HISTOGRAM OF NEIGHBORHOOD TRIPARTITE AUTHENTICATION WITH FINGERPRINT-BASED BIOMETRICS FOR IOT SERVICES

S. Kanchana

Department of Computer Science, PSG College of Arts & Science, Coimbatore, India

ABSTRACT

Internet of Things (IoT) and services is an interesting topic with a wide range of potential applications like smart home systems, health care, telemedicine, and intelligent transportation. Traditionally, key agreement schemes have been evaluated to access IoT services which are highly susceptible to security. Recently, Biometric-based authentication is also used to access IoT services and devices. They are involving a larger amount of memory with increased running time and found to be computationally infeasible. To provide robust authentication for IoT services, Histogram of Neighborhood Tripartite Authentication with Fingerprint Biometrics (HNTA-FB) for IoT services is proposed in this paper. This proposed HNTA-FB method uses binary patterns and a histogram of features to extract the region of interest. To reduce the memory requirements while providing access to IoT services, Histogram of Neighborhood Binary Pattern Pre-processing (HNBPP) model is proposed. The discriminative power of Neighbourhood Binary Pattern Registration (NBPR) is integrated with the normalized sparse representation based on the histogram. Additionally, this work presents a new Tripartite User Authentication model for fingerprint biometric template matching process. When compared with different state-of-the-art methods, the proposed method depicts significantly improved performance in terms of matching accuracy, computational overhead and execution speed and is highly effective in delivering smart home services.

KEYWORDS

Binary Patterns, Fingerprint Biometrics, Histogram, Internet of Things, Neighborhood Tripartite Authentication.

1. INTRODUCTION

The emergence of Internet-of-Things (IoT) paradigm permits advanced opportunities for medical devices with wireless connectivity, by facilitating monitoring of data and also the management of data in a un-interruptive manner. Munish Bhatia et al. investigated an intelligent healthcare framework based on IoT to ensure ubiquitous healthcare to the patient during his/her workout sessions [1]. Real-time health-oriented and non-health oriented attributes are acquired using several IoT devices, in the data accumulating layer. In the data categorization layer, the attributes have been acquired using several IoT devices were transmitted wirelessly to cloud storage.

Next, the data abstraction layer performed mining using temporal mining using the attributes and further quantified it in the form of a probabilistic parameter, called as Probabilistic State of Vulnerability (PSoV).

Finally, PSoV was utilized to train using back propagation ANN to ensure healthcare services in a un-interruptive manner during exercise sessions. With this, the accuracy of IoT-assisted smart workouts was said to be improved with high rate of statistical measurements for efficiency and accuracy. However, the running time consumed to facilitate IoT-assisted smart workouts was not concentrated. One of the fields that have experienced notable research attention for user authentication in IoT devices and services is by biometric features. Biometric identifiers depend on either physiological or behavioral patterns. This facilitates access through the smart device by the user from anywhere, anytime and anyplace which causes security-critical to IoT. A lightweight Biometric-based remote user authentication and key agreement scheme, called Multi-factor biometric user authentication was proposed for secure access to IoT services [2].

The security aspects were proved to be robust against multiple security attacks. Four different phases such as user registration, login, authentication and password change were used. Multi-factor biometric user authentication used only one-way hash, perceptual hash, and XOR operations and found less expensive [3]. Though security was said to be improved, the memory requirements to perform multi-factor biometric user authentication for IoT services was not concentrated. A vision-based hand gesture recognition model was investigated for the Internet of Things to provide a high-security system [4]. The design included edge segmentation and gesture estimation modules. With these two modules, security was said to be ensured. However, measures were not taken to safeguard against prominent attacks.

Biometric-based authentication and key agreement scheme were investigated it not only reduced the communication overhead but also minimized the computation cost involved [5]. However, existing security mechanisms, such as vision-based recognition model based on biometric along with gesture recognition model may not be efficient and reliable for providing secure communication solutions between devices in IoT. To this end, an end-to-end secure IoT-based solution was investigated with the aid of biometrics and pairing-based cryptography [6].

As the biometric features like face, fingerprint, iris and so on are unique, a biometric-based security solution is less susceptible to security breaches for IoT infrastructure. The computational cost multi-factor authentication model using Burrows-Abadi-Needham logic [7] was found to be higher. Extreme Learning Machine was applied to extract facial emotions to improve recognition accuracy [8].

A security layer between IoT and users for smart cities using ECG and fingerprint biometric authentication was proposed [9]. With these two traits, security aspects and improved equal error rate were also addressed. However, the accuracy with error rate was remained unaddressed. To provide solution to this issue, ECG-based Continuous Authentication system was designed [10]. To provide security in cloud-based IoT, quantum resistance signature schemes were applied [11]. However, the computational cost and memory was found to be compromised with increasing features.

To resolve these aforementioned problems, a fingerprint-based biometric authentication model for IoT-based services is presented to ensure the confidentiality of sensitive IoT devices. IoT gateway node tries to authenticate the user with the fingerprint biometric received from the user and the hand fingerprint template saved during the registration phase. Finally, user and IoT gateway node was made to achieve the mutual authentication. Our method achieves stronger security and shows improved performance on the communication overhead with minimum running time. The remaining part of this paper is organized as follows. Section 2 reviews the biometric authentication methods to access IoT services. Section 3 describes the proposed HNTA-FB method in detail. Section 4 provides the performance evaluation of the proposed methods compared with the state-of-the-art methods. Finally, Section 6 presents the conclusion.

2. RELATED WORKS

Research efforts have been dedicated to the construction of more precise, usable and secure biometric authentication mechanisms. Feature de-correlation algorithm was designed for analyzing security aspects along with mechanisms to combat against several attacks [12]. Jun Xu et al. proposed hand gesture recognition method using pictorial structure and edge information for ensuring accuracy under complex backgrounds, but interoperability rate and flexibility was said to be compromised. To resolve these issues, semantic-based IoT information services was designed to address security aspects and scalability for open IoT service platform [13].

To provide flexibility, a Network Function Virtualization (NFV) method was presented based on the Representational State Transfer (REST) architecture [14]. When considering communication between IoT devices, security is one of the major aspects to be addressed. Multi-layer parameters were introduced by Paul Loh Ruen Chze and Kan Siew Leong lessens resources with minimum routing information [15]. As a result, secure multi-hop routing was said to be ensured. Similarly, uniform access mechanism for heterogeneous things was provided using Field Programmable Gate Array (FPGA) and System on Chip (SoC)[16].

One of the biggest challenges for IoT access is facing two risks namely, safety threats and privacy violations. To provide the solution to address these risks, the survey of advanced algorithms using genetic programming, fuzzy set theory was designed by Jong Hyuk Park and Neil Yuwen Yen [17]. A comprehensive review of multi-biometric fusion methods for accessing IoT services was investigated [18]. However, the authentication accuracy was not concentrated. To address these complications, a novel authentication framework was designed using device-specific information [19]. In this paper, we present a biometric binary pattern representation and authentication method for IoT services using the fingerprint features with minimum computational time and overhead.

3. PROPOSED METHODOLOGY FOR BINARY PATTERN REGISTRATION AND AUTHENTICATION

A Histogram of Neighborhood Tripartite Authentication with Fingerprint Biometrics (HNTA-FB) for IoT services of human individuals is introduced by extracting the fingerprint features to the IoT network domain area. The system model description is preceded by elaborate description is provided in the follow ing sections.

3.1 Proposed framework

Initially, data model of the proposed HNTAFB method using Star IoT Network (SIN) is designed. The advantage of star IoT network is that all the complexity in the design of the network is managed by a central node or IoT Gateway Node '$\boldsymbol{GN}$'. The model of SIN involves an IoT gateway node through which the users are connected to perform several activities. All the other nodes only need to communicate in their time slot based on Time-Division Multiple Access (TDMA) basis. Figure 1 shows the system model using SIN.

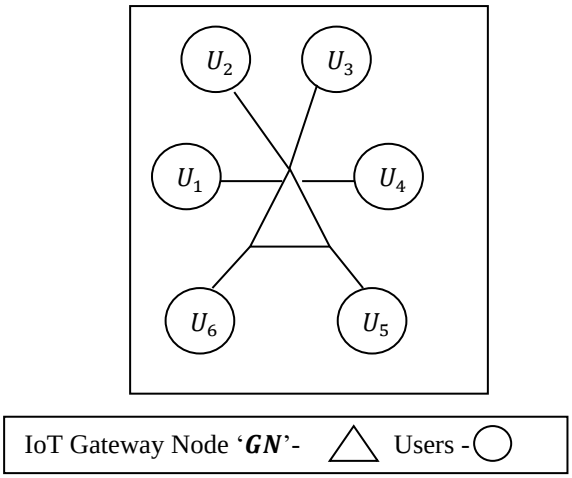

Figure 1. Star IoT Network

As shown in figure 1, SIN in the proposed method comprises a set of entities representing the set of users connected with the aid of a relationship set 'SIG'. The relationship set is mathematically formulated as given below.

$$SIG \rightarrow (U, R, C) \tag{1}$$

From (1), the star IoT graph 'SIG' in the proposed method comprises the set of users 'U', with the relationship set denoted as 'RS' and relational coefficient denoted as 'C' respectively. Each user 'U' is defined as below.

$$U \in U_i \quad (2)$$

$$U_i \rightarrow U_i \cup fp_1, fp_2, \ldots, fp_n \quad (3)$$

From (3), 'U_i' represent the set of users, where, 'FP_i' represent a fingerprint attribute of the user with fingerprint feature sets 'fp_1', 'fp_2' and so on extracted at different time settings 't_1', 't_2' respectively. The relationship set in the method is represented as '$RS\{U, I\}$' in the IoT setting, where 'U' represents the nodes or users and 'I' corresponds to the relationship or interactions that connect between the users and IoT devices. Here, the nodes or users are represented as points whereas the interactions between the users and IoT devices are presented as lines. Besides, the coefficient value 'C' symbolize$\{U_i\} * U \rightarrow r, where\ r \in RS$' corresponds to a function that assigns a relationship type 'r' between a given user, 'U_i' and IoT services.

3.2 Problem formulation

Let us consider a network environment of 'n' users and '$\gamma^1, \gamma^2, \ldots, \gamma^n$' templates of the '$n\ users$' in a biometric system for IoT services. Let us further assume that the 'n' users communicate with the IoT devices via IoT Gateway Node 'GN' using fingerprint as a biometric modality to provide an effective user authentication scheme for IoT services in a safe and controlled environment of the biometric system. Hence, the nth user template is of the form '$\varphi^n = \{\gamma_1^n\}$' consists of single units where 'γ_1^n ' denote the templates for fingerprint. Our objectives are defined by designing an IoT smart home network setting. An IoT Gateway Node is introduced along with the fingerprint biometric features of human individuals to measure the authenticity of the user and access IoT services.

3.3 Proposed method

In this section, a methodology for an effective security scheme in smart home IoT devices via fingerprint technique is investigated. Figure 2 represents the proposed method, Neighborhood Tripartite Authentication with Fingerprint Biometrics (HNTA-FB) for IoT services. HNTA-FB method is used as an authentication scheme for smart home monitoring by IoT device. To address security issues in IoT via biometrics using fingerprint as a modality, three steps are followed. They are user registration or feature extraction, preprocessing and matching or authentication.

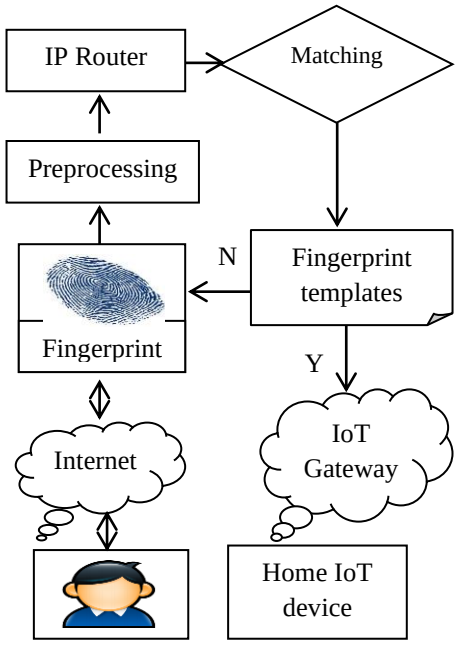

Figure 2. Block diagram of HNTA-FB for IoT services

As shown in figure 2, the user accesses the IoT devices through IP router, the system authorizes and validates the user through fingerprint images which are stored as templates. If the user fails to authorize him/her through fingerprint recognition as stored in templates. This fingerprint module can be integrated with different types of sensors like automated door lock, different electronic devices, security devices and so on. In system implementation, a biometric fingerprint security model is developed for smart home monitoring.

3.4 Neighborhood Binary Pattern Registration (NBPR) model

The proposed HNTA-FB method initially performs user registration with user node, gateway node 'GN' and IoT nodes or IoT devices. To register fingerprint features, a unique ID is generated for each user. Along with the registration between the user node, gateway node and IoT nodes, the user's biometric fingerprint features are extracted. It is denoted by 'ID_u', for a user 'u'. Similarly, any number of users registers their fingerprint in the biometric system and obtains a unique ID. Multiple fingerprint impressions of the same user are obtained and stored. Besides, the fingerprint feature registration in the proposed method is performed with the help of minutia features. A minutia for fingerprint impression is symbolized as below.

$$M = (P, Q, \theta) \qquad (4)$$

From equation (4), the minutia features 'M' are obtained for each user 'U_i' both using the location information '(P, Q)' and direction 'θ' information respectively. In this work, user

registration for the biometric fingerprint is performed using Neighborhood Binary Pattern Registration (NBPR) model. Each neighborhood pixel for the corresponding location information is represented as a binary pattern and is denoted by two bits. In binary patterns, the two bits is Most Significant Bit to represent the flag symbol and Least Significant Bit to represent the magnitude. The pseudo-code representation of the Neighborhood Binary Pattern Registration (NBPR) is given below.

Input: user node '$U = U_1, U_2, \dots, U_n$', gateway node 'GN' and IoT nodes or IoT devices '$D = d_1, d_2, \dots, d_n$', fingerprint impressions 'FP_i',
Output: Registered values '$RV(i,j)$'
1: Begin *2:For each user node 'U' with gateway node 'GN';IoT devices 'D' fingerprint impressions 'FP_i'* *3:Obtain minutia for fingerprint impression using (4)* *4: Obtain flag bit patterns using (5)* *5: Obtain magnitude bit patterns using (6)* *6: End for* *7: End*

Algorithm 1. Neighborhood Binary Pattern Registration

As given in above, NBPR algorithm gives both the flag 'F' and magnitude 'M' components for each pixel from its neighboring pixel. Let us consider 'mp' as the midpoint pixel and 's' as the number of neighbors of a midpoint pixel, then the first '$s\ MSB\ bits$' represent flag and the next '$s\ LSB\ bits$' represent magnitude.

The fingerprint image is scanned on its left-top, left-middle, left-bottom and right-top and considering each pixel which is surrounded by 8 neighboring pixels, forming a '$3 * 3$' matrix. The midpoint pixel depth value is 'd_{mp}' and neighboring pixel depth values are referred to as 'd_{np}'. Then, the flag bit patterns for '$3 * 3\ matrices$' are generated using the mathematical formulae as given below.

$$F(i,j) = \begin{cases} 0, d_{mp} - d_{np} \leq 0 \\ 1, d_{mp} - d_{np} > 0 \end{cases} \quad (5)$$

From equation (5), the flag bit patterns are generated by first identifying the difference between the midpoint pixel and the neighboring pixel. If the resultant value is less than zero, the flag bit is set as '0', otherwise the flag bit is set as '1'. The magnitude bit patterns for '$3 * 3\ matrices$' are generated using the mathematical formulae as given below.

$$M(i,j) = \begin{cases} 0, d_{mp} - d_{np} \leq s \\ 1, d_{mp} - d_{np} > s \end{cases} \quad (6)$$

From equation (6), the magnitude bit patterns are generated by first identifying the difference between the midpoint pixel and the neighboring pixel. With the obtained resultant value, the actual value is compared with the resultant value. If the resultant value is less than the actual value, then the magnitude bit pattern is set as '0', otherwise, the magnitude bit pattern is set as '1'.The sample representation of NBP is as shown in Figure 3.

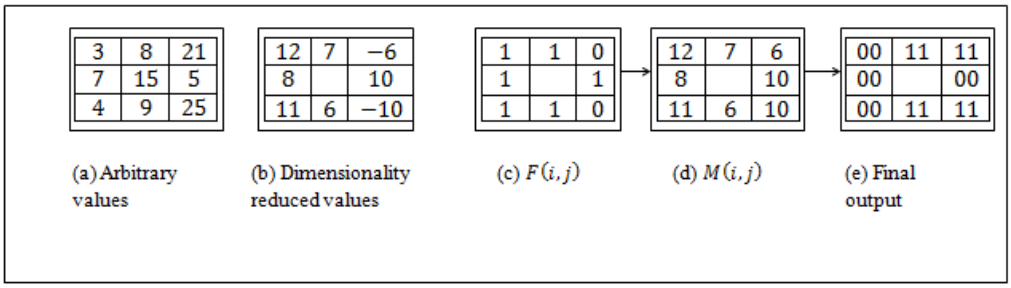

Figure 3. Representation of Neighborhood Binary Pattern

The arbitrary values for '$3 * 3$' matrix are considered in Figure 3(a). The reduced dimensionality values are shown in Figure 3(b). The flag bit of each coefficient is represented in Figure 3(c). The magnitude components of NBP are shown in Figure 3(d). Finally, the resultant registered value is obtained by comparing the actual values and resultant difference values and is represented in figure 3(e). As a result, small scale appearance of the biometric fingerprint image is obtained.

As both the pixel difference and magnitude difference is used, the model is found to be computationally simple, therefore utilizing lesser memory. In other words, by applying Neighborhood Binary Pattern for biometric fingerprint registration for IoT devices, running time is said to be reduced.

3.5 Histogram of Neighborhood Binary Pattern Preprocessing model

After obtaining NBP values from fingerprint images, preprocessing of fingerprint images is performed to extract the region of interest using Histogram of Neighborhood Binary Pattern Preprocessing (HNBPP) model for fingerprint features. Dominant region of interest is stored in a vector for fingerprint features and form the fingerprint template of the human individuals.

Three key modules are presented in the proposed HNBPP model namely, fingerprint gradient extraction, gradient direction, and proposed fingerprint normalization. In the HNBPP model, with the registered values (i.e. fingerprint features, user ID and fingerprint impressions) as input, preprocessing starts with the fingerprint gradient extraction. Here, vertical extraction and horizontal extraction are performed for pixel depth 'd'. It is mathematically formulated as given below.

$$G_i(j,i) = d\,(j,i+1) - d\,(j,i-1) \quad (7)$$

$$G_j(j,i) = d(j+1,i) - d\,(j-1,i) \quad (8)$$

From the above equations (7) and (8), 'G_i' represent the vertical fingerprint extraction and 'G_j' represents the horizontal fingerprint extraction with 'd(i,j)' denoting the pixel depth at coordinates 'i' and 'j' respectively. With the resultant fingerprint gradient extraction, next, the direction of extracted fingerprint gradient is formed. It is mathematically represented as given below.

$$\theta\,(j,i) = arctan\left[\frac{G_j(j,i)}{G_i(j,i)}\right] \quad (9)$$

Finally, fingerprint normalization is performed using the histogram obtained through vertical extraction, horizontal extraction, and direction of extracted fingerprint gradient. It is mathematically formulated as given below.

$$L1\ norm : f = \frac{V}{|V| + c} \quad (10)$$

The pseudo-code representation of Histogram of Neighborhood Binary Pattern Preprocessing (HNBPP) for normalizing the registered values obtained through the NBPR algorithm is given below.

Input: Registered values '$RV(i,j)$', user node '$U = U_1, U_2, \dots, U_n$', pixel depth '$d(i,j)$', gateway node 'GN' and IoT nodes or IoT devices '$D = d_1, d_2, \dots, d_n$', fingerprint impressions 'FP_i'
Output: Normalized fingerprint 'f'
1: Begin *2:For each user node 'U' with gateway node 'GN',IoT devices 'D' fingerprint impressions 'FP_i'* *3:For each Registered Values '$RV(i,j)$'* *4: Obtain vertical extraction and horizontal extraction using (7) and (8)* *5: Obtain gradient direction using (9)* *6:Stored the resultant of (7), (8) and (9) in vector 'V'* *7: Obtain normalized fingerprint using (10)* *8: End for* *9:End for* *10: End*

Algorithm 2. Histogram of Neighborhood Binary Pattern Preprocessing (HNBPP)

As given in the above HNBPP algorithm, for each user node with gateway node, IoT devices and fingerprint impressions as input, preprocessing the registered values obtained through the NBPR algorithm. The running time using NBPR algorithm was found to be less due to binary pattern registration, the computational complexity was found to be high. To reduce the computational complexity involved in fingerprint biometric-based authentication for IoT services, histogram model is used. By obtaining the histogram via vertical and horizontal factors along with gradient information and finally, normalizing the fingerprint biometric, the computational complexity is said to be reduced.

3.6 Tripartite Component User Authentication

With preprocessed fingerprint images of users, the process of template matching is performed to identify the matching accuracy. With the Tripartite Component User Authentication is applied to the preprocessed fingerprint images, the matching accuracy of test data to the available training data (fingerprint templates) are first extracted from the benchmark/real dataset. On the other hand, no access to IoT devices is said to take place upon unsuccessful matching. Therefore, whenever the user tries to access the IoT devices, the system validates the user through the fingerprint module we have included.

The pseudo-code representation of Tripartite Component User Authentication is provided below.

Input: user node '$U = U_1, U_2, \dots, U_n$', gateway node 'GN' and IoT nodes or IoT devices '$D = d_1, d_2, \dots, d_n$', fingerprint impressions 'FP_i', Normalized fingerprint 'f'
Output: Improved matching accuracy
1: Begin *2:For each user node 'U' with gateway node 'GN',IoT devices 'D' fingerprint impressions 'FP_i'* *3: For each Normalized fingerprint 'f'* *4: If '$f \in FP_i$'* *5: Verification OK* *6: Authentication Succeeded* *7: Access of IoT devices* *8: End if* *9: If '$f \notin FP_i$'* *10: Verification not OK* *11: Authentication not Succeeded* *12: No access of IoT devices* *13: End if* *14: End for* *15: End for* *16: End*

Algorithm 3. Tripartite Component User Authentication

With the successful matching of the test and trained dataset (obtained from fingerprint template), access of IoT devices is said to take place. On the other hand, if the user fails to authorize him/her through fingerprint recognition, he/she cannot access the IoT devices.

4. PERFORMANCE EVALUATION

The experimental evaluation is conducted using biometric samples that are extracted from the BioSecure datasets distributed by Association of BioSecure. The performance results of the proposed method are obtained using different training and test dataset samples contain data of both male and female. The training dataset is of the size 240 fingerprint images whereas the test dataset includes 150 images of user's fingerprint to access IoT services towards smart home systems. The experiments were implemented in MATLAB. The proposed method is compared with two existing methods namely Intelligent healthcare framework proposed by Munish Bhatia et al. (2017) and Multi-factor biometric user authentication proposed by Parwinder Kaur Dhillon et al. (2017). Fingerprint biometric user authentication to access smart home IoT services focuses on the aspects of matching accuracy and authentication to access smart home IoT services. The proposed method is evaluated in different aspects such as matching accuracy, Execution speed, and computational overhead.

4.1 Matching accuracy

The main goal of our experiments is to determine the rate of matching accuracy for fingerprint biometric user authentication using evolutionary algorithms. Matching accuracy is one of the performance parameters and is determined as the ratio of biometric samples that were matched correctly to the density of human biometric samples provided as input during experimentation. A random selection of 150 fingerprint images out of 240 images was made. The matching accuracy for fingerprint biometric user authentication to access smart home IoT devices of an individual user is evaluated by the following formula.

$$A = \sum_{size=1}^{n} \frac{Fusion\ template\ matched}{U_{size}} * 100 \qquad (11)$$

From equation (11), the accuracy 'A' is measured concerning the total number of fingerprint biometric samples 'U_{size}' and measured in terms of percentage (%). Figure 4 illustrates the matching accuracy for smart home IoT services using fingerprint biometric with a density of biometric samples in the range of 15 to 150. The decision point of ten different fingerprint biometric samples was selected in a random manner that achieved a substantial improvement in ratings. The results show better performance of the proposed HNTA-FB method, but it is not linear due to the presence of noise in fingerprint biometric images. The final values of the graph plotted in the figure confirm the working hypothesis that the matching accuracy for smart home IoT services using fingerprint biometric increases with the increase in the density.

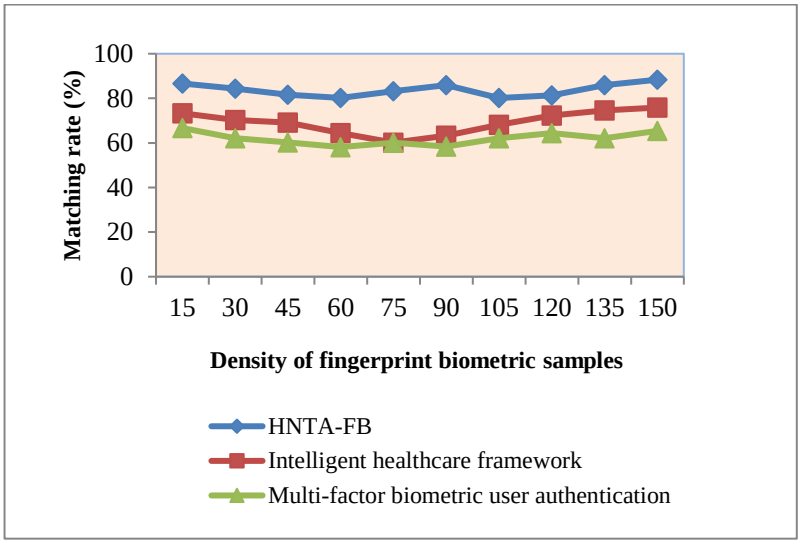

Figure 4. Matching accuracy using fingerprint biometric

The HNTA-FB method improved the matching accuracy for biometric authentication using the extensive Tripartite User Authentication algorithm, by 22% compared to Intelligent healthcare framework proposed by Munish Bhatia et al. (2017) and by 35% compared to Multi-factor biometric user authentication proposed by Parwinder Kaur Dhillon et al. (2017). This is because the HNTA-FB method adapted a fingerprint gradient extraction, gradient direction, and fingerprint normalization to decide upon the factor whether or not the two representations belong to the same user, resulting in the improvement of matching accuracy. Furthermore based on the resultant normalized value, to obtain maximum relevance they were converted based on tripartite values to access the IoT services that in turn improved the matching accuracy.

4.2 Execution speed

The execution speed for pattern registration is the time required to extract the minutiae features concerning the template size and is as given below. It is the product of template size considered and the time is taken for minutiae feature extraction.

$$ES_{ti\,me} = FT_{size} * Time\ (minutiae\ extraction) \qquad (12)$$

Where ES_{time} is the running time for pattern registration and FT_{size} refers to the template size considered during each iteration.

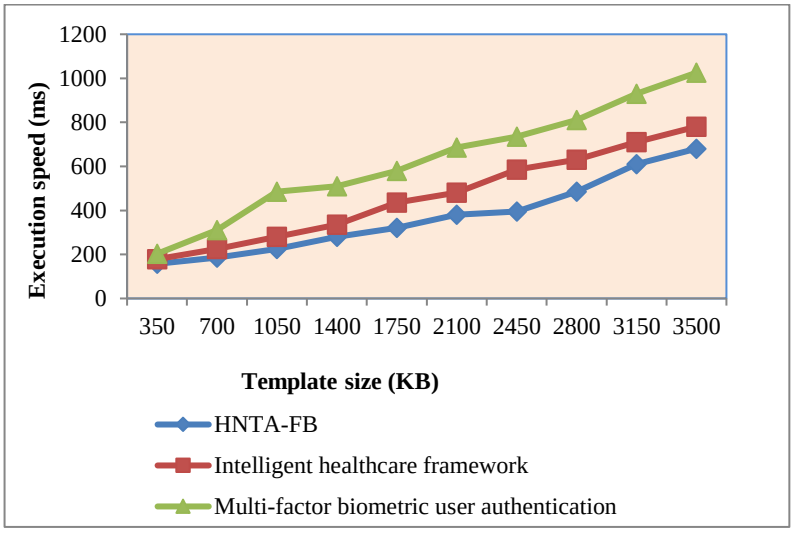

Figure 5. Measurement of execution speed for HNTA-FB

Experimental results for execution time are obtained for registration and authentication with fingerprint biometric templates. Higher, the template size, higher the running time for user registration. With higher template size, the size of individual fingerprint images grows exponentially, and therefore the running time for increased template size also increased. But from figure 5, it is comparatively observed that the proposed HNTA-FB method results from the lower execution time.

By applying the Neighborhood Binary Pattern Registration (NBPR) algorithm in HNTA-FB method, fingerprint images are extracted based on the minutiae, comparing their corresponding neighborhood structures via flag bit and magnitude bit patterns. The redundant information is removed from obtained fingerprint biometric of a user resulting in minimizing the user registration time. As a result, the time taken for authentication to access the IoT devices is also said to be reduced. The process is repeated with the template size of 350KB to 3500KB for conducting experiments. The results confirm that the running time increases, with the increase in the template size, though betterment achieved using HNTA-FB method.

As shown in figure 5, when compared to two other methods proposed by Munish Bhatia et al. (2017) and Parwinder Kaur Dhillon et al. (2017), the HNTA-FB method had better changes using the extensive NBPR algorithm. The NBPR algorithm applied in HNTA-FB method symbolizes the mean estimation of fingerprint image by scanning left-top, left-middle, left-bottom and right-top reducing a certain amount of noise present in the fingerprint. This, in turn, reduces the running time of user registration and therefore the authentication time for accessing IoT devices by 19% compared to Intelligent healthcare framework and 40% compared to Multi-factor biometric user authentication.

4.3 Computational overhead

Finally, the third goal of our experiments is addressed concerning computational overhead which is a measure of the amount of working storage required to perform fingerprint biometric template matching (algorithm). In other words, computational overhead measures the memory required to execute the algorithm at any point.

$$CO = U_{size} * Mem\,(G[i,j]) + Mem\left(\theta\,(j,i)\right) + Mem\,(L1\,norm) \qquad (13)$$

From the above equation (13), the computational overhead 'CO' is obtained using the density of human biometric samples 'U_{size}' and memory consumed for gradient extraction '$G[i,j]$', gradient direction '$\theta\,(j,i)$' and normalization '$L1\,norm$'. It is measured in terms of KiloBytes (KB). For all scenarios as shown in the figure, the computational overhead is increasing with fingerprint biometric samples considered from different users. Ten unique experiments were conducted for each review size. The sample calculation is provided below. Followed by the calculations measured for computational overhead using the proposed HNTA-FB method, Intelligent healthcare framework and Multi-factor biometric user authentication graphical representation are provided.

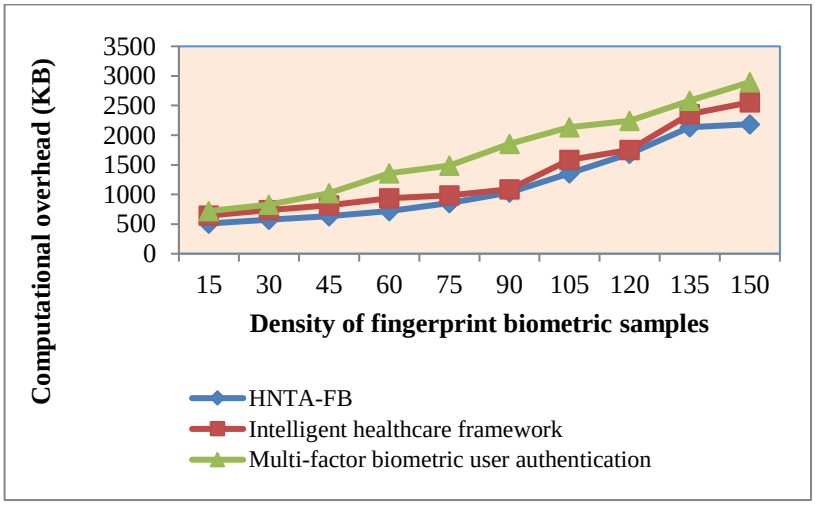

Figure 6. Measure of computational overhead

For better perception of the efficacy of the proposed HNTA-FB method, substantial experiments are conducted and illustrated in Figure 6. It shows the experimental results of computational overhead versus the density of fingerprint biometric samples considered. The targeting results of computational overhead using HNTA-FB method is compared with two state-of-the-art methods intelligent healthcare framework proposed by Munish Bhatia et al. (2017) and Multi-factor biometric user authentication proposed by Parwinder Kaur Dhillon et al. (2017). We have incorporated Histogram of Neighborhood Binary Pattern for fingerprint biometric of the human individuals which are differed from the state of the art methods. Here the dominant factors are stored via vertical and horizontal factors along with gradient information and finally, normalizing

the fingerprint biometric that reduces the dimensionality factor. With the resultant feature vectors obtained from fingerprint features, the resultant value is stored in vector based on the mutual information of the individual features. This in turn, reduces the computational overhead arising during access of IoT devices. Therefore the computational complexity for accessing IoT devices using fingerprint biometric feature is reduced by 15% compared to intelligent healthcare framework and 33% compared to Multi-factor biometric user authentication respectively.

5. CONCLUSION

Biometric-based authentication for accessing IoT devices and IoT networks is considered as a complex task due to the intrinsic features. To safeguard these IoT devices from malicious users, an efficient method is proposed with minimal complexity and time. In this article, we provide a method called Histogram of Neighborhood Tripartite Authentication with Fingerprint Biometrics (HNTA-FB) for IoT services. Initially, the fingerprint features are extracted using Neighborhood Binary Pattern Registration (NBPR) algorithm. With the extracted features, dominant attributes are stored in a vector form by applying Histogram of Neighborhood Binary Pattern Preprocessing (HNBPP) algorithm which resulted in the minimization of computational complexity for several users with the fingerprint as the biometric feature. The evaluation of the template matching is performed finally using the Tripartite Component User Authentication algorithm to authenticate the users so that only authenticated users are allowed to access the IoT devices. Through the experiments using real traces, we observed that HNTA-FB can be employed as a safe communication method for successful access of smart home IoT devices with reduced running time and computational complexity than the existing biometric authentication methods. Thus, the proposed method is suitable for smart home systems and other applications such as health care, surveillance and so on.

REFERENCES

[1] Munish Bhatia, Sandeep K. Sood, “A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective”, Computers in Industry, Elsevier, 2017. https://doi.org/10.1016/j.compind.2017.06.009 .

[2] Parwinder Kaur Dhillon, Sheetal Kalra, “A lightweight biometrics based remote user authentication scheme for IoT services”, Journal of Information Security and Applications, Elsevier, 2017. https://doi.org/10.1016/j.jisa.2017.01.003

[3] Ortega-Garcia, Javier, “The multi scenario multi environment biosecure multimodal database" IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010. https://doi.org/10.1109/tpami.2009.76

[4] Jun Xu, Xiong Zhang, and Meng Zhou, “A High-Security and Smart Interaction System Based on Hand Gesture Recognition for Internet of Things”, Hindawi, Security and Communication Networks, 2018. https://doi.org/10.1155/2018/4879496

[5] Li Yang, Zhiming Zheng, "Cryptanalysis and improvement of a biometrics-based authentication and key agreement scheme for multi-server environments", PLOS ONE, 2018, https://doi.org/10.1371/journal.pone.0194093

[6] M. Shamim Hossain et al., "Toward End-to-End Biometrics-Based Security for IoT Infrastructure", IEEE Wireless Communications, 2016. https://doi.org/10.1109/mwc.2016.7721741

[7] Younsung Choi, Youngsook Lee, Jongho Moon, Dongho Won, "Security enhanced multi-factor biometric authentication scheme using bio-hash function", PLOS ONE, 2017. https://doi.org/10.1371/journal.pone.0176250.

[8] Seyedehsamaneh Shojaeilangari, Wei-Yun Yau, Karthik Nandakumar, Li Jun, Eam Khwang Teoh, "Robust Representation and Recognition of Facial Emotions Using Extreme Sparse Learning", IEEE Transactions on Image Processing, 2015. https://doi.org/10.1109/tip.2015.2416634

[9] Juan S. Arteaga-Falconi, Hussein Al Osman, Abdulmotaleb El Saddik, "ECG and Fingerprint Bimodal Authentication", Sustainable Cities and Society, Elsevier, 2017. https://doi.org/10.1016/j.scs.2017.12.023

[10] Pedro Peris-Lopez, Lorena Gonzalez-Manzano, Carmen Camara, Jose Maria de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things", Future Generation Computer Systems, Elsevier, 2017. https://doi.org/10.1016/j.future.2017.11.037

[11] Haibo Yi, Zhe Nie, "Side-channel security analysis of UOV signature for cloud-based Internet of Things", Future Generation Computer Systems, Elsevier, 2018. https://doi.org/10.1016/j.future.2018.04.083

[12] Wencheng Yang, Jiankun Hu, Song Wang, Qianhong Wu, "Biometrics Based Privacy-Preserving Authentication and Mobile Template Protection", Hindawi Wireless Communications and Mobile Computing, 2018. https://doi.org/10.1155/2018/7107295

[13] Dong-Hwan Park, Hyo-Chan Bang, Cheol Sik Pyo, Soon-Ju Kang, "Semantic Open IoT Service Platform Technology", IEEE World Forum on Internet of Things, 2014. https://doi.org/10.1109/wf-iot.2014.6803125

[14] Igor Miladinovic, Sigrid Schefer-Wenzl, "NFV Enabled IoT Architecture for an Operating Room Environment", IEEE 4th World Forum on Internet of Things (WF-IoT), 2018. https://doi.org/10.1109/wf-iot.2018.8355128

[15] Paul Loh Ruen Chze, Kan Siew Leong, "A Secure Multi-Hop Routing for IoT Communication", IEEE World Forum on Internet of Things (WF-IoT), 2014. https://doi.org/10.1109/wf-iot.2014.6803204

[16] Shulong Wang, Yibin Hou, Fang Gao, Xinrong Ji, "A Novel IoT Access Architecture for Vehicle Monitoring System", IEEE 3rd World Forum on Internet of Things , 2016. https://doi.org/10.1109/wf-iot.2016.7845396

[17] Jong Hyuk Park, Neil Yuwen Yen, "Advanced algorithms and applications based on IoT for the smart Devices", Journal of Ambient Intelligence and Humanized Computing, 2018. https://doi.org/10.1007/s12652-018-0715-5

[18] Lavinia, Mihaela, Dinca, Gerhard Petrus Hancke, "The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods", IEEE Access (Volume: 5), 2017. https://doi.org/10.1109/access.2017.2694050

[19] Yaman Sharaf-Dabbagh, Walid Saad, "Demo Abstract: Cyber-Physical Fingerprinting for Internet of Things Authentication", ACM/IEEE Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017. https://doi.org/10.1145/3054977.3057323