International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-10, Issue-4, July 2022
https://doi.org/10.55524/ijircst.2022.10.4.25
Article ID IRPV1043, Pages 208-212
www.ijircst.org

Iris Recognition Based Data Security for Secure Transmission Over Internet of Things Network

Alkubra Nusaiba Hassan[1], and Dr. R. P. Singh[2]

[1]M.Tech Scholar, Electronics and Communication Engineering, RIMT University, Punjab, India,
[2]Assistant Professor, Electronics and Communication Engineering, RIMT University, Punjab, India,

ABSTRACT-The biometric traits of any human being such as fingerprint, tongue prints, face recognition, Retina Scan, Iris recognition etc. are unique and cannot be replicated or fabricated using modern technologically advanced processes. These unique traits are used to identify individuals for grating access to sensitive data over the cloud. In this paper we propose a biometric authentication system based on Iris recognition to allow user identity based data to be pushed on to the cloud for global access, if the user Iris image is authenticated with the database. The real time Iris scanner captures the Iris image and same is imported to the MATLAB workspace for feature extraction and matching. Upon successful matching, the data is transmitted to the ThingSpeak Internet of Things (IoT) analytics platform. The IoT framework is a massive network of physical devices sharing data according to set protocols. Most of the IoT enabled devices lack security protocols. Thus, biometric authentication in general and iris recognition in particular finds a perfect fit for securing data over an IoT framework.

KEYWORDS- Iris recognition, Data Security, Internet of Things Security, IoT Security Framework, ThingSpeak IoT Platform, Secure Transmission.

I. INTRODUCTION

Internet of things (IoT) is a system or interconnection of interrelated devices and sensors connected to the internet to transfer and receive data from one device to the other. The IoT is a massive global network that allows people to communicate with each other. The term "thing" in internet of things refers to any object that has a sensor attached to it and which is computationally enough mature to transmit data from its sensor into the cloud. The data in the cloud is analyzed and used to make decisions. Internet is the backbone of the digital revolution and the number of the network connected devices is increasing unprecedentedly. The number of internet enabled devices is assumed to reach around 75 billion by 2025. Nowadays, Internet of Things (IoT) presents high number of openings for customers and big business in many applications. In IoT applications, engineers and developers experience many experimental challenges, problems to use IoT applications securely, and safe sufficiently [1]. Users of IoT technology like customers, government offices and technical organizations, lack secure and safe IoT systems for their overall operations over internet. Security in connections between IoT clients and data servers are critical to any IoT framework [2]–[4], and this forms the basis of defense against computer hackers and data corruptions [5]. The best technique to protect sensitive data from such security oriented weaknesses is to use biometric authentication technologies such as Iris recognition for IoT authentication as card or token method [6]–[11]. Biometric traits of a particular human being are unique and do not match with any other human on the planet earth. Biometric-based authentication in security systems empowers many applications economically. The IoT is used nowadays in more critical environments like airports, border controls, defense security, access control systems in corporate offices, education research institutions etc. these frameworks require more secure connections with the rest of the world over internet to avoid intersection of critical information. These organizations require extraordinary security controls for authentication and authorization. For authentication and authorization realms, Uni-modal recognition systems face many problems such as those listed in [12]. These mentioned snags will lead to higher Equal Error rate (EER). Biometric authentications are Uni-modal or multi-modal. Multi- modal biometrics has the advantage on some addressed issues in comparison to the Uni-modal recognition as listed in work [13]. However, it is not fit for scenarios and is limited to some applications only. Moreover, multi modal biometrics is more expensive, requires more hardware components and running complex software algorithms for classification.

II. RELATED WORK

A few researchers have performed studies in IOT security fields using biometrics to authenticate users on generic IOT networks. In [14], Iris recognition based biometric authentication system is used for IoT but as a preceding step prior to IoT communication protocol. In a secure IoT communication link between clients and broker server based on Iris recognition technique (Authentication Server) was projected. The Iris recognition system talks with Message Queuing Telemetry Transport (MQTT) broker server running on a Beagle-Bone Black to improve the user authentication instead of using normal text method (username/password) method of authentication. In addition to the above mentioned surveys [15] introduces

and analyzes various biometric based authentication techniques, which might help researchers to focus on the security domain in IOT and develop solutions for IoT forensic investigation frameworks.

The author in [16] gives an impression of the biometric authentication based methods for use in the internet of things domain. That communicates between several computing edge devices embedded in the daily appliances to the internet, and it can permit the IoT gadgets to communicate with each other, advances the end user's quality of life, and increases competence and sustainability from routine activities. Thus, some more opportunities [17] are planned for the coming years to escalate the number of end users and devices involved in IOT. The assimilation of IOT with biometric authentication traits will improve security systems in different subfields and make them more robust and authentic and free from intersection of hackers.

III. PROPOSED WORK

In this section we present the proposed technique for an iris recognition based security system, accompanying the transmission of sensitive corporate data over an IoT framework as shown in figure 1. The proposed scheme involves a series of steps: starting from the Iris image acquisition using an Iris scanner to feature extraction using various filter techniques, such as Gaussian filter, canny filter, Sobel filter etc. After the feature extraction is done, the feature matching takes with stored images in the database. If there is a perfect match the identity based data will be allowed to transmit over the IoT framework. If the match is not perfect, the data will not be allowed to transmit over the IoT network. The experimental work for this proposed scheme was carried out in MATLAB computing software, embedded with image processing toolbox and thingSpeak IoT Analytics platform. . In addition to the security paradigm, we also tried to find out the percentage of dissimilarity in the feature extracted Iris images of two persons: who do not have any biological relation with each other, who are twins and Iris images of the same person. The percentage of dissimilarity is calculated by first obtaining a difference matrix followed by calculation of Average Difference as under

Difference matrix = filtered real time iris image – filtered database iris image

$$\textit{Dissimilarity percentage} = \sum_{k=1}^{n} \frac{Avege}{256*256} 100$$

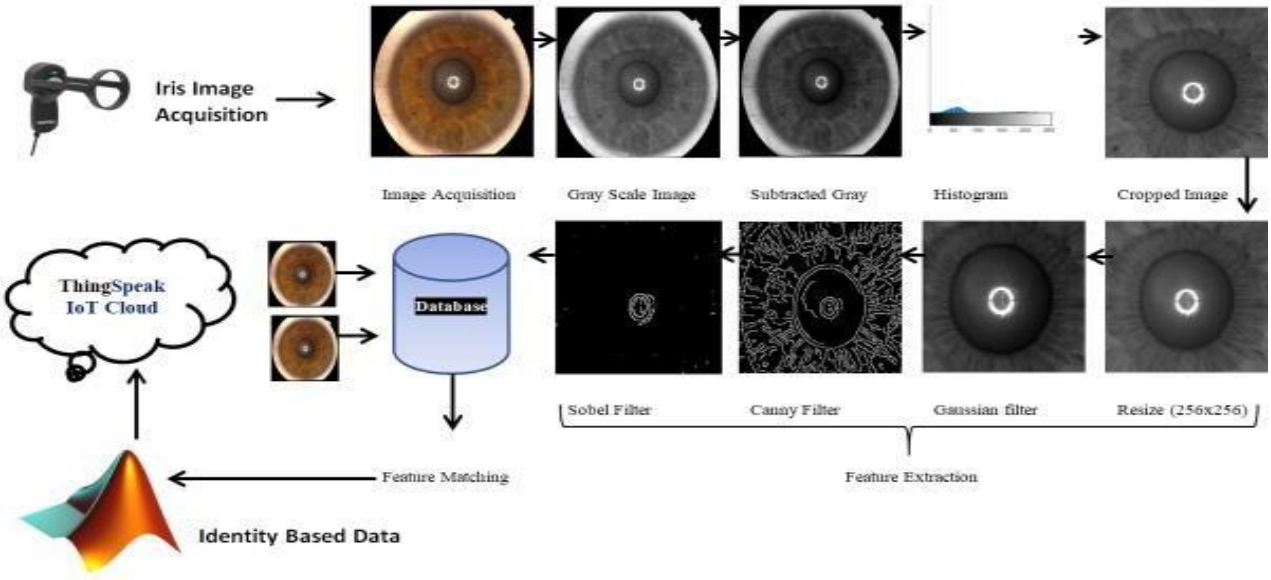

Figure. 1: The proposed technique for iris recognition based security for IOT

IV. METHODOLOGY

As mentioned in the proposed idea, the overall iris recognition process consists of many stages. These steps are discussed in more detail as under:

- Image acquisition: The initial stage in any image processing system is image acquisition. It is the process of using an optical equipment to capture real- world data (an unprocessed image) of an item and transforming it into a sequence of numerical data that can then be processed on a computer. This stage necessitates the use of a camera to capture images, a sensor to measure energy, and an optical system to concentrate the energy.
- Gray scale image: A grayscale image is a type of monochromatic image made entirely of shades of grey, ranging from black to white at its darkest point. This type of image is used in image processing since it requires less information per pixel because grey is the only colour in which the rbg component has equal intensities, unlike any other colour, which requires three intensities to indicate.
- Subtracted gray: In this stage, one gray scale picture array is subtracted from resulting in all negative values

being reset to zero.

- Histogram: A histogram is a visual representation of a picture. It usually has bars to illustrate the frequency with which data appears. It has two axes, x and y. The occurrences are represented on the x axis, while the frequency is represented on y axis. The varying heights of the bar represent different data occurrence frequencies.
- Cropped image: To improve composition of the image, this step entails chopping out the extra section of the image.
- Feature extraction: When the input image data is too extensive to process and a portion of it is redundancy-prone, the input is reduced to a smaller collection of data. Feature extraction is the term for this transformation process. The image is first downsized to a certain dimension of 256 by 256 pixels in this process. The scaled image is then run through a Gaussian filter, which reduces image contrast and smoothes it out, removing any noise. The processed image is next sent via the canny filter, which detects the edges of an image and, when combined with a Sobel filter, produces a high spatial frequency image. It is used to calculate the approximate absolute gradient magnitude at each point in a grayscale image input.

V. RESULTS AND DISCUSSION

The experiment was carried out for three sets of Iris images: Iris images of two persons who do not have a biological relation with each other, Iris images of two persons who are twins, and Iris images of the same person. The results reveal that, closer the biological relationship between the persons under trial, lesser is the percentage of dissimilarity between their features extracted Iris images. Thus, more are the chances of having a perfect match with the iris image in the database. The relationship criterion between the iris images and the amount of percentage dissimilarity is shown in table 1.

Table 1: Relationship criterion and percentage dissimilarity

S.No.	Type of IRIS Images	Average Difference (%)	Dissimilarity % age
01	No Relation	86.708	33.870
02	Twins (pair 1)	25.442	9.938
03	Twins (pair 2)	30.119	11.765
04	Same person images(RL)	30.426	11.885
05	Same person images(LL)	0	0
06	Same person images(RR)	0	0

Figure 2 shows the stepwise operation done on the Iris images for three different categories and the corresponding outputs obtained at each stage. The acquired RGB Iris Image is first converted to gray scale to reduce the number of color levels and the amount of pixel information to be provided. The subtraction of the gray scale image is done to obtain only shades of black and white for clear distinction. The histogram of the grayscale image represents tonal distribution of the black and white shades in a digital image. The number of pixels for each tonal value is plotted.The cropping of an image is done to remove the unwanted portions of the image or to adjust the outside edges of the image. For comparing two images, it is necessary to have the same number of pixels. This is acquired by resizing operation. The Gaussian smoothing filter is a 2-D convolution operator. Gaussian smoothing filter is used to `blur' images and remove details and noise components. It resembles the mean filter, but uses a different kernel that characterizes the shape of a Gaussian (`bell-shaped') hump. The Canny edge detector is a segmentation technique consisting of an edge detection operator that involves a multi-stage algorithm to detect an extensive range of edges in images. . Image filtering through Sobel operator is another segmentation technique which calculates the gradient of image intensity at every pixel of the image. The Sobel operator clearly shows how abruptly or smoothly the intensity levels changes at every pixel and therefore shows how a pixel represents an edge. The Iris image features extracted through Gaussian filter, canny filter and Sobel Filter are then subjected to matching process with the image features stored in database. If a match is obtained in the database, the identity based data is pushed on to the ThingSpeak IOT analytics platform, if data transmission is not halted. The identity based data is generated randomly using MATLAB and pushed on to IOT platform as shown in the figure 3.

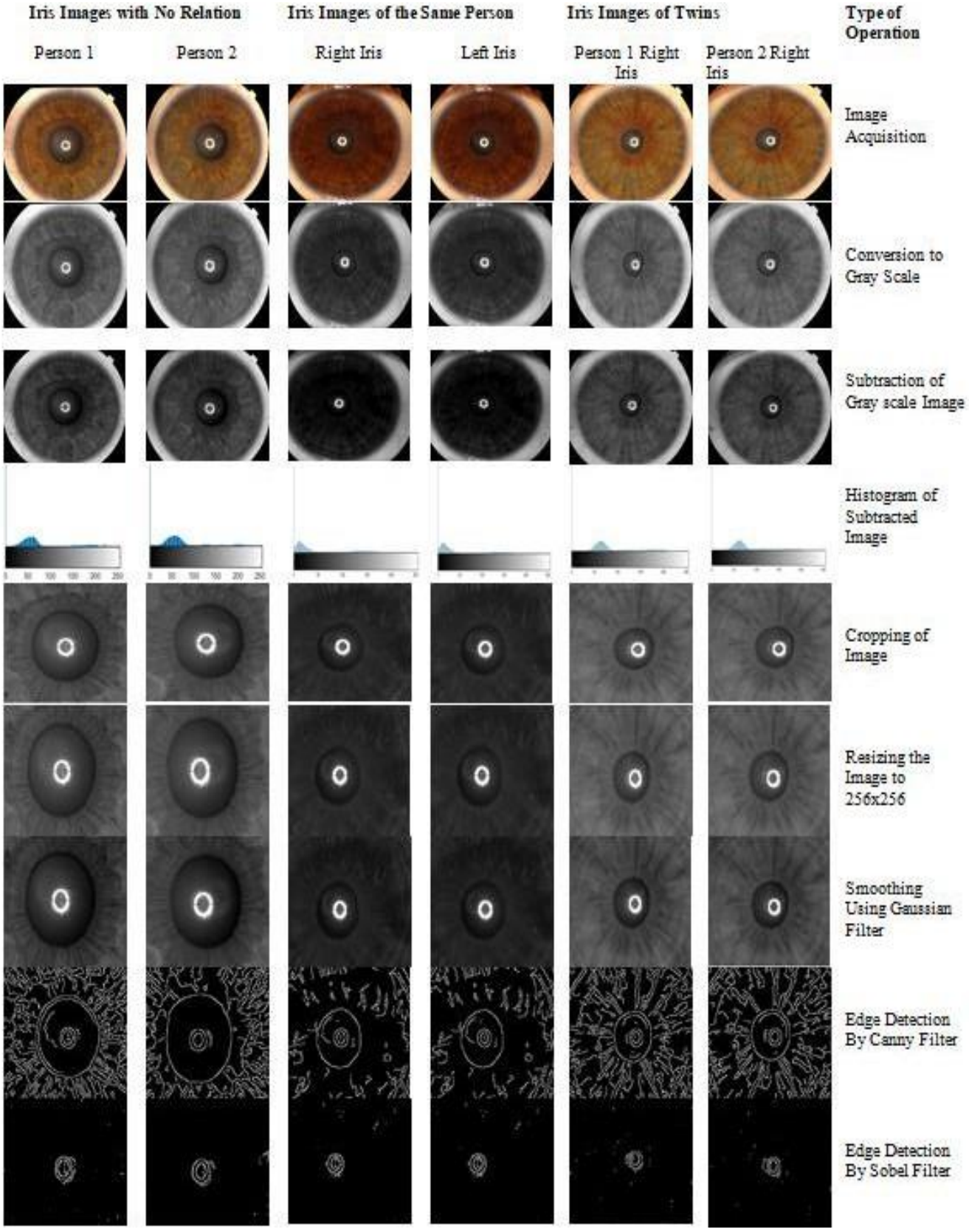

Figure 2: Stepwise operation on iris images and their corresponding outputs

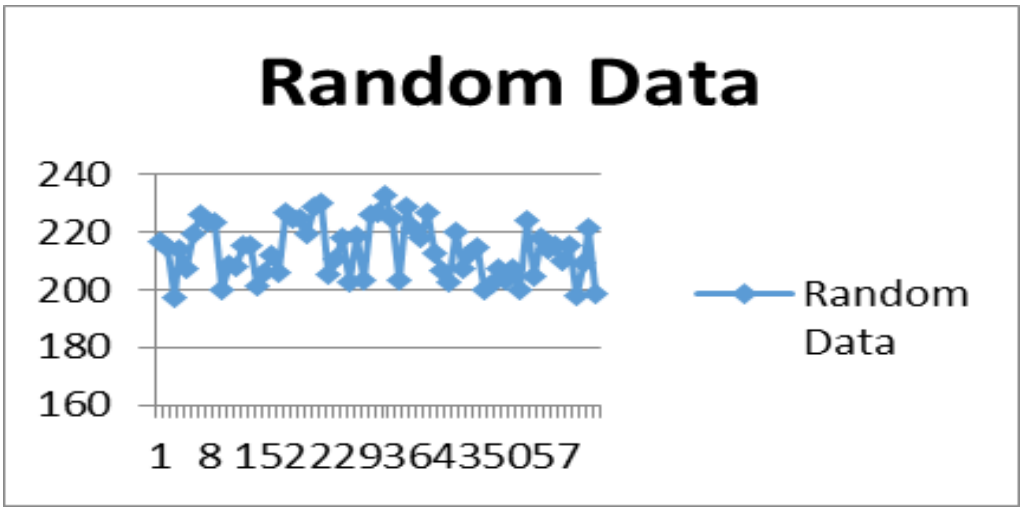

Figure 3: Random Data Pushed to ThingSpeak IoT Analytics platform on perfect Iris Match

VI. CONCLUSION

The proposed idea mentioned above was successfully implemented using MATLAB computing software embedded with the image processing toolbox and thingSpeak IoT analytics platform. The system tested Iris images from three different scenarios e.g. Iris images of two persons with no biological relation, Iris images of two persons who are twins and Iris Images of the same person. The percentage of dissimilarity reveals that closer the biological relation between the persons under trial, lesser is the percentage of dissimilarity and vice versa. A series of steps involved in the process of Iris recognition was implemented with corresponding image outputs at each stage. The user identity based data was successfully pushed on to the ThingSpeak IoT platform on verification of the matched Iris images.

REFERENCES

[1] Zongqiang Zhang; Feng Xia; Mingchu Li; Jianhua Ma , "An improved iris localization for authentic system," IEEE International conferences on internet of things, and cyber, physical and social computing,2011

[2] Yosra Ben Said, "Collaborative security for the internet of things," Economics and Finance, Institut des Telecommunications,2013

[3] Jasvir Singh Kalsi; Sarabjeet Kaur; Bhawneet Kaur, "Efficient biometric iris recognition using gamma correction & histogram thresholding – A review," International journal of advance electrical and electronics engineering (IJAEEE), Volume-4, Issue-3, 2015

[4] M. Shamim Hossain; Ghulam Mohammad; SK MD Mizanur Rahman; Wadood Abdul; AbdulHameed Alelaiwi; Atif Alamri, " Toward end to end biometrics based security for IOT infrastructure," IEEE wireless communication, October, 2016

[5] Ramdan Gad; Ahmed A. Abd El-Latif; Sherif Elseuoofi; Hany M Ibrahim; Mahmoud Elmezain; Wael Said. "IOT security based on iris verification using multi-algorithm feature level fusion scheme," IEEE, 2019

[6] Jaspreet Kaur; Shivali Puri; Varinderjit kaur, "Iris recognition using Hough's transform gamma correction and histogram thresholding method," International journal of engineering sciences and research technology, October, 2016

[7] Annies Joshy; Jalaja M. J, "Design and implementation of an IOT based secure biometric authentic system," IEEE, 2017

[8] WenchengYang; Michael N. Johnstone; Leslie F. Sikos; Song Wang, "Security and forensics in the internet of things: research advances and challenges," IEEE Workshop on emerging technologies for security in IoT, 2020

[9] Reza M. Pairizi; Ali Dehghantanha; Kim Kwang Raymond Choo, "Towards better ocular recognition for secure real world applications," IEEE, 2018

[10] Hasamuddin Mohammed; Mohammad Qayyum, "Internet of things: A study on security and privacy threats," IEEE, 2017

[11] R.Subha, "Biometrics in internet of things (IOT) security," International Journal of Engineering Research and General Science, Volume 5, Issue 5, September –October, 2017

[12] Ramadan Gad; Mahmoud Elmezain; AhmedAbd El- Latif, "IOT security based on iris verification using multi-algorithm feature level fusion scheme," IEEE, 2019

[13] J.Thirumalai; Gokul. R; Ganasekaran. P; Manellore Murali. M; Jackson Jublience Joseph. L, "An IOT based bank locker security system," International journal of engineering research and technology (IJERT), Volume 8, Issue 7, 2020

[14] Ramadan Gad; Ahmed Abd El-Latif; Mohammed Talha; M. Zorkany, "Iris recognition using multi-algorithmic approaches for cognitive internet of things (CIoT)," Future generation computer systems, December, 2018

[15] Ramadan Gad; Ahmed A. Abd El-Latif; Sherif Elseuofi; Hany M Ibrahim; Mahmoud Elmezain; Wael Said, "IoT security based on iris verification using multi-algorithm feature level fusion scheme," IEEE, 2019

[16] Belal M. Alsellami; Prapti D. Deshmukh, "The recent trends in biometrics traits authentication based on internet of things," IEEE, 2021

[17] M. Shamim Hossain; Ghulam Mohammad; SK MD Mizanur Rahman; Wadood Abdul; AbdulHameed Alelaiwi; Atif Alamri, " Toward end to end biometrics based security for IOT infrastructure," IEEE wireless communication, October 2016