart card access control system" US 5204663 A

[2] F. Aloul, S. Zahidi, and W. El-Hajj, "Two Factor Authentication Using Mobile Phones," in IEEE/ACS International Conference on Computer

Systems and Applications, vol. 6, pp. 641-644, May 2009.

[3] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric Authentication: A Review," International Journal of Science and

Technology, pp. 13-16, Sept. 2009.

[4] B. Kar, B. Kartik and P. K. Dutta, "Speech and Face Biometric for Person Authentication," 2006 IEEE International Conference on Industrial Technology, Mumbai, 2006, pp. 391-396. doi: 10.1109/ICIT.2006.372389

[5] FINGERPRINT IDENTIFICATION USING GRAPH MATCHING*

D.K.ISENOR and S.G. ZAKYt Department of Electrical Engineering,University of Toronto Toronto,Ontario, Canada, M5S IA4