ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter22852020.pdf
https://doi.org/10.30534/ijeter/2020/22852020

# A Unique Secure Multimodal Biometrics-Based User Authenticated Key Exchange Protocol for generic HIoT Networks

**M. Savitha[1] , M. Senthilkumar[2]**
[1] Research Scholar, Department of Computer Science, Government Arts College, Udumalpet India.
savithainmail@rediffmail.com
[2]Assistant Professor, Department of Computer Science, Government Arts and Science College, Avinashi, India.
msenthilkumar.cta.cit@gmail.com

## ABSTRACT

The Special sort of generic IoT network namely Hierarchical IoT Network (HIoTN) is one in which a client can legitimately get to the continuous information from the sensing nodes in a protected generic IoT networking environment especially for particular application. This innovation serves a platform for a new protected lightweight unimodel biometric-factor remote client verification system for HIoTNs in prior, called the Client Validated Biometric Key Administration Convention (UABKMP). These unimodal biometric systems possess various limitations such as Noisy data, Non-universality, Spoof attacks etc., which may greatly affect the overall security of the user. In this work, a new multimodal biometrics based temporal credential-based lightweight user authentication system is intended to manage this significant issue in the HIoTN setting, would be called the Secure Multimodal Biometrics-based User Authenticated Key Exchange Protocol (SMBUAKEP). In addition, fuzzy commitment methodology is greatly utilized in this research for the purpose of multimodal biometric verification. In this research, three approaches namely Real-Or-Random (ROR) is utilized for detailed security analysis using formal security, Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for formal security verification and SMBUAKEP for informal security analysis which has the ability to avoid multiple known attacks. An exhaustive similar examination for SMBUAKEP and some other pertinent frameworks has been accomplished, and the exploration shows that SMBUAKEP offers better security and functionality features and diminished expenses in both processing and correspondence communication comparative with existing frameworks, for example, UABKMP and UAKMP.

**Key words:** Generic IoT network, authentication, key management, security, Hierarchical IoT network AVISPA simulation, Real-Or-Random, fuzzy commitment approach, multimodal biometric.

## 1. INTRODUCTION

The digital electronics and wireless communications has become an essential part of life now-a-days and hence there is rapid growth in advancement. The Internet of Things (IoT) is another inevitable area by the people which has rapidly increased which also find its applications in industrial automation, intelligent transportation, medical, and eHealthcare services [1]. Additionally IoT plays a significant role in future Internet and involves with a huge number of shrewd imparting communicating objects or things. The IoT is also called as Internet of Everything (IoE) since it satisfies the regular desires of people by associating with things, processes, and data etc. in an effective manner [2].Various researches is being carried out for new emerging Wireless Sensor Networks (WSNs), Device-to-Device (D2D), and Machine-to-Machine (M2M) technologies to expand the tangible abilities of various sensors, thereby enhancing the wireless IoT technology [3].

The Intranet of Things [4] is another interesting scenario which connects the local networks with various paradigm such as M2M, D2D, and WSN and also possess only the regional information. The IoT networks pool resources with various intranet and cloud server for exploiting the comprehensive and historical information. Many sensor nodes are involve in IoT network which pose constrained network resources which paves main limitation in directing the sensed data directly to the gateway for all nodes. On the other hand, clustering of sensor nodes are done for transferring the sensed data to the corresponding cluster head/aggregator. The Internet link now takes its role in sending merged data to the gateway. This methodology is highly progressive and energy efficient when contrasted with the flat routing since sensed data is directly delivered to the gateway [5].

The traditional WSNs normally utilizes hierarchical routing or clustering protocols such as Low Energy Adaptive Clustering Hierarchy (LEACH), Hybrid Energy Efficient Distributed (HEED), Threshold Sensitive Energy Efficient Sensor Network (TEEN), and Stable Election Protocol (SEP) [6]. The LEACH is popular one among all the above since it utilizes distributive

clustering model in which various sensor nodes are autonomously accountable for governing their roles on a probabilistic methodology and the residual energy. All sensor nodes possess the same sensing and communicating capabilities [7] in the above mentioned conventional routing protocols .Due to the heterogenous features of the utilized IoT sensors, these protocols is not suited for subsequent generation IoT networks

The enormous measure of heterogeneous data originating from IoT devices/sensors is highly difficult to deal with which is the principle challenge involved in IoT networks. Cloud computing offers the best solution for offering flexible stack of storage, processing capacity, and different software services in a virtualized and accessible manner at consistent costs [8], [9].The utilization of restricted resources of wireless IoT networks is another brainy way to increase workload ,thereby maximizing the overall efficiency. Socially Aware Networking (SAN) is another new another worldview to abuse the social interactions among sensor hubs while concocting viable network arrangements. The new services and applications are created by collaborating individual nodes in IoT networks. In paper [10], the particular performance of the network is increased by utilizing the properties of Social IoT (SIoT).

In paper [11], cluster formation scheme is suggested for sorting the client groups by combining the network and social knowledge. The interactions among the devices and the energy level is not deliberated in the existing technique which is to be considered in future. While considering aa generic IoT based smart home architecture [12] shown in Fig. 2 ,there are two set (clusters) of installed smart devices namely appliance and monitor groups. Basically the partitioning of the entire IoT network is accomplished to form various disjoint clusters. The cluster head (CH) plays a main role which consist of various sensing nodes (devices) SNs as members in a cluster. The Process is as follows: SN in a cluster sends the detected information to the individual CH , the CH further sends information to the GWN and The GWN associates the outer world to the system through the Internet.On the off chance that a client (U) needs to get to a detecting hub SN comparing to a specific application in IoT, user needs to first send his/her login solicitation to the GWN. The GWN generally sends intermittently an inquiry message to the arrangement detecting hubs so as to gather the detecting data from them.

The crucial thing is that the cycle for gathering the data from sensing hubs which is not a real time which is an important criteria for captivating immediate actions along with decisions particularly in applications such as battle-field scenarios, healthcare, etc. Hence secure user authentication protocol for HIoTNs is mandatory for accessing the real-time sensitive information from the sensing nodes in the HIoTN by an authorized external party (user). As the detecting hubs are sent in an antagonistic domain, where the remote communication is uncertain, it represents a few dangers. The existing authentication protocols pose several security restrictions such as impersonation, sensing node capture, man-in-the-middle, replay and privileged insider attacks. This inspires us to strategy a progressively secure and reliable client verification conspire sent in HIoTN. The user authenticated key management protocol (UAKMP) is emphasized in [13] for scheming a new secure lightweight three factor remote user authentication.Still the more security is needed since the biometric itself didn't give exact results, so to increases the further security of the human involvement introduces a User Authenticated Biometric Key Management Protocol (UABKMP) which additionally improves exactness and productivity that outcome in monetary advantage.

Nevertheless, the constraints of unimodal biometric frameworks can be overwhelmed by fusing at least two wellsprings of biometric data called multimodel biometrics for setting up identity of client. It has also the capability to meet firm performance requirements levied by various applications. With this motivation, furthermore, the user must be legitimate by gain access to GWN and vice versa to provide further service. Both sides can established up a confidential session key for protected communication after effective authentication. The purpose of this significant problem, in the setting of HIoTN such as SMBUAKEP, is to manage a new multi-mode biometric temporary credential based lightweight user authentication system. However, this proposed protocol utilizes fuzzy commitment method for biometric multimodal verification. Thorough security testing by means of recognized security under the commonly used ROR model is performed, further formal security evaluation under the widely used software validation tool known as AVISPA, and informal security analysis show that SMBUAKEP is capable of resisting multiple identified attacks. The main contribution of the work is as follows:

- Initially, a novel efficient protocol for remote user authentication with iris and face biometric in HIoTN deployment is suggested called as SMBUAKEP.
- Cryptographic hash function is utilized which provides very efficient in addition to the symmetric encryption/decryption.
  Compared to these traditional methods of authentication, multimodal Biometrics based authentication is more convenient and faster. Spoofing is also eradicated which is difficult task for an attacker to spoof manifold biometric distinguishing features of a unpretentious user at once.
- In this multimodal biometric, the segmentation for iris is done using hybrid MBO, this method is implemented to select the Region of Interest of iris biometric images that is used for user authentication.
- For effective segmentation, dynamic template matching approach is employed.
- Next step involves the fuzzy commitment approach for biometric verification.
- Following the above, the ROR model is integrated for providing the formal security along with the informal security is also being done for exhibiting security of other potential attacks possible in the network.
- AVISPA tool is used at last for formal security verification by means of simulation to authenticate whether it is secure. The system architecture is given in Fig.1.

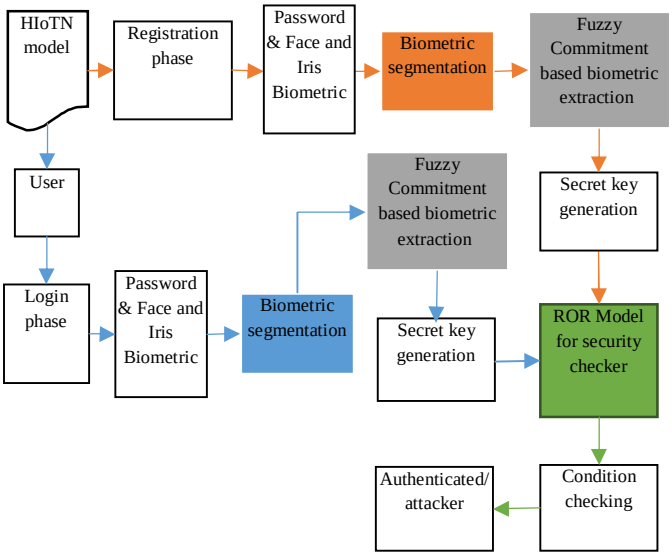



**Figure 1 :** Architecture Diagram for Secure Multimodal Biometrics-Based User Authenticated Key Exchange Protocol for generic HIoT networks

The paper is systematized as follows. Section 2 deliberates the most associated work with the secure protocol of IoTs. Section 3 designates the proposed method particulars. Section 4 deals with analysis and experimental results. Finally, Section 5 outlines the results and future scope.

## 2. BACKGROUND STUDY

He et al.[ 14] have established a shared authentication and a temporarily-related key agreement, which can effectively handle simulated user or sensor node attacks, anonymous attacks through offline code guessing and device assaults. Their scheme can be applied in WSNs in practice. But after monitoring attacks, insider's attacks and identity guessing attacks, this approach cannot be successfully accredited. To mitigate this issue , Jiang et al. [15] a new methodology namely link less enhanced authentication strategy. It is purely accountable for sensor node's problem and also energy consumption is also thereby reduced while defending against a series of security threats. The efficacy of WSNs and the safety factors in various environment is further improved by designing privacy-aware two-factor authentication scheme established on research outcomes of elliptic curve cryptography (ECC)[16] .

Amin et al. [17] improved the architecture of sensor network architecture and it concentrated on low-energy user authentication and key agreement system to achieve various factors such as two-way authentication dynamic addition of nodes and password updates for improving the session key protection. Choi et al. [18] uses a heuristic analysis paradigm to develop a user authentication protocol along with an ECC. This approach also reduces the WSN's energy consumption and additionally it achieves mutual authentication and key agreement between users and sensors. This strategy also prevents attacks such as session key attacks and sensor energy exhaustion attacks. In Sahingoz [19], the author presented a key strategy for distributed WSNs by means of management framework between sensor nodes and their neighbours by sharing the keys. Additionally multi-level dynamic key management is achieved by utilizing UAV which acts as management center of asymmetric key. In [20] three factor user authentication was used which accomplishes superior results in contrast with two factor user authentication strategy.

In this research, the various goals of the proposed methodology are 1)User and sensor hub mutual authentication 2)User's identity cannot identified by the attacker termed as anonymity 3) generation of session key once the authentication procedure is accomplished a session key should be generated shared by the user and the sensor node;4)The registered user's password and biometric template is not stored by the GWN.5)Resistant to various attacks 6) password update offline .The protocol which is proposed in this research is trivial and superior to the existing protocols with respect to the computational complexity.

## 3. PROPOSED METHODOLOGY

The architecture of generic IoT based smart home is shown in Fig. 1 in which the devices which are connected are segregated into two groups or clusters namely appliance group and monitor group. And the devices in the group are termed as agents. The communication is accomplished to the central controller by means of wireless medium. The user interface plays a vital role in controlling the smart home system. Furthermore central controller plays a vital role in monitoring the group by accessing the user information. But ,security is an main requirement to protect from several threats and attacks associated with HIoTNs [21].The connection between smart devices is accomplished through Internet via nearby gateway node (GWN).

Hence designing a secure user authentication protocol for HIoTNs is the essential thing for accessing the real-time sensitive information from the sensing nodes by an authorized external party (user).Various threats are possible since sensing nodes are organized in a hostile environment in an insecure wireless network. The various security limitations in major existing authentication protocols are impersonation, sensing node capture, man-in-the-middle, replay and privileged insider attacks. The above limitations inspires to strategy a more secure and reliable user authentication scheme organized in HIoTN.

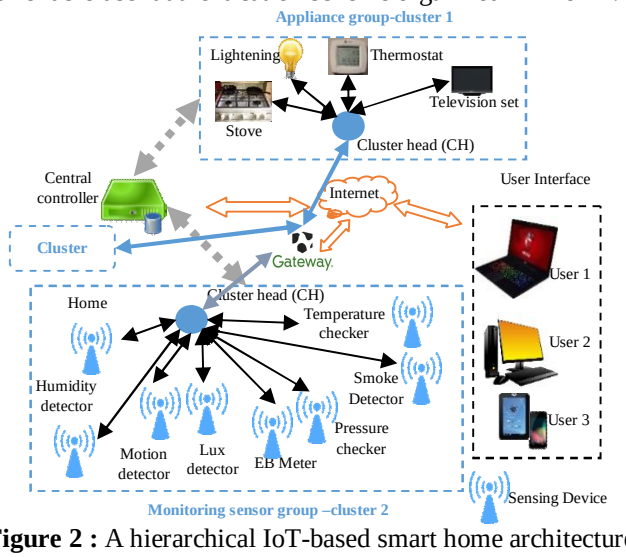



**Figure 2 :** A hierarchical IoT-based smart home architecture

### 3.1. Network Model

This section deals with the network model[22] for HIoTN shown in Fig.1 and the model is shown for a particular application for HIoTN. The hierarchial structure may vary based on various applications.There is only one gateway node (GWN) for each application. Also there is a resource-constrained sensing nodes ($SN_k$) ,resource rich cluster head nodes be ($CH_j$) and most powerful gateway node be (GWN) and also there exist hierarchy among GWN, CH and SN in this network model.Consider hierarchical IoT-based smart home application shown in Fig. 2 in which numerous sensing nodes are arranged (installed) for those applications in many disjoint clusters.The sensed information are transferred to the sensing node $SN_k$ in a particular cluster to its own $CH_j$, and the information is forwarded to the GWN. All sort of communication is accomplished through the wireless channels.

### 3.2. Secure Multimodal Biometrics-Based User Authenticated Key Exchange Protocol

In this section, we put forward the proposed level dependent authentication designed using Elliptic Curve Cryptography (ECC). In the proposed scheme, we assume that the gateway device is fully trusted and secure device. The proposed protocolconstructs six phases in it, namely 1) offline sensing node registration; 2) registration of each user; 3) Login for the user; 4) authentication & key agreement; 5) password & biometric update and revocation. The phases of SMBUAKEPare explained in further section.

**Offline Sensing Node Registration Phase:** The execution of offline sensing node registration is done through the gateway node (GWN). During registration process, the GWN indicates a 160-bit long random secret key K as a password for each deployed sensing node $SN_k$, and calculates the temporal credential of $SN_k$ as $TC_{SN_k}$. After that, the GWN stores the information $\{TC_{SN_k}, ID_{SN_k}\}$ into the memory of $SN_k$ prior to it is positioned in the target field of HIoTN, where $ID_{SN_k}$ is the $SN_k$'s identity and $TC_{SN_k}$is the temporal credential.

**User Registration Phase:**The registration process of a user $\mathbb{U}_i$ is mandatoryfor accessing the real-time information from the sensing nodes $SN_k$ at the GWN. The following are the steps for User Registration Phase

**Step 1- Password:** $\mathbb{U}_i$ picks a password $PW_i$ on user choice then a 128-bit random secret $r_a$, computes the masked password $MPW == h(PW_i||r_a)$. The registration request $\langle MPW_i \rangle$ is then transmitted securely to the GWN by $\mathbb{U}_i$.

**Step 2-Biometric:**In order to make sure the privacy and revocability of biometric data,a revocable template which is also known as cancelable template [23], utilized in biometric based system. The iris and face segmented biometric data is transformed into a revocable/cancelable template $C_{Ti}$ form by using a transformation function, say $f$ (.), with the help of a transformation parameter $TP_i$, that is, $C_T = f(SBIO, T_P)$.

After receiving $PW_i$ imprints his/her personal biometrics $BIO$of iris and face once $\mathbb{U}_i$ at the sensor of a particular terminal the segmentation of iris biometric images is done using Modified Bat Algorithm with Active Contour Model and face is segmented using Dynamic template matching approach. Further the resultant segmentedirisand face biometrics as $SBIO_i$is utilized in this work to generate the key, $PW_i$ is ready to calculate secret biometric key $K$ and public parameter $\tau_i$ with the help of the fuzzy commitment extractor probabilistic generation function ascancelable transformation function $f$(.).

A set of feature points ($SBIO_i$) captured from the segmented image of a user is used to generate $C_{Ti}$ with $TP_i$using $f(.)$. This canelable template is used in the implementation of the proposed authentication protocol. The detailed steps of the patient registration procedure are described as follows.

1) The patient generates a cancelable templates, that is, $C_{Ti} = f(SBIO_i, TP_i)$.

2) $\mathbb{U}_i$selects a key SK randomly and encodes SK into a codeword, KCW uses the error correction encoding technique Ψenc, that is, KCW = Ψenc(SK).

3) $\mathbb{U}_i$locks KCW with the cancelable biometric template CTi (i.e. $LTK_i = KCW \oplus C_{Ti}$ ). LTK is The helper data or locked key of the user $\mathbb{U}_i$

4) $\mathbb{U}_i$computes$PW_i = h(\mathbb{U}ID_i||SK||PW_i)$ and sends ($\mathbb{U}ID_i$, $PW_i$) along with a registration request to the Gateway node stores. $\mathbb{U}ID$is the user unique id.

5) The GWNstores all authentication parameters

6) $\mathbb{U}_i$computes$fi = h(\mathbb{U}ID_i||PW\ Di||C_{Ti})$ and stores $\{TP_i, LTK_i, h(K), f_i, f(.), \Psi enc(), \Psi dec()\}$ into GWN. $h(k)$is the one way hash function with secret key $K$and Ψenc(), Ψdec() is the encoding and decoding functions of error correction technique

### 3.3. Iris Segmentation Using Hybrid MBO for Generating Segmented Biometrics

Iris Segmentation is done using the Hybrid MBO for Generating Segmented Biometrics. The initialization of the changing contour, the encroachment of the contour convergence on the local minima, and the manual choice of internal energy weight parameters are the primary problems in the snake model, however. This results in the incorrect delineation of the region of concern resulting in the iris picture being incorrectly segmented. In this part, MBA has been used to solve some of the active contour model's (ACM) problems and to produce the precise segmentation of the biometric image input iris that is checked by the user's authentication process. The taken iris samples are given in Fig.2.

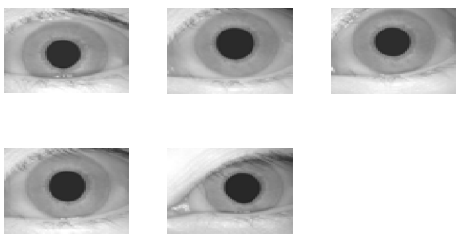
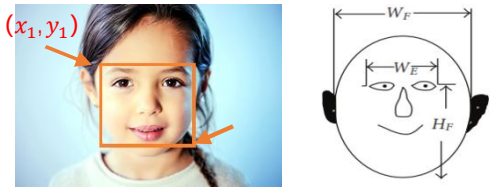


**Figure 2 :** Input Iris Sample

### 3.4. Dynamic template matching approach for Face segmentation

In real time, the challenging task is that the segmentation of face into uniform invariant shape and pose ,also that should be suitable for recognition. In the face identification system, the real time input from a web camera is crucial task in case of implementation. This research proposed a system to implement a face segmentation efficiently. Then fuzzy commitment approach is applied for biometric authentication.

The segmentation of face is accomplished by dropping a rectangle on the face image with top left corner coordinates $(x_1, y_1)$ and bottom right corner coordinates $(x_2, y_2)$ as shown in Figure 2. After which the region of face enclosed within this rectangle is segmented.




**(a)** **(b)**

**Figure 3 :** Example face: (a) Defining the face region by Rectangular boundary (b) Feature ratios defining sketch of face

The following are the facial features related by segmenting the face are given below :

(i) The ratio of two eye(E) distance (D) denoted by $D_E$ (extreme corner eye points) to the width(W) of the face F as $W_F$ excluding the ear regions as illustrated in Fig.2 (b)
ii) Following, the ratio of $D_E$ to the height (H) of the face$H_F$ from the centre of the line joining two eyes to the chin.
The ranges of the ratio$D_E / W_F$ is given by 0.62–0.72 and $H_F / D_E$is 1.1–1.3.
iii)Pruning of ears: Pruning of ears is nothing but the ear structure may vary from person to person. Some people may have big and prominently extending outwards and some of the may have less prominent. Hence it should be pruned for uniform face segmentation

**Defining rectangular boundary:**

Once the pruning is done ,the rest of the skintone area are encased in between two vertical lines. The left vertical (LV) and right vertical line (RV) outcorp on the x-axis gives $x_1$and $x_2$, respectively, as shown in Fig.2 and the width of the face $W_F$is

The localization of eyebrows and eye regions is accomplished to evaluate the value of $y_1$ for which template matching is done. A decent decision of the layout containing eyes alongside eyebrows ought to oblige varieties in outward appearances, varieties in basic segments, for example, presence or absence of facial hair and mustache, and division of countenances under shifting posture and scale by utilizing a couple of eyes as one inflexible article rather than singular eyes.

Dynamic template concept is introduced to avoid the fixed template size due to the dependability of the size of the face. The width of the layout containing eyes and eyebrows is resized corresponding to the width of the face $W_F$ keeping a similar angle proportion, Subsequent to finding the width of the face $W_F$. The resized format whose width is relative to the width of the face is the thing that we call a dynamic template. Therefore, dynamic templates $D_k$ with widths $W_k$ are constructed, where $W_k$ is given as in Eq.(1)

$$W_k = \gamma_k \times W_F \; \forall k = 1, 2, \ldots, 6 \tag{1}$$

where the range of $\gamma$ is between0.62 to 0.72 in steps of 0.02 keeping the same aspect ratio. . Thus, six dynamic templates $D_1, D_2, \ldots, D_6$ with widths $W_1, W_2, \ldots, W_6$are obtained. Consider $(x_d, y_d)$ and $Cr(x_d, y_d)$be the left corner coordinates of the dynamic template and correlation coefficient obtained by template matching when the top left corner of dynamic template $D_k$ is at the image co-ordinates$(x_d, y_d)$respectively.
The evaluation of correlation coefficient $Cr$ is as follows in Eq.(2)

$$Cr = \frac{\langle FI_T D_k \rangle - \langle FI_T D_k \rangle}{\sigma(FI_T)\sigma(D_k)} \tag{2}$$

Where $FI_T$denotes the patch of the face image $FI$ which must be matchedto $D_k$, $\langle\rangle$ is the average operator, $FI_T D_k$represents the pixelby pixel product, and $\sigma$is the standard deviation over thearea being matched. The face regions enclosed within the boundary of the rectangle formed using the coordinates $x_1$,$y_1$,$x_2$and the heights $H_{F_k}(k = 1, 2, \ldots, 10)$ are segmented and normalized to the size of the average face template. Some of the faces segmented and normalized by this process. From this centre point, height of the face $H_{F_k}$ is computed by

$$H_{F_k} = (1.1 + \beta) \times W_E^* \; \forall k = 1,2, \ldots ,10 \tag{3}$$

Where $\beta$ is a constant whose value ranges from 0 to 0.2 in steps of 0.02.

The face regions encased inside the limit of the rectangle shape framed utilizing the directions $x_1$,$y_1$,$x_2$ and the heights $H_{F_k}$ are segmented and standardized to the size of the normal face layout. For ongoing necessity, the mean and the variance of the average normal face format are processed early and utilized as constants for the calculation of the connection coefficient $\partial_k$ computed as in Eq.(4).

$$\partial_k = \frac{\langle BIO_j AF \rangle - \langle BIO_j \rangle \langle BIO_j AF \rangle}{\sigma(BIO_j)\sigma(AF)} \tag{4}$$

where $BIO_j$ is segmented and normalized face images, AF is the average face template, $\langle FI_{seg} AF \rangle$ represents the pixel by pixel product, and $\sigma$ is the standard deviation over the area being matched. The Height (number of pixels) of the face $H_{F_k}$ corresponding to the maximum correlation coefficient $\partial max = max(\partial_k)$, is added to the y-coordinates of the centre point between the two eyes to obtain $y_2$. Lastly, the face regions encased inside the rectangle formed using the coordinates $(x_1, y_1)$ and $(x_2, y_2)$) is segmented Finally, the face region enclosed within the boundary of the rectangle formed using the coordinates $(x_1, y_1)$ and $(x_2, y_2)$) is segmented. The

input image sample of face is illustered in Fig.4. The full process if $BIO_j$ segmentation is illustrated in Fig.5.

**Figure 4 :** Input Facial image sample

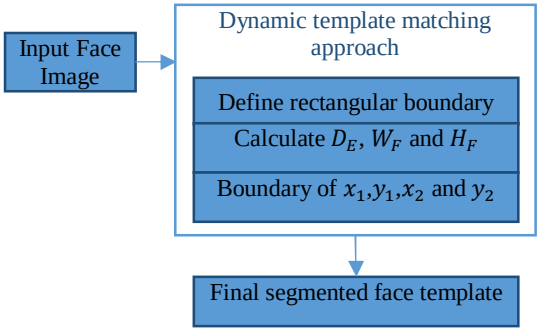



**Figure 5 :** Face segmentation for generating $SBIO$

**Fusion Module**

In this, various sensors are used for extracting the multimodal biometric system employing image fusion usually images in a single attribute. Also there is dependency in the features extracted from these images and merging of these features can be done into single vector which is supposed to have has high dimensionality and represents identity in different space. Additionally feature vector can be still diminished using feature reduction technique. This kind of Feature combination is commonly utilized when list of capabilities are homogenous. Here another unique technique for combination is been proposed in which face and iris pictures are melded as list of capabilities got from iris and face pictures are contradictory, non-homogenous and connection between them isn't known . The outputs of feature extraction modules are sub images (XX band) of original face and iris images. The DWT coefficient of each face XX subsample and iris XX subsample are fused together and generate fused segmented biometrics (SBIO). From this fused image one dimensional vector is extracted which is treated as a single template vector.

### 3.5. Fuzzy commitment approach

In this research, multi-server authentication protocol is expected to design using fuzzy commitment approach for biometric verification. The fuzzy commitment technique which is greatly utilized in biometric-based remote authentication. It is utilized to verify biometrics attributes signified in binary vector. The main merit is that compact size of the sketch. Let the selected biometric format is a n-bit paired string. A consistently irregular key of length l bits is produced and used to solely record a n-bit codeword of appropriate suitable error correcting code. The sketch is then separated from the layout. Toward the end sketch is put away in the database. We utilize a cancelable biometric format and a error correction strategy in this approach and also to reinforce our plan. The error correction technique is embraced alongside the fuzzy commitment scheme to deal with the boisterous biometric signal. Moreover, we utilize the timestamp and the arbitrary nonce to make our plan strong to the replay and man-in-the-center assaults [24].

#### 3.5.1. Login Phase

Following the registration procedure, a user $U_i$ is now equipped to login in the structure using the following steps:

Step 1: After the identity, password are entered and biometric information $(SBIO_i')$at the sensor node are imprinted by each user, a cancelable template $C'_{Ti}$ from query $SBIO_i'$using transformation function f(.) and transformation parameter $TP_i$, that is, $C'_{Ti} = f(SBIO_i', TP_i)$

Step 2: GWN unlocks $K'_{CW}$ with $C'_{Ti}$ and decodes it to regenerate the key $K'$ as follows: $K' = \Psi dec(LTK_i \oplus C'_{Ti}) = \Psi dec(K'_{CW})$

Step 3: GWN checks $h(K') \neq h(K)$ rejects the session immediately. Otherwise it continues.

Step 4: $\mathbb{U}_i$ enters the identity of an accessed sensing node $N_k$, where after choosing one time secret $x_1$ and current timestamp $T_1$, compute

$M_1 = E_{TC_{\mathbb{U}_i^*}}(x_1, ID_{SN_k}), M_2 = h(x_1||PW_i||ID_{GWN}||ID_{SN_k}||T_1)$.

Finally the login request message will be $\langle PW_i', M_1, M_2, T_1 \rangle$ is then transmitted publically.

#### 3.5.2. The Biometric Template Revocation Phase

The biometric template plays a main role in any biometric based security system for higher protection of the system. Below is the procedure for biometric template update.

1) Scanner is used to capture a new instance of a biometric image of the User $\mathbb{U}_i$ and thereby extracting the unique features from the newly captured biometric image such face and iris.Let the the segmented feature set is represented by $(SBIO_i')$ .

2) The $\mathbb{U}_i$provides $\mathbb{U}ID_i$, PWi along with $(SBIO_i')$for successful login.

3) The GWN computes $C'_{Ti}$from $(SBIO_i')$ using f(.) and $TP_i$.

4) After successful login, the user$\mathbb{U}_i$ provides a new transformation parameter $T_{Pi}^{new}$.

5) The GWN computes the following:

$C_{Ti}^{new} = f(SBIO_i', T_{Pi}^{new}), LTK_i^{new} = LTK_i \oplus C'_{Ti} \oplus C_{Ti}^{new}, f_i^{new} = h(\mathbb{U}ID_i||PW_i||C_{Ti}^{new})$

6) The GWN replaces $LTK_i$ and $f_i$ with $LTK_i^{new}$and $f_i^{new}$, respectively.

### 3.5.3. Authentication and Key Agreement Phase with ROR model

Once the login request message is received from section 2.1.3 the following steps are taken place to accomplish the authentication and session key SK instituting between $(\mathbb{U}_i, SN_k)$ through GWN.

Step 1: Checking the condition that $|T_1 - T_1^*| \leq \Delta T_1$, where $\Delta T_1$ is the maximum transmission delay. After that the decryption of $M_1$ is done using temporal credential $TC_{U_i}$ and stored in a database.

Step 2: The GWN is computes $M_3$ as in and checks $M_3 = M_2$. If condition is met the new $TempID_{SN_k}$ is generated else the session stops instantly and calculates $M_4$ and transmits via $CH_j$

Step 3: After receiving $M_4$ at time $T_2^*$ and check $|T_2 - T_2^*| \leq \Delta T_2$, where $\Delta T_1$ is the maximum transmission delay, if condition is met the $M_4$will be decrypted and checks $M_3 = M_2$. Else the connection ceases instantly and choosing one time secret $x_2$and current timestamp $T_3$, compute $M_7, M_8 and\ M_9$ as in tehn $SN_k$ sends the authentication reply message to GWN.

Step 4: Do the step of 1 to 3, the messages can be retransmitted thrice the retrials.

Step 5: A validate client has the privilege to bring up-to-date password as well as biometric information at any time entirely locally without concerning the GWN as and when it is required.

STEP 6: Security checking for the authentication process will be done using SMBUAKEPbased ROR model. $SN_k$, $\mathbb{U}_i$ and GWN are the three main participants involved in the network. Beneath this model, all the communications can be controlled by adversary $A$containing the interpretation and amending all the transmitted messages, and also fabricating new messages as well as injecting them.

STEP 7: On receipt of $\{M_9\}$, server computes $h(h(\mathbb{U}_i)||SK_{ji})$ and validates its equality with the received value $M_9$. The successful verification implies that no replay or forgery is executed and $\mathbb{U}_i$ is authenticated finally.

**User's Key Change Phase:** The proposed convention is that the client's key can be changed by re-enlistment process. At the point when the key is undermined, $\mathbb{U}_i$ can do reenrollment by his/her biometric, and afterward another key is created arbitrarily; this key varies from the past.

**Security Analysis**

The importance of the suggested protocol in terms of safety is emphasized here. The threat model is used in communication networks to officially evaluate crypto protocols, as the threat model assumes that two parties can interact through an unsafe channel. HIoTNs can receive a risk model where the communication channel between two parties is risky and end points (detecting hub and client) can't as a rule be trusted[25].

**DoS attack :** The proposed convention is impervious to a DoS assault by pre-confirmation, as every application ought to be related with timestamp T_1 encoded by the $\mathbb{U}_i$'s key; thus, an enormous number of unapproved demands can't get into the GW hub.

**Node compromise attack**

The use of the client is first validated by the GW hub by the recommended convention which opposes a node bargain assault. After validation, the application is moved to the hub of the sensor to answer the client question. The replay assault are forestalled by utilizing the timestamps $Ti$in the proposed convention. On the off chance that an enemy blocks the message$E_K(R, T_1)$ and tries to repeat the same login message to the GWN, the login demand check due to (T_2− T_1) > $\Delta T$, where T_2 signifies when the replayed message is acknowledged by the GWN.

**Repudiation attack**

The repudiation attack is nothing but the communication participation denial wherever communication involves. U_i's iris is needed to redevelop the $\mathbb{U}_i$'s key in this research, in this manner, the U_i can't deny that he/she has taken an interest with a specific goal in mind;the recommended convention opposes repudiation assaults since we likewise assume that the GW hub is considered a hub of trust;

**A stolen verifier attack:** The client keys have been encoded in the GW node database due to the reason that any supportive data is not obtained by the attackers who have stolen GW node.

**Node Capture Attack**: The entity selects a random value in the communication authentication process to produce a session key that will be discarded at the end of the session.

**Replay Attacks**: f a malicious attacker gets a session key or captures HIoTN's network traffic, it is not valid for the session key to recognize malicious visitors and authenticate their identity. Due to illegal identity, resend message will be discarded.

**Biometric Template Protection:** In this research, cancellable template is obtained by transforming the biometric data and inhibiting the confidentiality of the biometric data of an authorized registered user. To be protected, the template is not stored anywhere. The information on the client explicit arbitrary number $Rc_i$ plays a vital role which is computationally infeasible from the Biometric template extraction from a lost or stolen smart card of a user. Along these lines, the client biometric template is secured in the proposed system.

## 4. EXPERIMENTAL RESULTS AND DISCUSSION

In this research, operating system Ubuntu 16.10 is utilized and we exhibited significant parameters in Table 1. Each pair of neighbor sensors is separated with the distance of 20 m and the sensor set is arranged in grid manner. Every step carries 20 to 120 sensors with step size of 20.Only one HGWN is involved in the simulation and thereby communication is accomplished

between the users and sensors. The test involves almost 50 users and the speed involved is 2 m/s, in a 400×300 $m^2$area.On the whole, every client sends a packet in each 4s and the simulation time is 1800s. Furthermore, the presented SMBUAKEPscheme is evaluated by performance comparison with existing schemes of UABKMP and UAKMP. Also, the NS-2 is greatly utilized for analysis purpose and various parameter metrics such as throughput, end-end delay, packet delivery ratio, communication overhead are analysed.

**Table 1 :** Elementary factors in simulation

| Description | Value |
|---|---|
| SensorsArea | 400×100 $m^2$ |
| Number of users | 50 |
| Number of sensors | 120 |
| User speed | 2 m/s |
| UsersArea | 400 × 300 $m^2$ |
| Time forSimulation | 1800 s |

### 4.1. Packet Delivery Ratio (PDR)

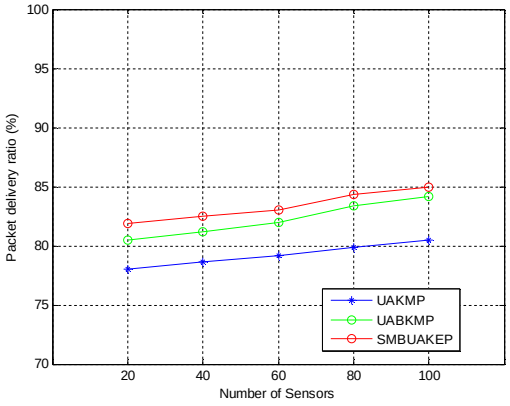



**Figure 6 :** Packet Delivery Ratio vs. No. of sensors

Fig. 6 illustrates the packet delivery ratio with respect to number of sensors, which is defined as the ratio of the number of delivered and transmitted message to the user. The Packet delivery ratio simply portrays state of message sent to the destination node.

The proposed SMBUAKEP have a higher packet delivery ratio when contrasted with the UABKMP and UAKMP approach. From the figure, the appropriate delivery ratio also increases gradually, when number of sensor increases. The graph infers that when the number of sensor value is 100 and corresponding PDR of UABKMP is 84.2%, UAKMP is 80.5% and proposed workSMBUAKEP has 85% that indicates the proposed work is more effective for HIoTN. The effectiveness of the proposed protocol can counter attack various known attacks and also adds supplementary functionality features when contrasted with other schemes with the added feature of less computational cost. The numerical results of Packet delivery ratio is given in Table.2.

**Table 2 :** Numerical Results of Packet delivery ratio

| Methods | Packet delivery ratio Comparison | | | | |
|---|---|---|---|---|---|
| Number of sensors | 20 | 40 | 60 | 80 | 100 |
| UAKMP | 78 | 78.6 | 79.2 | 79.9 | 80.5 |
| UABKMP | 80.5 | 81.2 | 82 | 83.4 | 84.2 |
| SMBUAKEP | 81.9 | 82.5 | 83 | 84.3 | 85 |

### 4.2. Throughput (TP)

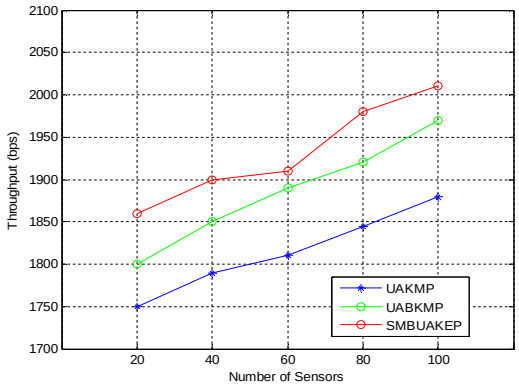



**Figure 7 :** Throughput vs. No of sensors

The throughput vs. No of sensors is shown in Fig.7 and the proposed SMBUAKEP is contrasted with prevailing UABKMP and UAKMP method. It is noted that the proposed SMBUAKEPattains higher throughput when compared with existing UABKMP and UAKMP. Whenever the nodes count increases, which also improve the throughput performance by the nodes. The proposed SMBUAKEPhas throughput rate of 2010bps at the sensor size of 100 when comparing with existing UABKMP and UAKMP providing low throughput results which is 1970bps and 1880bps lesser than the proposed method respectively. The updating of password and biometric template in its memory nearby deprived of communicating the RC is the main reason behind. Thus, the password/biometric template update procedure is efficiently executed.Which is through the proposed method has throughput.The numerical results of Throughput is given in Table.3.

**Table 3:** Numerical Results of Throughput

| Methods | Throughput | | | | |
|---|---|---|---|---|---|
| Number of sensors | 20 | 40 | 60 | 80 | 100 |
| UAKMP | 1750 | 1790 | 1810 | 1845 | 1880 |
| UABKMP | 1800 | 1850 | 1890 | 1920 | 1970 |
| SMBUAKEP | 1860 | 1899 | 1910 | 1980 | 2010 |

### 4.3. End-To-End Delay (EED)

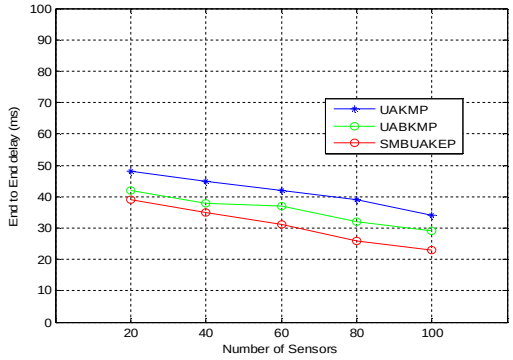



**Figure 8 :** End to End Delay vs. No of sensors

The End to End Delay vs. No of sensors is shown in Fig.8 and the proposed SMBUAKEP is contrasted with prevailing UABKMP and UAKMP method. Whenever the nodes count increases, which also which also decreases the delay by the nodes, while comparing with the existing methods. The proposed SMBUAKEPhas delay rate of 23ms at the sensor size of 100 when comparing with existing UABKMP and UAKMP providing high delay results of 29ms and 34ms higher than the proposed method respectively. In proposed work, the secret key value of a sensor node is calculated using the ROR model at each layer with respect to the attacks. Through this without knowing the secret credentials, the opponent cannot update the password which is computationally difficult chore.This leads to the proposed work have lesser end-end delay when compared with the existing work.The numerical results of EED is given in Table.4.

**Table 4 :** Numerical Results of EED

| **Methods** | **End to End Delay** | | | | |
|---|---|---|---|---|---|
| Number of sensors | 20 | 40 | 60 | 80 | 100 |
| UAKMP | 48 | 45 | 42 | 39 | 34 |
| UABKMP | 42 | 38 | 37 | 32 | 29 |
| SMBUAKEP | 39 | 35 | 31 | 26 | 23 |

### 4.4. Communication overhead

End to end delay is defined as the total time taken to complete the successful data transmission.

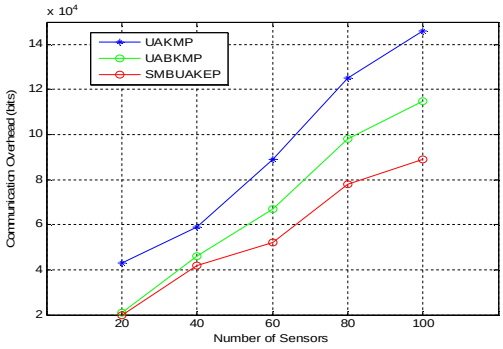



**Figure 9 :** Communication overhead vs. No of sensors

The communication overhead is contrasted with the proposed SMBUAKEP and existing UABKMP and UAKMP scheme. The proposed SMBUAKEP has the communication overhead value of 89000bits. The UABKMP method has communication overhead rate of 115000bits at the sensor rate of 100. When comparing the communication overhead rate of existing UAKMP providing high results of 146000bits at same senor rate. The significance of the proposed research is that lower communication overhead with the prevailing methods.The numerical results of communication overhead is given in Table 5.

**Table 5 :** Numerical Results of Communication Overhead

| **Methods** | **Communication Overhead** | | | | |
|---|---|---|---|---|---|
| Number of sensors | 20 | 40 | 60 | 80 | 100 |
| UAKMP | 43000 | 59000 | 89000 | 125000 | 146000 |
| UABKMP | 21000 | 46000 | 67000 | 98000 | 115000 |
| SMBUAKEP | 20000 | 42000 | 52000 | 78000 | 89000 |

## 5. CONCLUSION AND FUTURE WORK

In this research, suggested a new Secure Multimodal Biometrics-based User Authenticated Key Exchange Protocol for HIoTs environments utilizing a multimodal biometric-based fuzzy commitment approach. The Fuzzy commitment Approach aids in error correction from noisy biometric information. The various security administrations such as privacy protection of client's identity and biometric information, shared verification and session key foundation among client and sensor hub facility of any time password updating and biometric data revocation without interacting with the RC and server are dealt in this research. The proposed technique opposes disavowal of administration assaults by means of early error identification mechanism during login.

The hash function and fuzzy commitment scheme is greatly utilized by fulfilling the computational intricacy and overhead necessities during login and levelling out the mutual authentication and session key agreement procedures. The demonstration of proposed plan security is achieved through proper security appraisal utilizing the ROR model, informal (non-mathematical)security investigation, and formal security check utilizing the AVISPA simulation tool. Conversely ,the proposed methodology has the ill effects of cyber-attack and single point of failure and these limitations can be elucidated by means of utilizing Blockchain. This block chain can fortify the security of IoT by enlightening the system self-protection by shielding basic security-related information.

## REFERENCES

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A

survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, Fourth quarter 2015. https://doi.org/10.1109/COMST.2015.2444095

2. S. K. Sharma, T. E. Bogale, S. Chatzinotas, X. Wang, and L. B. Le, "Physical layer aspects of wireless IoT," in Proc. IEEE ISWCS, Sept 2016, pp. 304–308.
3. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
4. M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless- and mobility-related view," IEEE Wireless Commun., vol. 17, no. 6, pp. 44–51, Dec 2010.
5. H. Shin, S. Moh, I. Chung, and M. Kang, "Equal-size clustering for irregularly deployed wireless sensor networks," Wireless Pers. Commun., vol. 82, no. 2, pp. 995–1012, 2015. https://doi.org/10.1007/s11277-014-2262-5
6. S. P. Singh and S. Sharma, "A survey on cluster based routing protocols in wireless sensor networks," ProcediaComput. Sci., vol. 45, pp. 687– 695, 2015.
7. A. Bagula, A. P. Abidoye, and G.-A. L. Zodi, "Service-aware clustering: An energy-efficient model for the internet-of-things," Sensors, vol. 16, no. 1, p. 9, 2015.
8. M. M. Hassan, H. S. Albakr, and H. Al-Dossari, "A cloud-assisted internet of things framework for pervasive healthcare in smart city environment," in Proc. of EMASC. ACM, 2014, pp. 9–13.
9. S. K. Sharma and X. Wang, "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," IEEE Access, vol. PP, no. 99, pp. 1–1, 2017. https://doi.org/10.1109/ACCESS.2017.2682640
10. A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, "The cluster between internet of things and social networks: Review and research challenges," IEEE Internet Things J., vol. 1, no. 3, pp. 206–215, June 2014.
11. G. Zhang, K. Yang, and H. H. Chen, "Socially aware cluster formation and radio resource allocation in D2D networks," IEEE Wireless Commun., vol. 23, no. 4, pp. 68–73, Aug 2016.
12. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," IEEE Internet of Things Journal, 2017.
13. Wazid, Mohammad, Ashok Kumar Das, VangaOdelu, Neeraj Kumar, Mauro Conti, and Minho Jo. "Design of secure user authenticated key management protocol for generic iot networks." IEEE Internet of Things Journal 5, no. 1 (2017): 269-282. https://doi.org/10.1109/JIOT.2017.2780232
14. He, D.; Kumar, N.; Chilamkurti, N. (2014): A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. International Symposium on Wireless and Pervasive Computing, pp. 263-277.
15. Jiang, Q.; Ma, J.; Lu, X. (2015): An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070-1081.
16. Jiang, Q.; Kumar, N.; Ma, J. (2016): A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. International Journal of Network Management, vol. 27, no. 3, pp. 254-160.
17. Amin, R.; Biswas, G. P. (2015): A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, vol. 36, pp. 58-80.
18. Choi, Y.; Lee, D.; Kim, J. (2014): Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, vol. 14, no. 6, pp. 10081.
19. Sahingoz, O. K. (2013): Large scale wireless sensor networks with multi-level dynamic key management scheme. Journal of Systems Architecture, vol. 59, no. 9, pp. 801-807. https://doi.org/10.1016/j.sysarc.2013.05.022
20. Park, Y.; Park, Y. (2016): Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks: Sensors, vol. 16, no. 12, pp. 2123.
21. El-Hajj, M., Chamoun, M., Fadlallah, A. and Serhrouchni, A., 2017, October. Analysis of authentication techniques in Internet of Things (IoT). In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-3). IEEE.
22. A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646 – 1656, 2012.
23. Arya, K. V., and Saurabh Singh. "Generating cancelable fingerprint using drawing code." In Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011) December 20-22, 2011, pp. 189-195. Springer, New Delhi, 2012.
24. Aaron Don M. Africa, Patrick Bernard T. Arevalo, Arsenic S. Publico and Mharela Angela A. Tan, " Fuzzy Logic Control System with Gaussian Membership Functions" International Journal of Emerging Trends in Engineering Research,Volume 7 No. 9, 2019. https://doi.org/10.30534/ijeter/2019/16792019
25. Prevesh Kumar Bishnoi and Dr. Dharmender Kumar, "Cloud Based Electrical Device Control Middleware APIs for IoT", International Journal of Emerging Trends in Engineering Research, Volume 8, No. 2 2020. https://doi.org/10.30534/ijeter/2020/34822020