EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 7/ October 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

NFC Based Access Control System

A. T. GHORUDE
G. S. PATIL
A. S. CHAVAN
S. S. BORSE
Dept. of Computer Science
Sandip Institute of Engineering & Management
Nasik (M.S), India

Abstract:

The security concerns are increasing day by day and so as to provide a reliable security for any organization we have implemented three levels authentication using the NFC. The first level is the username and password, second is mobile authentication using NFC reader that will fetch the IMEI number from mobile. The last phase is the face authentication. Hence by ongoing these phase, the valid user can be identified and access right can be given to him/her.

Key words: NFC, mobile authentication, IMEI, Face authentication.

Introduction:

NFC is a new, short range, high frequency, low bandwidth, and wireless communication technology. NFC communication is activated by touching two NFC enabled devices together, or bringing them into close range. The range is usually few centimeters, and it operates at the frequency of 13.56 MHz. The maximum data transfer rate is 424kbit/s. NFC is based on Radio frequency Identification (RFID) thus its communication involves initiator and a target, the initiator actively generates a

Radio Frequency (RF) field that can be used as a signal to power a passive target. The initiator (active) has its own internal power that can be used to power the ICs that generate the outgoing signal; while the target (passive) has only ICs with no internal power, which makes it to be in different forms like tags, stickers or cards. [Anugerah Ayu, 2014].

The currently existing system for that provides security for access rights includes the 1. Biometric system 2. NFC based access control system using information hiding etc. 3. Software Card Emulation in NFC-enabled Mobile Phones. *Biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode. [Anil K. Jain, 2004].

In biometric system, once the figure prints are obtained, and then validation is done. But if the figure prints are obtained by wrong ways then this system can be misused. Also in the second method each user has their stego photo, where a code is encrypted in that photo. When that photo is tapped near NFC reader, it extracts the code and then verifies the user by using the principle of encryption and decryption. But if invalid person get to know your photo then there are chances of misuse. So we are modifying this system and instead of stego photo we can have use live face recognition system, as no one can steal you face identify. So there is no chance of misuse.

In the third system of using cards, there are many risks associated with this. It becomes difficult for card emulation Applications to store sensitive data (e.g. credentials for access control systems, private signing keys for payment solutions, tickets...) Moreover, the lack of a trusted execution environment could allow for (intentional) interference by other applications. For instance, recent vulnerabilities of the Google Wallet allowed an attacker to recover credit card numbers, account

balance, card holder information and even the wallet's PIN code, because, even though Google Wallet has access to a secure element, this data was cached within the app's private data storage in the mobile phone memory. [Michael Roland, 2012]

Now, the user comes near the office where our system is enabled. The user needs to run the android application and that application will ask the user name and password to the user and when user enters it that will be sent to server for verification. After first phase is completed successfully then the mobile authentication is done, in this the user has to tap his/her mobile to NFC reader, then NFC reader fetches the IMEI number for verification. The data fetched by reader is sent to server by Wi-Fi system.

If the second phase is correctly verified then only the next phase can be executed and the camera in the mobile is automatically switched on. The user needs to click the live image in frontal position and then that image will be sent to the server's PC for further processing. The three levels of authentications can be used at very important organization like CBI, forensic department, research centers where only the VIP peoples are allowed to enter.

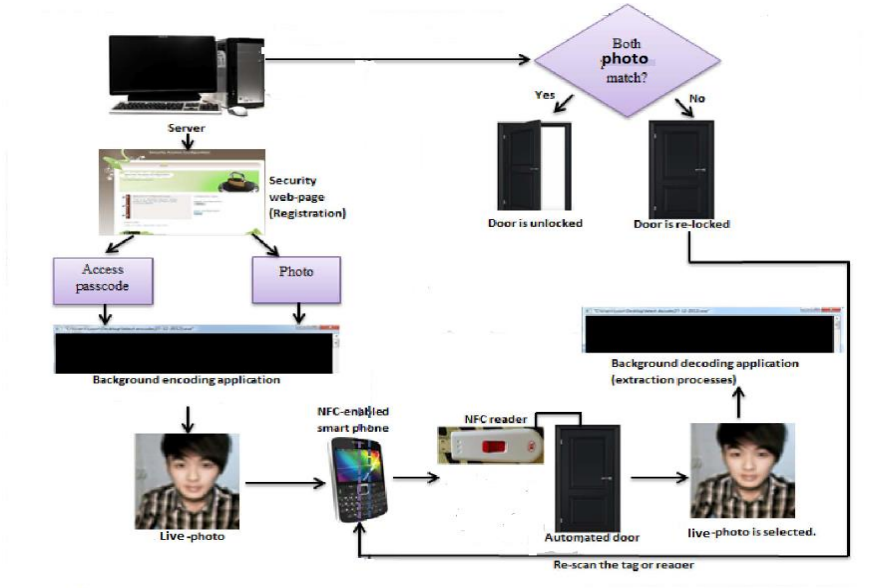
Material and Methods:

While implementing this system, we are keeping a track of all the users. We need to maintain the database, where each new user needs to do the registration. At the first time of registration we need to assign a unique username and password to each user, also collect their IMEI number and some face samples and in our database. The verification at first two levels is done by comparing with the database that is stored at server side.

For identification in the third level which is face recognition, we are using the three algorithms:

1. Color features extraction using average RGB values algorithm.
2. Texture co-occurrence algorithm.
3. Geometric shape algorithm.

The image is nothing but collection of pixels. The average RGB value is computed so that pixel by pixel matching is done. Greater the matching criteria higher will be the efficiency. Along with this we need to compute the outline of face for matching purpose. So this is the required material and method.



System algorithm:

1. Color features extraction using average RGB values algorithm:

As we know that the image is nothing but collection of pixels. Here each pixel has some value that is nothing but color values. So average RGB values of each pixel is calculated and matched with the current image to the sample image that is stored in the database. We can fix the criteria of matching percentage. This is an important part as suppose if the user gets in scratch

or pimple on the face that can be ignored so we need to keep the matching percentage less than 100.

2. Geometric shape:

In this algorithm, the shape of face is computed. Here if the outline of the face matches then we can go for further processing. If the outline of face itself doesn't match for a person it clearly indicates that he or she is invalid user. So implementing this algorithm first reduces the further calculations for invalid persons.

Mathematical Model:

As we know that user is expected to capture the image in frontal position that is 2D image but if suppose the person lifts or nods their face that comes out to be the 3D image and hence we must be able to resolve such cases. So the angle of rotation and lifting can be given by,

$$\theta = \arcsin(h/r)$$

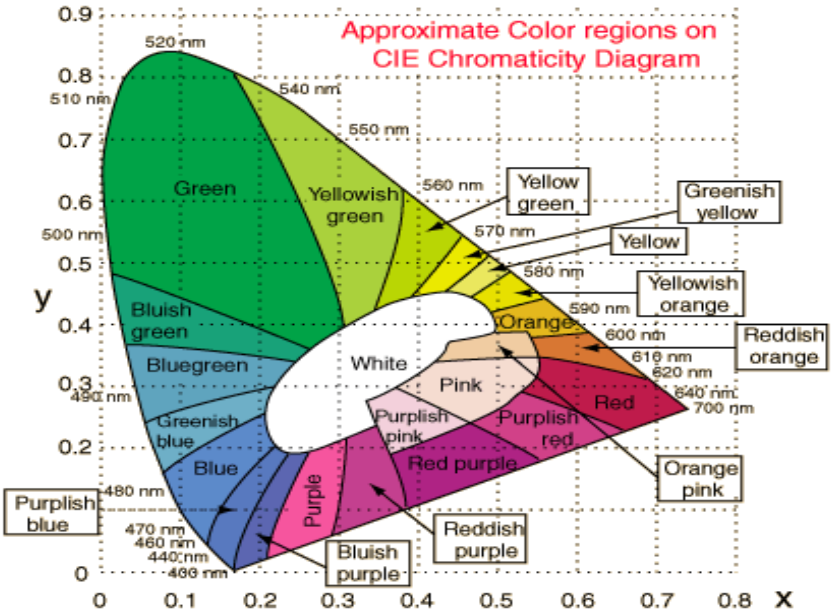
Where, (h/r) is the height and depth difference between eyes and ears.
Now, we need to convert the 3D images to the 2D image and hence this can be done by computing the linear transformation matrix that is given by,

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_v \\ y_v \\ z_v \end{bmatrix}$$

Where, x, y, z are the co ordinates points of 2D image, x_V, y_V, z_V are the co ordinates points of 3D image, After the conversion process the co ordinate show the equality relation between x and y that is $x=x_V$ and $y=y_V$. Z co-ordinate is not considered as 2D image deals with only x and y co-ordinates.

Also x, y, z and x_V, y_V, z_V co-ordinate points have some value that is color value.

This value can be given by tongue shape chromaticity diagram given below,



Here, RGB value are calculated by following formula,

$$X = \sum_{380}^{780} R(\lambda)E(\lambda)\bar{x}d\lambda$$

$$Y = \sum_{380}^{780} R(\lambda)E(\lambda)\bar{y}d\lambda$$

$$Z = \sum_{380}^{780} R(\lambda)E(\lambda)\bar{z}d\lambda$$

Where, $E(\lambda)$ = light source distribution
$R(\lambda)$ =surface reflectance

Non functional requirement:

Performance requirement:
Here the time required for processing is as least as possible to give the quick identification also only one valid person should be given access as this is the basic function that should be satisfied.

Safety requirement:
Here our system contains the database that should be ensured with appropriate safety so as to avoid the misuse by hackers or other people. We can enable our server PC with the firewall system so that we can check each incoming and outgoing files. This works on the mechanism of good bits in and bad bits out.

Ease in use:

NFC is a powerful means, a highly stable wireless connectivity technology that provides intuitively simple and safe two-way interactions between electronic devices. It has the impending potential to make almost all wireless technologies easy enough so that everyone and even the non-technical persons can use them. [K.Preethi, 2012]

The most secure NFC-based applications target Nokia smart phones, most probably since NFC-enabled Nokia smart phones are already available for some time and equipped with secure hardware. [Alexandra Dmitrienko]

Result and Discussion:

We have used the three levels authentication system for granting the access rights. Even if the invalid person gets to

know username and password along with IMEI number still they have not passed through the third level of authentication. So we can not only restrict the intruder but also avoid the misuse of our system.

The time required for this system depends on the user. If the input is given in the required way the processing can be done efficiently. The time required for entering the IMEI number manually is more. So we are using the NFC system for mobile authentication. If the image sample of face is clicked in the frontal position (2 D) then time required is less for processing but if the user lefts or nods their face with an angle then a 3D image is formed. So the conversion of 3D image to 2D image needs to be done first and then further processing is done.

If this system is used for more number of people then the high quality resolution camera should be used to maintain the clarity. If the quality of camera is high then there will be ease in the process of face identification. The user also needs to adjust the light while clicking their own image.

Conclusion

Thus we can implement NFC based access control system for better reliability of access right. If this system is used for more number of people then the high quality resolution camera should be used to maintain the clarity. If the quality of camera is high then there will be ease in the process of face identification. The user also needs to adjust the light while clicking their own image. We are using NFC that uses less time to fetch the data so the processing requires less time. We just need to maintain our database by the people working in the organization. If the user buys a new mobile then such updates can be made in our database so there is ease in handling this system. By using this system we can restrict the fake users

and allow the only valid users. The system is very useful and can be implemented for many organizations.

REFERENCES:

1. NFC Smartphone Based Access Control System Using Information Hiding, 2013 IEEE Conference on Open Systems (ICOS), December 2 - 4, 2013, Sarawak, Malaysia.
2. Android-Based Mobile Payment Service Protected by 3-Factor Authentication and Virtual Private Ad Hoc Networking, 978-1-4577-1719-2/12/$26.00 ©2012 IEEE.
3. Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare? Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU) June 18, 2012, Newcastle, UK
4. TouchIn: An NFC Supported Attendance System in a University Environment. *International Journal of Information and Education Technology, Vol. 4, No. 5, October 2014* \
5. SmartTokens: Delegable Access Control with NFC-enabled Smartphones alexandra.dmitrienko@trust.cased.de
6. An Introduction to Biometric Recognition. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004
7. Contactless Communication through Near Field Communication. International Journal of Advanced Research in Computer Science and Software Engineering
8. Research Paper Available online at: www.ijarcsse.com