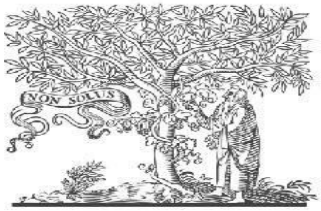
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 28th jul 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 06

10.48047/IJIEMR/V12/ISSUE 07/14

Title **Security threats in Fog computing environment: Enhancing Multimodal Biometric Authentication by Feature Level Optimization in Edge and Fog Paradigm**

Volume 12, ISSUE 07, Pages: 121-134

Paper Authors **Dipti Prava Sahu, Biswajit Tripathy, Leena Samantaray**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Security threats in Fog computing environment: Enhancing Multimodal Biometric Authentication by Feature Level Optimization in Edge and Fog Paradigm

Dipti Prava Sahu[*1], Biswajit Tripathy[2], Leena Samantaray[3]

[1]Research Scholar, Department of Computer Science & Engineering, Biju Patnaik University of Technology, Rourkela, Odisha, 769004, India

[2]Professor, Master of Computer Applications, Einstein College of Computer Application and Management, Khurda, Odisha, 752060, India

[3]Professor & Principal, Department of Electronics and Communication Engineering, Ajay Binay Institute of Technology, Cuttack, Odisha, 753014, India

E-mail: diptiparva29@gmail.com[1], biswajit69@gmail.com[2], leena_sam@rediffmail.com[3]

Corresponding Author : Dipti Prava Sahu

Abstract

The widespread adoption of Fog computing has ushered in new possibilities for efficient data processing and reduced latency at the network edge. However, the integration of edge and fog devices into the computing ecosystem introduces security challenges that demand comprehensive solutions. In this research, we address security threats in the Fog computing environment and propose an enhanced multimodal biometric authentication system (MBAS) that leverages face, ear, and hand vein images. Feature extraction techniques using Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA) are applied to enhance the discriminative power of the biometric traits. To further improve the accuracy of authentication, we employ a feature fusion mechanism based on Grade Level, Multi-Objective Mode Optimization Genetic Algorithm (MOMGA) feature selection is used to select the most relevant and discriminative features for classification. The authentication process is performed using the K-Nearest Neighbors (KNN) classifier. The effectiveness of the proposed method is evaluated using a real-world dataset comprising face, ear, and hand vein images collected from a diverse set of individuals. Experimental results demonstrate that the proposed approach achieves superior authentication accuracy compared to conventional biometric systems. Additionally, the use of MOMGA feature selection enhances the model's generalization capability and improves the system's resistance to attacks.

Keywords: Fog computing, multimodal biometric authentication, Independent Component Analysis, Linear Discriminant Analysis, Grade Level fusion, Multi-Objective Mode Optimization Genetic Algorithm.

1. Introduction

Fog computing has emerged as a promising paradigm that extends the capabilities of cloud computing closer to the edge of the network, thereby enabling faster data processing and reduced latency for applications and services [1]. However, the integration of edge and fog devices into the computing ecosystem introduces new security challenges that need to be addressed to ensure the confidentiality, integrity, and availability of data and services. Various researches [2] aims to explore security threats in the fog computing environment and propose an enhanced MBAS using feature-level optimization within the edge and fog paradigm. The rapid growth of Internet of things (IoT) [3] devices and the increasing demand for real-time data processing has led to the adoption of fog computing as a viable solution. Fog computing's ability to handle data at the network edge has shown promising benefits, such as improved response times and reduced data transfer to the cloud. Nevertheless, this shift also opens new attack vectors, as edge and fog devices may lack robust security measures compared to traditional centralized cloud data

centers [4]. The motivation behind this research lies in the need to comprehensively address security concerns in the fog computing environment, especially when it comes to implementing authentication mechanisms that can guarantee secure access to sensitive data and services.

The main problem addressed in this research is the security threats present in the fog computing environment, particularly in the context of MBAS [5], which combines multiple biometric traits, such as fingerprints, facial features, voice, or iris patterns, to enhance the accuracy and reliability of the authentication process [6]. However, integrating this approach within the edge and fog computing paradigm poses significant challenges. Some key aspects of the problem include vulnerabilities in edge and fog devices, data privacy and confidentiality, network connectivity and reliability, feature level optimization. Edge and fog devices, being resource-constrained [7], may lack the necessary security measures, making them susceptible to various attacks, including physical tampering, malware injections, and unauthorized access. As fog computing involves processing [8] and storing data at the network edge, ensuring data privacy and confidentiality becomes critical, especially when dealing with sensitive user information used for biometric authentication. The intermittent connectivity [9] and dynamic nature of edge and fog devices can lead to disruptions in communication, potentially impacting the authentication process. Ensuring authentication reliability under varying network conditions is a vital challenge. To achieve accurate MBAS [10], feature-level optimization is necessary to select and combine relevant biometric features effectively. However, this optimization process needs to be performed efficiently and securely within the constrained fog computing environment. So, this research seeks to propose an enhanced MBAS that addresses the security threats in the fog computing environment by considering feature-level optimization while ensuring data privacy, reliability, and efficiency in edge and fog-based authentication systems. So, the novel contributions of this work are as follows:

- Proposed an enhanced MBAS for the fog computing environment by integration of face, ear, and hand vein images as biometric modalities for authentication.
- Utilized ICA and LDA for feature extraction to enhance discriminative power and employed Grade Level fusion to combine features from different modalities effectively.
- Introduced MOMGA for feature selection, optimizing multiple objectives simultaneously and KNN classifier for final authentication decision-making.
- Demonstrated the effectiveness of the proposed system in enhancing security and accuracy of user authentication in edge and fog computing environments.

Rest of the paper is organized as follows: section 2 contains the related works with biometrics modes of operation. Section 3 focused on detailed operation of proposed MOMGA feature selection process. Section 4 focused on implementation of proposed MBAS with ICA, LDA, feature fusion, MMOGA. KNN stages. Section 5 focused on simulation results, discussion of performance measures, and comparison. Finally, section 5 concludes the article with possibility of future enhancement.

2. Related works

The word bio refers to life and metric refers to measurement. The science and technology known as biometrics are used to identify people by their bodily and or temperament. The information gathered from a component of the human body, such as fingerprints, palm veins, facial photographs, ear patterns, eye patterns (iris and retinal scan), DNA, and hand veins, is used to infer biological function. Voice, signature, movement, typing rhythm, and other cognitive traits are connected to a person's pattern of conduct. In [11] authors presented a framework that combines AI and IoT for health monitoring applications. The authors discuss the potential benefits and challenges of integrating these technologies to improve healthcare systems. In [12] authors survey focuses on the fusion of multimodal medical signals using AI techniques for smart healthcare systems. The authors review various approaches and methodologies employed in this domain. In [13], the authors provide a review of AI-based sensors used in next-generation IoT applications, with a focus on their potential in healthcare and other domains. In [18]

authors proposed a resource-aware and secure framework for wearable healthcare systems. The authors address the challenges of data security and resource management in such systems. In [19] authors explored the integration of edge-cloud computing and AI for the Internet of Medical Things (IoMT) and discuss the architectural considerations and applications. In [20] authors proposed the concept of "Crowd-IoT," which involves crowdsourcing data in IoT applications. The authors discuss the architecture, security implications, and potential applications of this approach. In [21] authors investigated the secure deployment of the Internet of Robotic Things (IoRT). They analyze the architecture, applications, and challenges related to the integration of IoT and robotics. In [22] authors focused on enhancing the performance of intrusion detection systems (IDS) for detecting attacks on IoT and edge devices. The author presents techniques to improve the accuracy and efficiency of IDS in these environments. In [23] authors presented a review of biometric information protection using fingerprints-based steganography. The authors discuss methods to secure biometric data in IoT and other applications. In [24] authors proposed a linear adaptive congestion control mechanism, LACCVoV, for optimizing data dissemination in vehicle-to-vehicle communication. The study focuses on enhancing communication efficiency in vehicular IoT scenarios. In [25] authors presented a zero leakage OTMP-P2L scheme for edge security access. The authors focus on improving trustworthiness and security in edge computing environments. In [26] authors explored the potential of Low Power Wide Area Networks (LPWAN) and embedded machine learning in advancing wearable devices. The study highlights their role in the next generation of IoT-enabled wearables. In [27] authors provided an overview of enabled technologies and future challenges on the Internet of Things (IoT) domain. The authors cover various aspects of IoT, including enabling technologies and potential issues. In [28] authors analyses privacy-preserving edge computing and IoT models specifically in the healthcare domain. The authors discuss techniques to ensure data privacy and security in healthcare applications. In [29] authors proposed a big data-driven scheduling optimization algorithm for Cyber-Physical Systems (CPS) using cloud platforms. The study aims to improve efficiency and resource allocation in CPS scenarios. In [30] authors discussed the transfer of activity recognition models in Fog Computing architectures. The authors explore techniques to efficiently transfer models for improved data processing in Fog-based IoT scenarios.

2.1 Biometrics and Mode Types

The importance of the biometric in recent years has been increased with the need for accuracy. Biometric based technology is simple, convenient, user friendly, highly secure, socially acceptable, cannot be forgotten or stolen, always available and hold identical feature set, hence it endorses to use in an application that requires higher security. Figure 1 shows the various biometric traits of a person that can be used for authentication purpose.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

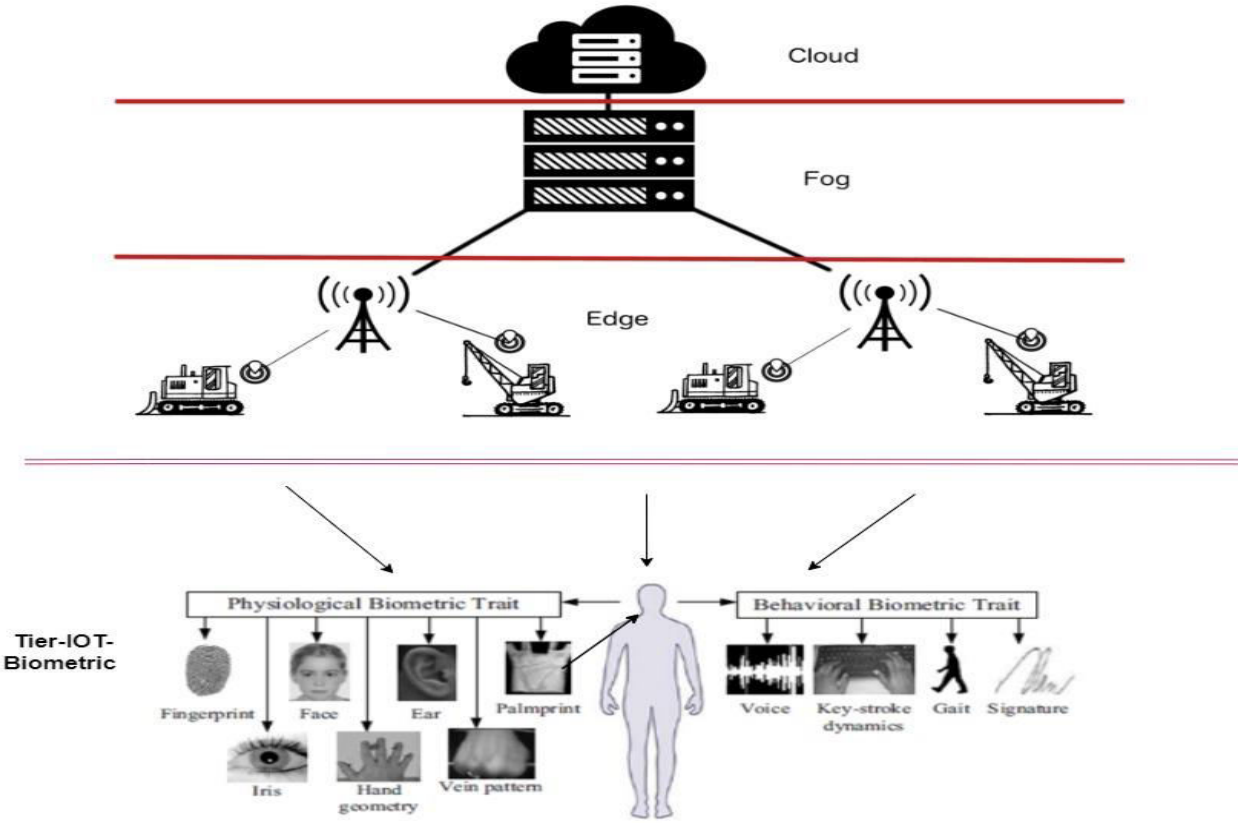


Fig. 1. Biometric traits to identify a person.

2.2 Mode of Operation

Depending upon the application, a biometric system operates in various modes like enrolment mode, verification mode and identification mode (Behera, N. K. Set al. 2022). They are explained as follows

Step 1-Enrolment Mode: First, a user must register his/her biometric trait in the system. In this mode, the user's raw data is collected, processed, and its points are obtained. These characteristics are then saved as a master template along with further details like a name or roll number. This master template is compared with test template for recognition. Figure 2 shows the enrolment process of a biometric system.

Step 2-Verification Mode: To begin, a user is required to register their unique biometric characteristic within the system. The raw data of the user is gathered in this mode, and then it is processed, and its points are obtained. After that, these attributes are added to an existing master template alongside additional information such as a name or roll number. During the recognition process, this master template and the test template are compared to one another. The enrolment procedure for a biometric system is depicted in Figure 3.

(PROCEEDINGS OF ICRAST'23) ISBN:978-93-5915-119-9

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

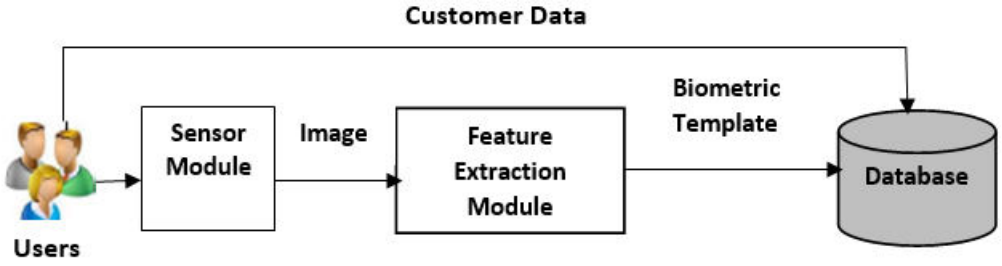


Fig. 2. Enrolment process of biometric system.

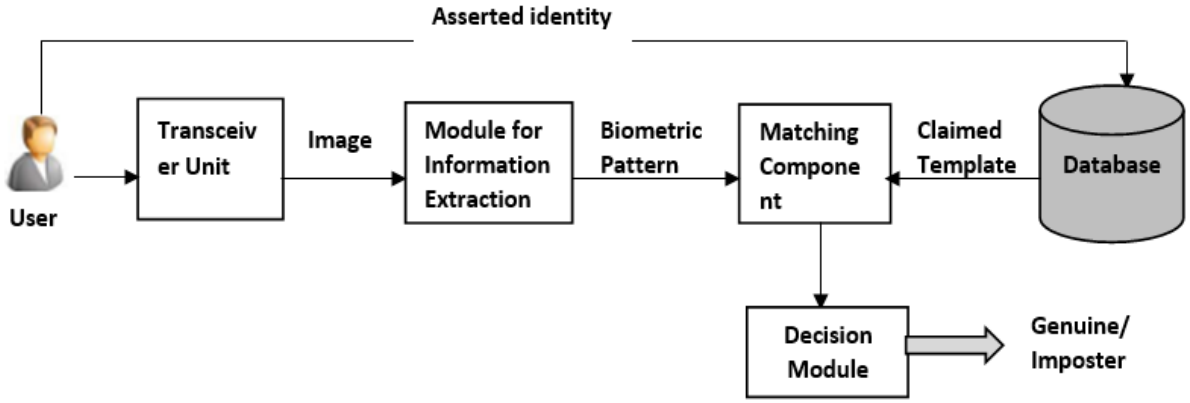


Fig.3. Steps in an identification system's verification mode.

Step 3-Identification Mode: By using the identification mode to search all user templates in the database, a person can be identified. In this case, the user is not required to supply any identity information to the system. To determine his or her identification, the system runs a one-to-many comparison. The steps in an authentication system's identification mode are shown in Figure 4.

3.Multi-Objective Mode Optimization Genetic Algorithm (MOMGA)

The simultaneous optimization of numerous objective functions is necessary for many real-world issues. These objective functions frequently clash, leading to a collection of optimal solutions rather than one. The existence of multiple solutions is since no single solution can be deemed superior in terms of all the objective functions. Pareto-optimal solutions are what these solutions fall under. A multi-objective function is generally formulated as in equation 1

$$\frac{Min}{Max} fg_i(x) \; for \; i \; = \; 1 \ldots \ldots .. N_{obj} \tag{1}$$

Subject to

$$\begin{cases} fg_j(xz) = 0\,, \; jy = 1 \ldots \ldots MY \\ vh_k(xz) \leq 0, \; kd = 1 \ldots \ldots KD \end{cases} \tag{2}$$

Here, f_{gi} is the i^{th} objective function, xz is the decision vector that represents a solution, N_{obj} is the number of objectives, MY and KD represent the equality and inequality restrictions, respectively. When comparing two solutions in multi-objective optimization, the concept of dominance is applied. A feasible solution is termed non-dominated while addressing an optimization problem if it is not dominated by any other conceivable solutions. The following strategy is used to identify a set of non-dominated solutions. If $x(1)$ is strictly superior to $x(2)$ in at least one objective and not poorer than $x(2)$ in any objective, then $x(1)$ wins (2). If both requirements are met, solution

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

$x(1)$ is superior to solution $x(2)$, or vice versa (Deb et al. 2001). A pareto set is a collection of non-dominated or perfect solutions in the decision space, and a pareto front is a representation of the collection in the objective space. Figure 5 depicts Pareto optimality, or the min-min dilemma, for two objective functions.

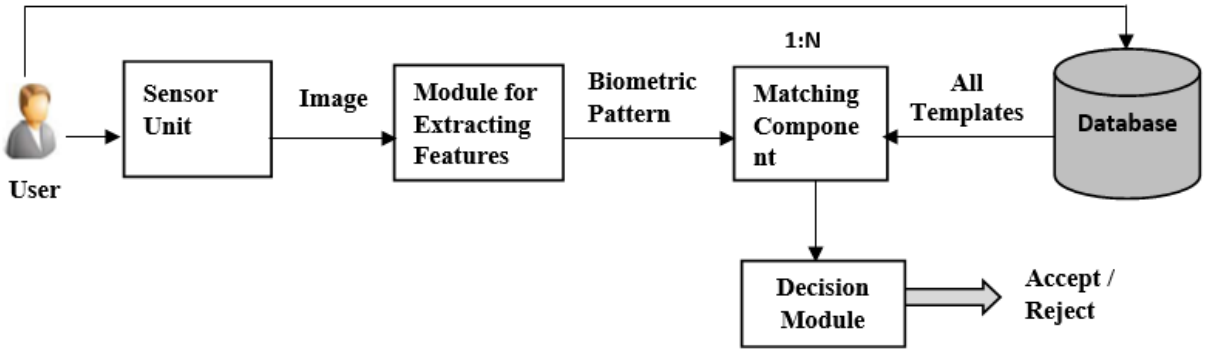


Fig.4.Steps in an authentication system's identification mode.

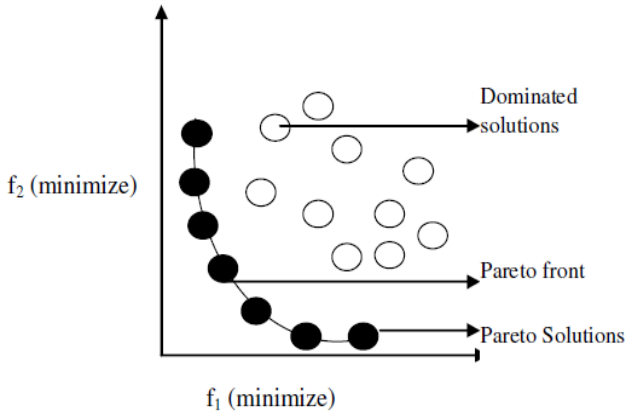


Fig.5. Pareto optimality curve for min-min problem

The classical optimization methods result in the following difficulties.

- To discover numerous pareto-optimal solutions, an algorithm must be applied numerous times.
- Some algorithms are sensitive to the shape of the pareto optimum front.
- Most algorithms require some understanding of the problem being tackled.

The effectiveness of the single goal optimizer affects how widely distributed Pareto-optimal solutions are. To solve the difficulties faced by the classical methods, many evolutionary algorithms are evolved.

4. Proposed MOMGA Based MBAS

In this work, MMOGA is modified and applied to solve the multi-objective need of MBAS. The MOMGA technique is proposed here to handle the feature selection effectively to improve the recognition rate in MBAS. To achieve this the rank level fusion is performed on the three biometric modalities namely a face, ear, and hand dorsal vein images. The overall flow diagram of MOMGA based MBAS is illustrated in the Figure 6. Initially, raw images of face, ear and hand dorsal vein are obtained from ORL face database, USTB ear database and NCUT hand vein database respectively. After removing the noise, the essential feature vectors are extracted using ICA and LDA

algorithms. ICA and LDA algorithms focussed on reducing the dimensions of the feature vector. The feature vectors obtained from face, ear and dorsal hand vein are combined using rank level fusion. It is followed by application of MOMGA on the concatenated feature vector set to obtain the optimal feature subsets. Finally, to perform the matching operation KNN classifier is used in this proposed work. As a result, the overall recognition rate of the system is increased using MOMGA technique.

4.1 Feature Extraction using ICA technique

Many unsupervised statistical methods are available to extract the features from the raw images. ICA is the one used to find a newer set of images from the computed eigen values and eigen vectors of those images. This ICA algorithm requires an image data matrix to be available before for solving the problem. ICA suffers from memory usage as it follows the batch processing method.ICA cannot be useful when applied to data that are available incrementally. Hence, ICA is used in this workbecause it is relevant for memory consuming datasets. The aim of this algorithm is to construct the covariance matrix C_{n+1} starting from the old covariance matrix C_n and the new observed data x_{n+1}. IPCA technique extracts the features from face, ear and hand vein images and represents it in the form of feature vectors. Then the feature vectors are combined using the rank level fusion method. Then it is sent to the evolutionary algorithm-based feature selection method to achieve the optimal subsets.

4.2 Feature Extraction using LDA technique

Machine learning commonly encounters large data sets with hundreds of different features or variables. As a result, the number of variables in the universe grows considerably, making it more challenging to analyse the data and draw conclusions. The LDA technique, a simple method, is used to solve this issue by lowering the dimensionality of the variable space. LDA, which is used to find a linear combination of attributes that distinguishes between two or more classes of objects or events, generalises Fisher's linear discriminant technique. The first LDA, which had been initially published for a 2-class problem, was developed by C.R. Rao in 1948 to create what is now referred to as "multi-class LDA or multiple discriminant analysis." A dataset of n-dimensional samples is projected into a smaller subspace k that is less than or equal to n-1 to preserve class-discriminatory information. The axes' orientations that maximise the separation between different classes are determined via a supervised technique known as LDA. The procedures for carrying out a linear discriminant analysis are as follows.

Step 1- calculating d-dimensional mean vectors for the various dataset classes. The face classes in the database will be $X_1, X_2, \ldots, X_c$, and there will be k facial images in each face class X_i, where i is $1, 2, \ldots, c$. The equation (3) is used to calculate the mean vector I of each class X_i.

$$\mu_i = \frac{1}{k}\sum_{j=1}^{k} x_j \tag{3}$$

Step 2- Calculated as given in equation, the mean vector μ of all classes in the database.

$$\mu = \frac{1}{c}\sum_{i=1}^{c} \mu_i \tag{4}$$

Step 3- Computation of scatter matrices i.e., between class and within-class scatter matrix. The within class scatter matrix is computed as shown in equation (5).

$$S_W = \sum_{i=1}^{c}\sum_{x_k \in X_i}(x_k - \mu_i)\,(x_k - \mu_i)^T \tag{5}$$

Step 4- The class scatter matrix is calculated using the equation as shown in Equation (6).

$$S_B = \sum_{i=1}^{c} N_i\,(\mu_i - \mu)(\mu_i - \mu)^T \tag{6}$$

(PROCEEDINGS OF ICRAST'23) ISBN:978-93-5915-119-9

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

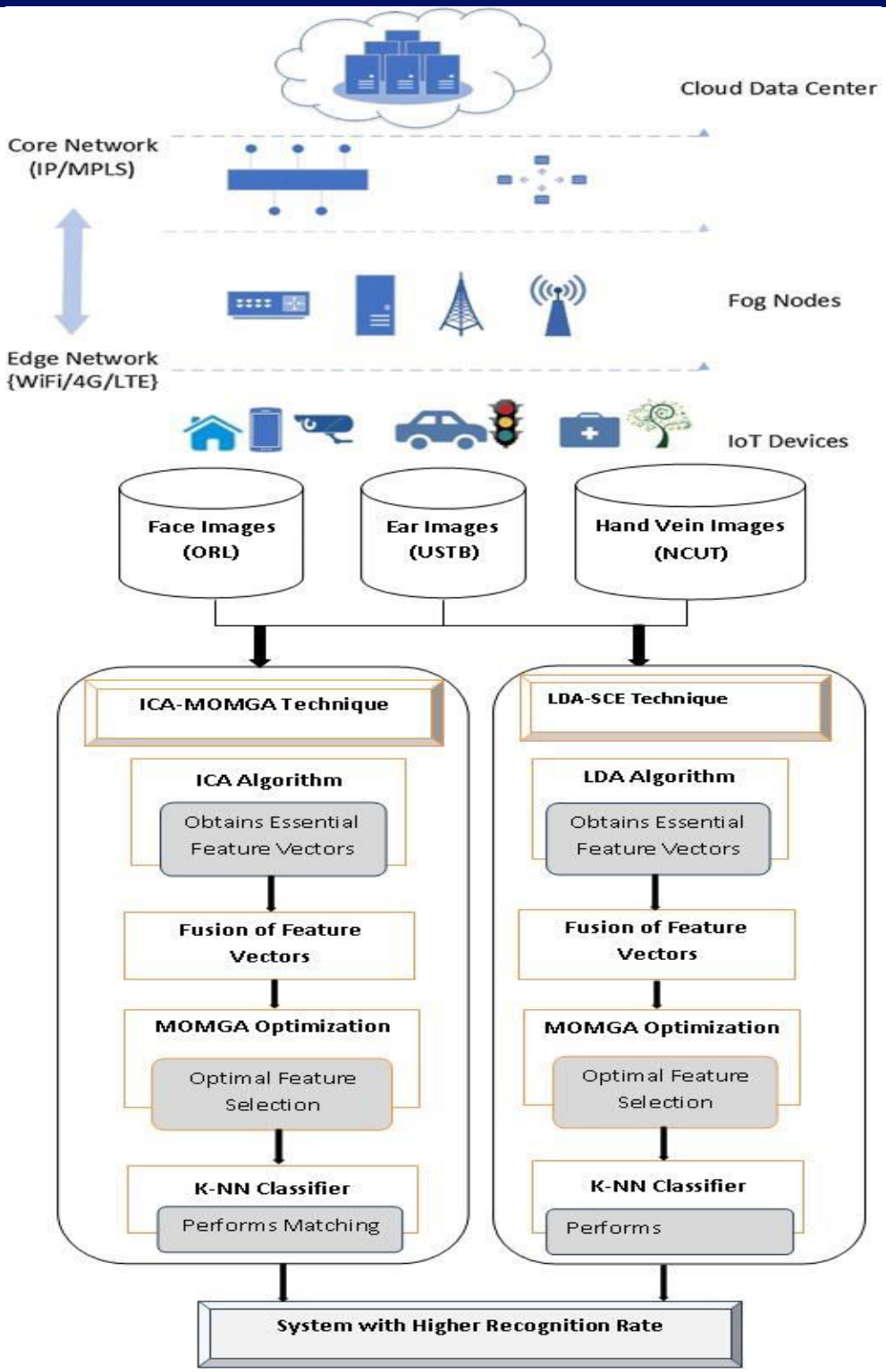


Fig. 6. Flow diagram of MBAS with MOMGA Based Feature Selection Technique.

Step 5- Computation of the product of SW-1 and SB.

(PROCEEDINGS OF ICRAST'23) ISBN:978-93-5915-119-9

Step 6- Computing eigenvectors $(e_1, e_2, \ldots . e_d)$ and related eigen values $(\lambda_1, \lambda_2, \ldots \ldots . \lambda_d)$ for product scatter matrices.

Step 7- Eigenvector sorting by decreasing eigen values and selecting k eigenvectors with the largest eigen values to construct a $d\ x\ k$ dimensional matrix W.

Step 8- Transformation of samples of $d\ x\ k$ eigenvector matrix onto the new subspace results in the formation of matrix $Y = X\ x\ W$. Here, X is a $n\ x\ d$-dimensional matrix representing the n samples and y are the transformed $n\ x\ k$ dimensional samples in the new subspace.

Using the above steps LDA technique projects the face, ear, and hand dorsal images into the new subspace. Then these vectors need to be fused using the rank level fusion method. After performing this operation, the resulting vector is optimized using MOMGA feature selection technique.

4.3 Fusion of Features Using Grade Level

Li, X., et al. offered three options for aggregating the ranks provided by the matchers. The highest rank, the borda count, and logistic regression are all used. The highest rank method employs the highest (least) rating for each potential match obtained using several matchers. As an alternative, the borda Count technique takes advantage of the ranks assigned to users by matchers depending on the effectiveness of modules. As the final stage in the logistic regression technique, a weighted total of the individual ranks is employed, where the weights are distributed to various matchers via regression models. For the dorsal hand vein, the ear, and the face, it was proposed to utilise three matches. If the identities exist in at least two matchers, they are considered for review. Assume that if an identity is only detected in one matcher, it is not evaluated. In this work, the logistic regression method is combined with rank level fusion. This method multiplies the weights assigned to each individual matcher by the starting ranks. The final list of ranks is calculated by multiplying the number of qualities by these additional rankings.

4.4 KNN Classifier

The categorization of the items is done using the instance-based learning technique known as KNN. The phrase "lazy learning approach" is another name for it. This method differs from all previous algorithms in that the objects are classified by majority vote among peers and assigned to one of the k nearest neighbours. Compared to other methods, this classifier is proven to be more accurate and to take less time to execute, making it a good choice for classifying photos. Here, a new image space is used, and a test set is identified based on the image space point that is closest to it. For calculating the closeness between data points in the KNN, the metric of Euclidean distance is chosen. The equation in Figure 4 is used to represent the Euclidean distance d (x, y).

$$d(x, y) = \sqrt{(x_{test} - y_1)^2 + \ldots\ldots + (x_{test} - y_n)^2} \quad (7)$$

Where x_{test} is the test image and y indicate the training sets. Euclidean separation Find the closest location or the shortest path between the training and test sets. The matching action is carried out here using this classifier.

5. Results and Discussion

On a workstation with a Xeon E5 processor with six cores and 64GB of RAM, the suggested MOMGA approach is simulated in MATLAB. Utilizing MATLAB, feature extraction and selection are performed. The Olivetti Research Laboratory database is where the simulation's face images come from. We extracted ear photographs from the University of Science and Technology Beijing database I, which has about 150 shots with 60 volunteers. About 20 right and about 20 left vein shots taken from the backs of 110 people's hands are included in the database of hand vein images from North China University of Technology.820 images from the three databases, representing 140 participants, are used for the experimental evaluation. For the evaluation of the suggested approach, the performance measures FAR (False Accept Rate), FRR (False Reject Rate), and GAR (Genuine Acceptance Rate) are used. The

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

following sections examine the outcomes of the proposed approaches. The experimental analysis of the proposed MOMGA technique is performed and compared with combination of various traits.

5.1 Measurement of FAR And GAR Using ICA-MOMGA Feature Selection Technique

The proposed MBS using ICA-MOMGA based feature selection is analysed using ROC curve with the combination of different modalities. FAR and FRR are used as a function of decision threshold which controls the trade-off between the two error rates. It is measured in terms of %. The likelihood that an impostor will be acknowledged as a real person is known as FAR. The likelihood that a genuine person will be dismissed as a forger is known as FRR. The two terms FAR and FRR are equivalent. Typically, a smaller FAR causes a higher FRR, and a smaller FAR causes a larger FRR. Typically, the FAR is used to specify the system performance requirement. A FAR of 0 means that no impostor is recognised as a real person. Another term for a biometric system's efficiency is GAR. As the FRR is decreased, a system's GAR rises. Table 1 shows the GAR estimation using the ICA-MOMGA feature selection algorithm. Figure 7 shows the simulated outcomes of FAR for various GAR levels. When employing the MOMGA feature selection method, the FAR for the proposed MBS that uses photos of the facial, ear, and palm venous increases by 4.53 percent for the facial and palm venous and 0.62 percent for the face and ear.

Table 1. GAR estimation using the ICA-MOMGA Feature Selection Algorithm.

GAR (%)	Edge devices Palm, Facial, and Ears	Edge devices Facial & Ear	Edge devices Palm Venous & Facial
0.001	74	74	71.5
	77	78	73.5
	78	75.7	74.2
	78.6	79.8	75.7
	81.8	82	75.6
	83	84	78.6
0.01	81.6	81.3	84.7
	86.3	87.6	83.4
	91.3	92.5	93.2
	95	96	94.5
	96	96.2	93.6
	97.3	97.7	94.2
0.1	98.4	97.7	95.3
	98.2	97.6	94.2
	99.3	97.2	94.4
	99.1	97.5	94.2
	99.3	97.4	94.6
1.0	99.2	97.3	94.3

(PROCEEDINGS OF ICRAST'23) ISBN:978-93-5915-119-9

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

5.2 Measurement of FAR and GAR using LDA-MOMGA Feature selection Technique

The proposed MBS using LDA-MOMGA based feature selection is analysed using ROC curve with the combination of different modalities. It is measured in terms of percentage (%). Table 2 shows the GAR estimation using the LDA-MOMGA Feature Selection Algorithm.

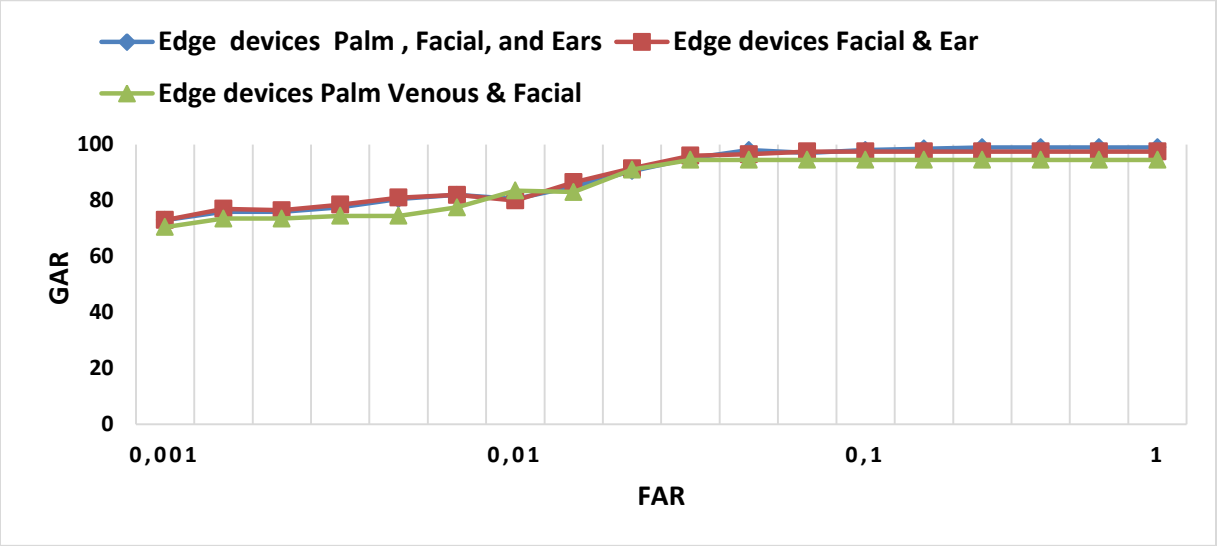


Fig. 7. Measurement of FAR and GAR using ICA-MOMGA feature selection

Table 2. GAR estimation using the LDA-MOMGA Feature Selection Algorithm.

GAR %	Edge devices Palm, Facial, and Ears	Edge devices Facial & Ear	Edge devices Palm Venous & Facial
0.001	68.5	68	66.5
	72	72.5	68
	72.5	72.5	68
	73.5	74.5	69
	76	76.5	70
	77	75.5	71.5
0.01	76.5	75.5	79.5
	81	82	77.5
	85.5	85	86
	88	91	89
	93	90.5	88
	92	90.5	90

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

0.1	92	92.5	89.5
	92	91.5	88.5
	94	92	88
	93	91	88
	92	92.5	89.5
1.0	92.78	90.92	89.11

Figure 8 shows the simulated outcomes of FAR for various GAR values. The MOMGA feature selection method boosts the FAR for the proposed MBS employing photos of the facial, ears, and palm venous by 4.25 percent for the facial and palm venous and 0.56 percent for the face and ear.

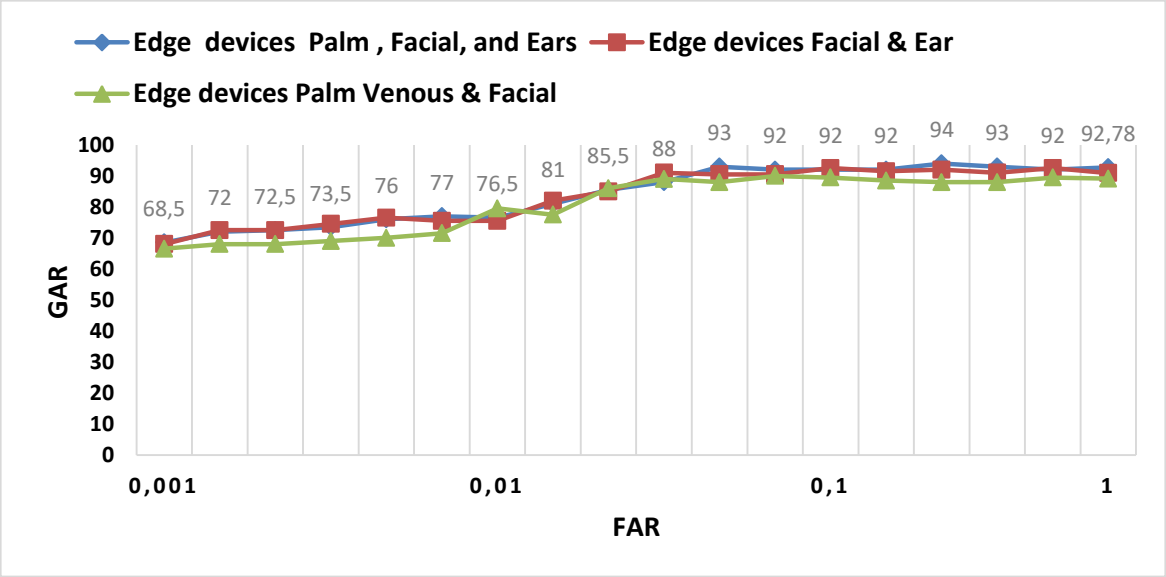


Fig.8. Measurement of FAR and GAR using LDA MOMGA feature selection

6. Conclusion

The proposed enhanced MBAS utilizing feature-level optimization and KNN classifier within the edge and fog paradigm offers a simple yet effective solution to address security threats in fog computing environments. By fusing the discriminative features extracted from face, ear, and hand vein images and optimizing their selection through MOMGA, the system achieves improved accuracy and robustness in user authentication. Using the ICA with SCE feature selection technique, the average GAR percent for the head, ear, and palm veins was 3.13 percent, 8.25 percent, and 3.13 percent, respectively. The average GAR percent for the facial, muffs, and hand veins utilising the LDA with SCE feature selection approach is 3.25 percent for each, whereas the head and palm veins have an average GAR percent of 8.55 percent. The system can be extended to include other emerging biometric modalities, such as gait recognition, vein pattern analysis, or behavioral biometrics, to enhance the richness and diversity of the authentication process.

References

[1] Sarier, N. D. (2021). Multimodal biometric authentication for mobile edge computing. *Information Sciences*, *573*, 82-99.

[2] Othman, S. B., Almalki, F. A., &Sakli, H. (2022). Internet of things in the healthcare applications: overview of security and privacy issues. *Intelligent Healthcare*, 195-213.

[3] Ang, K. L. M., Seng, J. K. P., &Ngharamike, E. (2022). Towards crowdsourcing internet of things (crowd-iot): Architectures, security and applications. *Future Internet*, *14*(2), 49.

[4] Saravanan, T., &Saravanakumar, S. (2021, December). Privacy Preserving using Enhanced Shadow Honeypot technique for Data Retrieval in Cloud Computing. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1151-1154). IEEE.

[5] Behera, N. K. S., Behera, T. K., Nappi, M., Bakshi, S., & Sa, P. K. (2021). Futuristic person re-identification over internet of biometrics things (IoBT): Technical potential versus practical reality. *Pattern Recognition Letters*, *151*, 163-171.

[6] Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials*, *22*(2), 1121-1167.

[7] Saravanan, T., Ambikapathy, A., Faraz, A., & Singh, H. (2021). Blockchain and Big Data for Decentralized Management of IoT-Driven Healthcare Devices. In Convergence of Blockchain, AI, and IoT (pp. 57-81). CRC Press.

[8] Yahuza, M., Idris, M. Y. I. B., Wahab, A. W. B. A., Ho, A. T., Khan, S., Musa, S. N. B., & Taha, A. Z. B. (2020). Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. *IEEE Access*, *8*, 76541-76567.

[9] Wang, J., Ni, M., Wu, F., Liu, S., Qin, J., & Zhu, R. (2019). Electromagnetic radiation based continuous authentication in edge computing enabled internet of things. *Journal of Systems Architecture*, *96*, 53-61.

[10] Zhang, J., & Tao, D. (2020). Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal*, *8*(10), 7789-7817.

[11] Aiswaryadevi, V. J., Sruthi, M. S., Kiruthika, S., Sunitha Nandhini, A., Sathya Bama, S., Soundarya, S., & Priyanka, G. (2021). Artificial Intelligence and IoT Framework for the Health Monitoring System. In *Artificial Intelligence and IoT* (pp. 35-49). Springer, Singapore.

[12] Muhammad, G., Alshehri, F., Karray, F., El Saddik, A., Alsulaiman, M., & Falk, T. H. (2021). A comprehensive survey on multimodal medical signals fusion for smart healthcare systems. *Information Fusion*, *76*, 355-375.

[13] Mukhopadhyay, S. C., Tyagi, S. K. S., Suryadevara, N. K., Piuri, V., Scotti, F., &Zeadally, S. (2021). Artificial intelligence-based sensors for next generation IoT applications: a review. *IEEE Sensors Journal*, *21*(22), 24920-24932.

[14] Saravanan, T., Saravanakumar, S., Rathinam, G., Narayanan, M., Poongothai, T., Patra, P. S. K., &Sengan, S. (2022). Malicious attack alleviation using improved time-based dimensional traffic pattern generation in UWSN. *Journal of Theoretical and Applied Information Technology*, *100*(3).

[15] Ang, K. L. M., & Seng, J. K. P. (2019). Application specific internet of things (ASIoTs): Taxonomy, applications, use case and future directions. *IEEE Access*, *7*, 56577-56590.

[16] Casado-Mansilla, D., Moschos, I., Kamara-Esteban, O., Tsolakis, A. C., Borges, C. E., Krinidis, S., ... & Lopez-De-Ipina, D. (2018). A human-centric & context-aware IoT framework for enhancing energy efficiency in buildings of public use. *IEEE Access*, *6*, 31444-31456.

[17] Li, X., Yu, Q., Alzahrani, B., Barnawi, A., Alhindi, A., Alghazzawi, D., & Miao, Y. (2021). Data fusion for intelligent crowd monitoring and management systems: A survey. *IEEE Access*, *9*, 47069-47083.

[18] Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Generation Computer Systems*, *95*, 382-391.

[19] Sun, L., Jiang, X., Ren, H., & Guo, Y. (2020). Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. *IEEE Access*, *8*, 101079-101092.

[20] Ang, K. L. M., Seng, J. K. P., &Ngharamike, E. (2022). Towards crowdsourcing internet of things (crowd-iot): Architectures, security and applications. *Future Internet*, *14*(2), 49.

[21] Rana, A. K., Sharma, S., Dhawan, S., & Tayal, S. (2021). Towards Secure Deployment on the Internet of Robotic Things: Architecture, Applications, and Challenges. *Multimodal Biometric Systems*, 135-148.

[22] Saheed, Y. K. (2022). Performance Improvement of Intrusion Detection System for Detecting Attacks on Internet of Things and Edge of Things. In *Artificial Intelligence for Cloud and Edge Computing* (pp. 321-339). Springer, Cham.

[23] Hashim, M. M., Mohsin, A. K., & Rahim, M. S. M. (2019, September). All-encompassing review of biometric information protection in fingerprints based steganography. In *Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control* (pp. 1-8).

[24] Sangaiah, A. K., Ramamoorthi, J. S., Rodrigues, J. J., Rahman, M. A., Muhammad, G., &Alrashoud, M. (2020). LACCVoV: linear adaptive congestion control with optimization of data dissemination model in vehicle-to-vehicle communication. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 5319-5328.

[25] Han, D., Du, X., & Lu, Y. (2020). Trustworthiness and a zero leakage OTMP-P2L scheme based on NP problems for edge security access. *Sensors*, *20*(8), 2231.

[26] Sanchez-Iborra, R. (2021). LPWAN and embedded machine learning as enablers for the next generation of wearable devices. *Sensors*, *21*(15), 5218.

[27] Din, I. U., Guizani, M., Hassan, S., Kim, B. S., Khan, M. K., Atiquzzaman, M., & Ahmed, S. H. (2018). The Internet of Things: A review of enabled technologies and future challenges. *Ieee Access*, *7*, 7606-7640.

[28] Almusallam, N., Alabdulatif, A., &Alarfaj, F. (2021). Analysis of Privacy-Preserving Edge Computing and Internet of Things Models in Healthcare Domain. *Computational and Mathematical Methods in Medicine*, *2021*.

[29] Niu, C., & Wang, L. (2022). Big data-driven scheduling optimization algorithm for Cyber–Physical Systems based on a cloud platform. *Computer Communications*, *181*, 173-181.

[30] Samarah, S., Zamil, M. G. A., Rawashdeh, M., Hossain, M. S., Muhammad, G., &Alamri, A. (2018). Transferring activity recognition models in FOG computing architecture. *Journal of Parallel and Distributed Computing*, *122*, 122-130.