ISSN 2347 - 3983

Volume 7, No. 11 November 2019

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter327112019.pdf

https://doi.org/10.30534/ijeter/2019/327112019

An Efficient and Secured Biometric Authentication for IoT

K. RUTH RAMYA[1], B. MANJULA JOSEPHINE[2], K. DURGA PRAVEEN[3], M. BALA MARUTHI[4], CH.SAI KUMAR[5]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, ramya_cse@kluniversity.in

[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, manjulajosephine@gmail.com

[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, pandu.97007@gmail.com

[4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, balumannava0009@gmail.com

[5]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, saikumarchinni36@gmail.com

ABSTRACT

The Internet of Things (IoT) is that the ability to produce everyday devices with the way of identification and otherwise for communication with one nother. The spectrum of IoT application domains is extremely massive together with sensible homes, sensible cities, wearable's, e-health, etc. Consequently, tens and even many billions of devices are going to be connected. Such devices can have sensible capabilities to gather, analyze and even create selections with none human interaction. Security may be a supreme demand in such circumstances, associated specially authentication is of high interest given the injury that might happen from a malicious unauthenticated device in an IoT system. Fingerprint based mostly biometry authentication approaches can enhance the protection in several industries and endless applications reminiscent of police work, automotive business, sensible town development, sensible home etc. This paper presents the fingerprint {based mostly primarily based mostly} identification for breakdown the protection challenges in IoT based applications.

Key words: Fingerprint Biometrics; Internet of Things; Multifactor Authentication; Security attacks.

1. INTRODUCTION

Technological revolution in info and communication Technology sector is being increased to facilitate the users of advanced and intelligent services. It integrates the event of sensible devices and IoT services. IoT envisions a future networking paradigm and repair orientating infrastructure within which spatially distributed physical objects are going to be deployed to make info networks to facilitate advanced and intelligent services [1]. The devices cited as "things" could embrace numerous types of sensors, actuators, RFID, mobile devices and sensible appliances. Researchers estimate that IoT can encompass fifty billion objects by 2020[2]. Most of the IoT devices are often monitored and controlled by sensible device applications. IoT devices and applications are interfaced and accessed solely by genuine users. Authentication systems is also physical devices or logical model. the best implementations of physical authentication devices are sensible cards and secret tokens. Compared to those ancient ways of authentication, biometry based mostly authentication is a lot of convenient and quicker. it's safer to use biometric based mostly authentication to access our personal devices.

1.1 IoT Generic design

While ancient net connects folks to a network, IoT contains a completely different approach within which it provides Machine-to-Machine (M2M) and Human-to-Machine (H2M) property, for heterogeneous forms of machines so as to support form of applications (e.g., distinguishing, locating, tracking, monitoring, and controlling) [8]. Connecting a large variety of heterogeneous machines [9] results in a colossal traffic, thus the necessity to manage the storage of huge information [10,11]. Therefore, the TCP/IP design, that has been used for an extended time for network property, doesn't suit the wants of IoT relating to numerous aspects together with privacy and security (e.g., info privacy, machine's safety, information confidentiality, encoding, and network security) [12], measurability, dependableness, ability, and quality of service [13].

Although various architectures were planned for IoT, there's still a necessity for a reference design [14,15]. the fundamental design model planned within the literature may be a three-layer design [13,16–18], as shown in Figure 1a. It consists of: perception, network and application layers.

Perception layer: it's the physical layer that senses the setting to understand the physical properties (e.g., temperature, humidity, speed, location, etc.) victimization end-nodes, through the employment of various sensing technologies (e.g., RFID, GPS, NFC, etc.).

Network Layer: it's the layer guilty of obtaining information from the perception layer and transmission it to the appliance layer through numerous network technologies (e.g., 3G, 4G, 5G, Wi-Fi, Bluetooth, Zig-Bee, etc.). it's conjointly accountable of information management from storing to process with the assistance of middle-wares reminiscent of cloud computing.

Application Layer: it's the layer that's guilty of delivering application-specific services to the user. The importance of this layer is that it's the power to hide various markets
(e.g., sensible cities, sensible homes, health care, building automation, sensible metering, etc. [1,2]) .

Another planned superimposed design is that the five-layer design (Figure 1b) [13,16–18]. The 5 layers are from high to bottom: business, application, processing, transport, and perception layers.

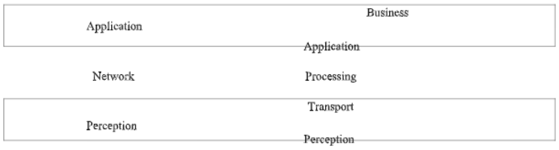
The functions of perception, transport (i.e., network layer) and application layers are a similar as within the three-layer design. The remaining layers of the design are:

Processing layer: conjointly referred to as the middle-ware layer, it's accountable of providing numerous forms of services, principally storing, analyzing, and process information with relation to the machine results.

Business layer: Its work covers the IoT system actions and practicality. the appliance layer sends the info to the business layer whose role is to create business models, graphs, and flowcharts to investigate information, so as to play a task in deciding regarding business ways and road-maps.

Other architectures may also be known within the literature. In the authors used a five-layer design supported Service orientating design (SOA) that helps the mixing of IoT in enterprise services. In , the authors thought of a non-layered approach for the design
(e.g., cloud design, fog design, social IoT, and design supported human brain processing).

For the remainder of this paper, we tend to contemplate the three-layer design.



(a) The-layer design (b) Five-layer architecture

Figure 1:. IoT design models.

1.2 Security Challenges in IoT

IoT setting is enabled by open wireless technologies reminiscent of Bluetooth, frequence Identification (RFID), embedded sensors, actuators, moreover as Wi-Fi for dominant the connected devices. IoT setting is collaboration of assorted technologies and distributed and distributed devices . because the numbers of connected devices will increase, new challenges may also be accrued. Security necessities can differed by the employment of applications and methods. If any of sensible devices are lost or purloined, it's simple for the hacker to retrieve all the sensitive info from the devices. There are many potential attacks which can be masquerading, spoofing, Middleman attack, do's attack, and secret changes. it's necessary to think about of these attacks and things within the IoT setting. Moreover, existing ways aren't enough to beat the challenges. Security challenges within the setting of little embedded devices should be simple to implement and value effective. Mechanisms for enhancing the protection in Iota setting should provide by well unnatural authentication.

1.3 Biometric based mostly authentication and IoT Domain

Biometrics based mostly authentication has been receiving in depth attention within the Iota network society due to its dependableness and growing would like of security. It offers higher security and fewer likelihood of spoofing associated is tried to be an economical and correct answer to the matter [6]. Many surveys and studies are conducted by many researchers targeted on imposing the protection by biometry in Iota setting [7]. As unauthorized users aren't ready to show a similar distinctive physical properties to possess a positive authentication, dependableness are going to be ensured. This can be far better than the standard ways of victimization passwords, tokens or personal positive identification (PINs) at a similar time provides a price effective convenience approach of getting nothing to hold or keep in mind [8]. Most of the schemes target the key institution between the user and entry node. identification has not been thought of for Iota applications for 2 main reasons; 1) Iota architectures aim at automatization with no human interventions 2) variety of Iota devices have restricted computing capabilities, whereas onerous and soft biometric authentication ways embrace a lot of complicated calculations for deciding, identity prediction classifiers, meta-biometric prediction classifiers. Biometric authentication using both fingerprint and palm print have been developed by the author [19]. In 2019 the author again implemented a novel SFM-CPABE method that has low computational time and high efficiency when compared to traditional cloud security models [20]. Among biometrics the fingerprint biometrics is more efficient and affordable biometrics [21]. And methodologies about the internet security, aspects of security, encryption methodologies have been proposed by the authors[22-26].

2.IMPLEMENTATION

Fingerprints are made of a series of edges and furrows on the surface of the finger and have a core around which patterns like swirls, loops, or arches are curved to ensure that each print is unique [13]. An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form arc, and have a habit of to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger. The ridges and furrows are characterized by irregularities known as minutiae, the distinctive feature upon which finger scanning technologies are based. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. There are five stages involved in finger-scan verification and identification: 1. Fingerprint Image Acquisition 2. Image Processing method 3. Locating Distinctive Characteristics 4. Template Creation method 5. Template Matching method A sensor takes a mathematical snapshot of the user's unique pattern, which is then saved in a fingerprint database. A fingerprint enhancement algorithm (that uses Gabor filters as band-pass filters to remove the noise and preserve true ridge/valley structures) is included in the minutiae extraction module to ensure that the performance of the system is not affected by variations in quality of fingerprint images

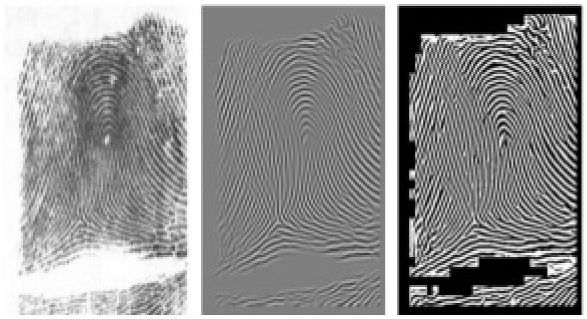


Figure 2: Construction of Grey Scale Image from Fingerprint Image

2.1 Proposed Technique for Fingerprint based mostly Identifications

A well-performed biometric modality ought to contain the traits reminiscent of individuality, accuracy, richness, easy acquisition, and dependableness and user acceptance. Among numerous biometric based mostly authentication methodologies, Fingerprint based mostly authentication is thought to be associate effectual technique for distinguishing persons with high confidence. The planned model of framework for IoT setting by biometric based mostly authentication by fingerprints victimization Star IoT Network is meant.

Illustrates the model involves associate IoT entry node through that the users are connected to perform many activities. The advantage of star IoT network is that every one the quality within the style of the network is managed by a central node or Iota entry Node ‘$\boldsymbol{GN}$’. As shown within the figure, the planned technique includes a group of entities representing the set of users connected with the help of a relationship set ‘SIG’. the link set is mathematically developed as given below.

$SIG \rightarrow (U, R, C)$ -------------------(1)

From (1), the star IoT graph ‘SIG’ within the planned technique includes the set of users ‘U’, with the link set denoted as ‘RS’ and relative constant denoted as ‘C’ severally. every user ‘U’ is outlined as below.

$U \in Ui$ ---------------------------(2)

$Ui \rightarrow Ui \cup fp1 , fp2 , \ldots , fpn$----------------------- (3)

‘Ui ’ represent the set of users, where, ‘FPi ’ represent a fingerprint attribute of the user with finger print feature sets ‘$fp1$ ’, ‘$fp2$ ’ and then on extracted at completely different time settings ‘$t1$ ’, ‘$t2$ ’ severally. the link set within the technique is drawn as ‘RS’ within the IoT setting, wherever ‘U’ represents the nodes or users and ‘I’ corresponds to the link or interactions that connect between the users and IoT devices. Here, the nodes or users are drawn as points whereas the interactions between the users and IoT devices are given as lines. Besides, the constant worth ‘C’ symbolizes ‘ $*U \rightarrow r$, $w\square erer \in RS$’ corresponds to a perform that assigns a relationship kind ‘r’ between a given user, ‘Ui ’ and IoT services. The network is associate extended integration of sensible applications, things and open wireless technologies for storing and forwarding a lot of important info. 2 stages within the planned framework are registration and authentication. Throughout registration stage victimization multifactor fingerprint identities, the user registers their personal digital assistants and devices with the entry. The entry node provides on demand IoT services to the registered user once authentication. Nothing management maintains a register of devices, sensors and actuators which might be accustomed briefly disables or isolates the affected devices till they'll be patched. This feature is especially necessary for key devices reminiscent of entry devices so as to limit their potential to cause hurt or disruption, as an instance, by flooding the system with faux information if they need been compromised. At any time, the user access the Iota devices through network, the system authorizes and validates the user through fingerprint module (i.e. fingerprint images) that are hold on as templates. In alternative words, if the user fails to authorize himself through fingerprint recognition as hold on in templates, he cannot access the IoT devices. This fingerprint module has the aptitude to be integrated with differing kinds of sensors like machine-driven door lock, completely different electronic devices, security devices and then on. In system implementation, a biometric fingerprint security model is developed for sensible home observation. Actions are often applied mechanically employing a rules engine with rules supported vulnerability management policies.

Feature Extraction Most Feature extraction algorithms function on the following four steps ℵ Determine a reference point for the fingerprint image, ℵ Tessellate the region around the reference point, ℵ Filter the region of interest in different directions, and, ℵ Define the feature vector.

Fingerprint Matching Fingerprint matching refers to finding the similarity between two given fingerprint images. Due to noise and distortion introduced during fingerprint capture and the inexact nature of feature extraction, the fingerprint representation often has missing, spurious, or noisy features.

Therefore, the matching algorithm should be immune to these errors. The matching algorithm outputs a similarity value that indicates its confidence in the decision that the two images come from the same finger. The existing popular fingerprint matching techniques can be broadly classified into three categories depending on the types of features used:[8]

ℵ Minutiae-based
ℵ Correlation-based
ℵ Euclidean distance-based

One of the main difficulties in the minutiae-based approach is that it is very difficult to reliably extract minutiae in a poor quality fingerprint image. The simplest correlation-based technique is to align the two fingerprint images and subtract the input image from the template image to see if the ridges correspond. For the third approach, matching is based on a simple computation of the Euclidean distance between the two corresponding feature vectors, and hence is extremely fast.

3.ALGORITHM

Step 1: Acquire I/P fingerprint

Step 2: Perform Normalization on input finger, to adjust the intensity value by adjusting the range of gray level values.

Step 3: Perform Segmentation, to separate the foreground regions in the image from the background regions. The foreground regions consist of fingerprint area containing the ridges and valley and background consist of regions outside the borders of the fingerprint area. If we do not remove background regions from the fingerprint then the extraction algorithm extracts noisy and false Minutiae.

Step 4: Perform Image Enhancement through Fingerprint image was rotated with the difference of 10 degree by selecting arbitrary image rotation option from the image menu till the core of both the images become uniform with respect to each other.(4)The core of fingerprint was kept at 90 degree which was adjusted by selecting image > image rotation > arbitrary image rotation.(5)The core aligning 90 degree was checked with the help of grid option. The straight line of the grid should run parallel to the core line.

Step 5: Converts Enhanced Image into Binary Image through Binarization. It is the process that converts a grey level image into a binary image.

4. PSEUDO CODE

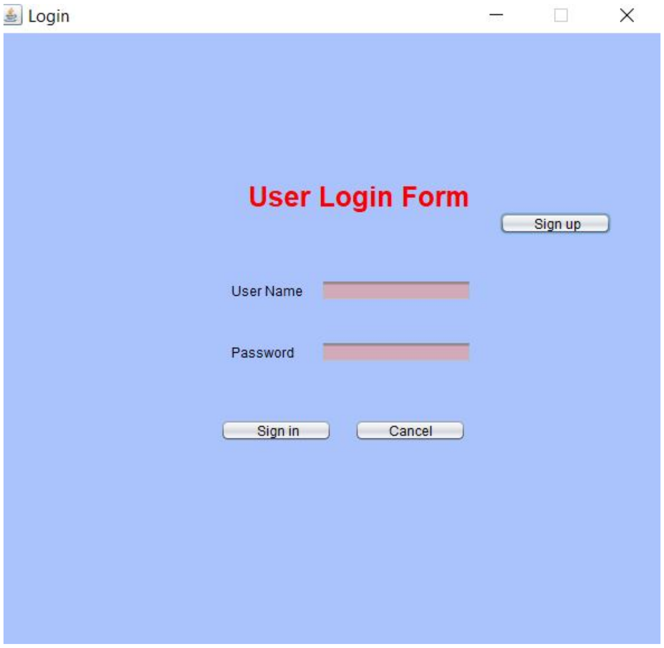
```
def distance(x, y, W):
come one + sqrt((x - W) ** a pair of + (y - W) ** 2)

def create_segmented_and_variance_images(im, W,
threshold):
(x, y) = im.size
variance_image = im.copy()
segmented_image = im.copy()
for i in range(0, x, W):
for j in range(0, y, W):
box = (i, j, min(i + W, x), min(j + W, y))
block_stddev = ImageStat.Stat(im.crop(box)).stddev[0]
variance_image.paste(block_stddev, box)
if block_stddev < threshold:
segmented_image.paste(0, box) # build block black if
rejected
come (segmented_image, variance_image)
```

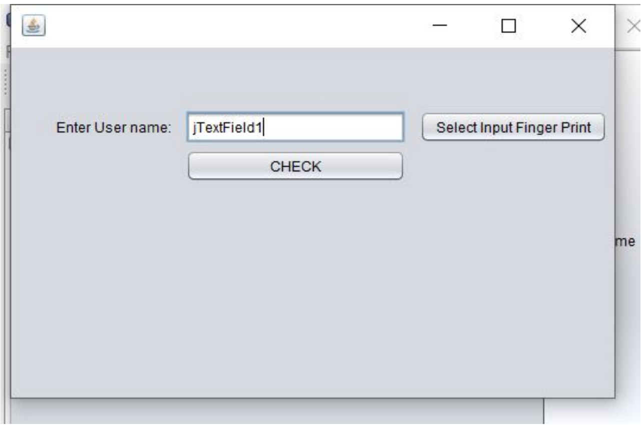
5. CONCLUSION

IoT technology enhances the prevailing life vogue by desegregation all the devices to a digital level within the in depth directions. The appliance areas of IoT infrastructure are going to be extended from sensible devices to sensible homes, sensible industries, and educational activity establishment's aid organizations, Scientific and analysis industries and sensible town development. Digital users have their own sensible devices with custom-made authentication procedures and completely different security standards for various functions. All told these applications and technologies, usually associate identification of many challenges, many security attacks in IoT setting were analyzed during this article. The planned model of framework for IoT setting by biometric based mostly authentication by fingerprints victimization Star IoT Network is meant. The advantage of star IoT network is that every one the quality within the style of the network is managed by a central IoT entry Node. The planned framework is going to be developed additional and its security analysis and performance measures to be analyzed on IoT context in future.

6. RESULTS

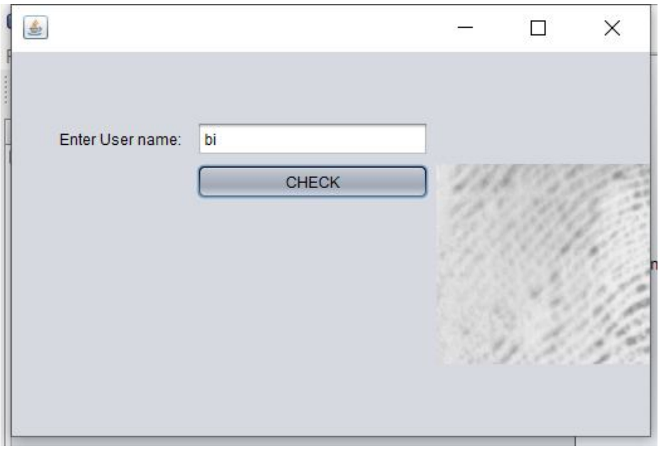


USER VALIDATION

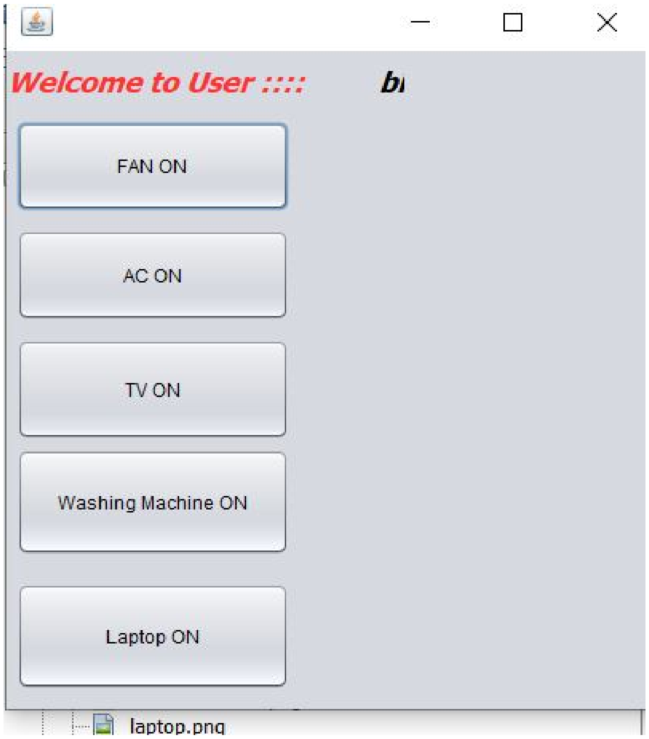


Enter User name: jTextField1

SELECTION OF USER ID AND USER FINGERPRINT FOR AUTHENTICATION



Enter User name: bi



Welcome to User :::: bi

AFTER THE USER IS BEING GRANTED ACCESS

REFERENCES

[1]. Par winder Kaur Dhillon, Sheetal KaltA. **A light-weight biometry based mostly remote user authentication theme for IoT services**. Journal of knowledge Security and Applications.2017.

[2]. R.Gaikwad. net of Things(iot**): Revolution of net for sensible environment"** Oracle, Tech Rep.2016.

[3]. Munish Bhatia, Sandeep K.Sood," **A comprehensive health assessment framework to facilitate IoT-assisted sensible workouts; A prophetic aid perspective**" computers in business 02, 0166-3615, 2017, pp-50-66. https://doi.org/10.1016/j.compind.2017.06.009

[4]. Igor Tomi ci c, Petra Grd, Miroslav Ba ca, "**A review of soppy biometry for IoT**", MIPRO 2018. https://doi.org/10.23919/MIPRO.2018.8400203

[5]. Chun-Xiao Ren, Yu-bin Gong, Fei Hao, Xin-yanCai,and YuXiaoWu " **once biometry meets Iot: A survey**", Proceedings of sixth international Asia Conference on engineering science and Management Innovation, 2016.pp. 35-643.

[6]. Aswathi S &amp; Mr. Anoop, "**A Survey On Iris, Face, And Fingerprint Spoofing Detection Systems** ", world Journal Of field And Researches, 2017, Pp.29-37.

[7]. K. Jain, S. C. Dass, and K. Nandakumar, "**Can soft biometric traits assist user recognition**" vol. 5404, 2004, pp. 5404 – 5404 – twelve.

[8]. K. Jain, P. Flynn, and A. A. Ross, **book of facts of biometry**. Secaucus, NJ, USA: Springer-Verlag the big apple, Inc., 2007.

[9]. Johnson. P. A., F. Hua, and S. Schuckers, "**Comparison of quality based mostly fusion of face and iris biometry**," in International Joint Conf. on biometry (IJCB), Oct. 2011, pp. 1–5. https://doi.org/10.1109/IJCB.2011.6117481

[10]. Marco, R. Casas, J. Falco, H. Gracia, J.I. Artigas, A. Roy, Location-based services for old and disabled folks, Comput. Commun. thirty one (6) (2008) 1055–1066. https://doi.org/10.1016/j.comcom.2007.12.031

[11]. M. Bhatia, S.K. Sood, **Temporal informative analysis in smart-ICU monitoring: m-Healthcare perspective**, J. Med. Syst. forty (8) (2016) pp.1–15.

[12]. M.S. Hossain, G. Muhammad**, Cloud-assisted industrial net of things (IIoT)-enabled framework for health observation**, Computer. Network. one hundred and one (2016) 192–202,

[13]. Dawood, "**Cloud And Iotbased Home Automation: Closed-Loop management Of Appliances**", International Journal Of inventive analysis Thoughts (Ijcrt), Volume.5, Issue 2, pp.83-86, June 2017.

[14]. S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, and L. Veltri, "**A ascendable and self-configuring design for service discovery within the net of things**," IEEE net of Things Journal, vol. 1, no. 5, pp. 508– 521, 2014. https://doi.org/10.1109/JIOT.2014.2358296

[15]. Kantarci, M. Erol-Kantarci, and S. Schuckers, "**Towards secure cloud central net of biometric things**," in Cloud Networking (CloudNet) IEEE fourth International Conference on. IEEE pp. 81-83, 2015.

[16]. Reid and M. S. Nixon, "**Using comparative human descriptions for soft biometry**," in biometry (IJCB), 2011 International Joint Conference on. IEEE, 2011.

[17]. Dantcheva, P. Elia, and A. Ross, "**What else will your biometric information reveal? a survey on soft biometry**," IEEE Transactions on info Forensics and Security, vol. 11, no. 3, 2016.
https://doi.org/10.1109/TIFS.2015.2480381

[18]. M. C. D. C. Abreu and M. Fairhurst, "**Enhancing identity prediction employing a novel approach to combining hard-and soft-biometric info**," IEEE Transactions on Systems, Man, and informatics, half C (Applications and Reviews), vol. 41, no. 5, pp. 599–607, 2011.

[19]. Sahithi, S., Anirudh, A., Swaroop, B., Ruth Ramya, K., **"Biometric security for cloud data using fingerprint and palm print"**, International Journal of Innovative Technology and Exploring Engineering, 2019, 8(6), pp. 338-343.

[20]. Kalangi, R.R., Chandra Sekhara Rao, M.V.P., "**A novel single user fingerprint minutiae based integrity verification and encryption algorithm for cloud data**", International Journal of Innovative Technology and Exploring Engineering, 2019, 8(5), pp. 746-751.

[21]. Ruth Ramya, K., Saahithi, S., Gnaneswar, T., Afsar Jaha, S.D., "**A survey on biometric based crypto techniques**", International Journal of Engineering and Technology(UAE), 2018, 7(2), pp. 1091-1095.
https://doi.org/10.14419/ijet.v7i2.7.12234

[22]. Reddy, B.K., Supriya, C.H., Prasad, B.D., Ramya, K.R., "**A biometric security for cloud data using voice as a key**", International Journal of Recent Technology and Engineering, 2019, 7(6), pp. 728-736.

[23]. Kalangi, R.R., Chandra Sekhara Rao, M.V.P, "**A novel multi-user fingerprint minutiae based encryption and integrity verification for cloud data**", International Journal of Advanced Computer Research, 2018, 8(37), pp. 161-170.

[24]. Ramya, K.R., Malleswari, D.N., Rani, C.R., Bhattacharyya, D., Kim, H.-J., "**Key aggregate based homomorphic encryption for efficient authentication for secure cloud storage**", International Journal of Database Theory and Application, 2016, 9(11), pp. 137-148.
https://doi.org/10.14257/ijdta.2016.9.11.13

[25]. Ruth Ramya, K., Sasidhar, T., Naga Malleswari, D., Rahul, M.T.V.S., "**A review on security aspects of data storage in cloud computing**", International Journal of Applied Engineering Research, 2015, 10(5), pp. 13383-13394.

[26]. Vamshinath, N., Ruth Ramya, K., Krishna, S., (...), Mwaseba, G.L., Kim, T.-H., "**Homomorphic encryption for cluster in cloud**", International Journal of Security and its Applications, 2015, 9(5), pp. 319-324.
https://doi.org/10.14257/ijsia.2015.9.5.31

[27] Rao, K. R., & Josephine, B. M. (2018, October). Exploring the Impact of Optimal Clusters on Cluster Purity. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 754-757). IEEE.
https://doi.org/10.1109/CESYS.2018.8724114