



APPLICATIONS OF MULTIMODAL BIOMETRICS AUTHENTICATION FOR ENHANCING THE IOT SECURITY USING DEEP LEARNING

Gergito Kusse^{1*} and Tewoderos Demissie²

¹ Lecturer, Department of Computer Science, Debre Tabor University, Ethiopia,

² Lecturer, Department of Information Technology, Bule Hora University, Ethiopia,

Corresponding author: gergito2@gmail.com

Abstract

The Internet of Things (IoT) integrates billions of electronic devices into computer networks to provide advanced and intelligent services that enable devices to communicate with each other by exchanging information with minimal human interaction. The security issue is at higher risk in IoT systems than in other computing systems. Maintaining the security requirement when attacking the physical surface of the IoT system device is a challenging task. Implementing security mechanisms like authentication and access control for the IoT ecosystem is necessarily needed to ensure the security of IoT devices. The key used for security may be stolen, forgotten, or forged. Also, the key may be generated by intruders or men in the middle of traditional security mechanisms. Biometric security is becoming more advanced and sophisticated with technological advancements and is mostly used in authentication systems. In unimodal biometrics, only one biometrics character can be applied which does not apply to ensure the security of IoT systems. In this paper, Multimodal biometrics authentication was used for securing edge devices in the IoT ecosystems. Face image and fingerprint image were used as multimodal biometrics systems for authenticating users to secured IoT devices. A pi-camera module and fingerprint sensor were used to capture biometric data. Image processing techniques were then applied to the images. Then CNN algorithms were used for feature extraction and model creation. During model creation, the RELU function was used as an activation function, soft-max for image classification, and Max-pooling for image dimensional reduction which helped the model speed up the training process. Experimental results show that the accuracy of the face image and fingerprint image is 92% and 89% respectively, which is a promising result that achieves the objective of the study.

Keywords: *Internet of Things, Multimodal Biometrics, Authentication, CNN, Deep Learning*

Received: 19 March 2022; Revised: 23 March 2023; Accepted: 27 March 2023; Published: 30 April 2023.

Corresponding author- Gergito Kusse



I. Introduction

IoT integrates billions of electronic devices into networks to provide advanced and intelligent services that can communicate with one another by exchanging information with minimal human intervention. IoT structures are complicated and contain integrative arrangements. Therefore, maintaining the security requirement in attacking the physical surface of the IoT system device is challenging. The security issue is at higher risk in IoT systems than in other computing systems, and the traditional solution may be ineffective for such systems. Solutions have to include holistic considerations to meet the safety requirement. However, IoT devices are usually paintings in unattended surroundings. Consequently, an interloper may additionally bodily get admission to those gadgets. IoT gadgets are related normally over Wi-Fi networks in which an outsider might also access private facts from a communication channel with the aid of eavesdropping. IoT devices cannot support complex security structures given their limited computation and power resources [1].

Biometric authentication is a security process that relies on the unique biological characteristics of individuals to verify who they are [2]. Biometric authentication and recognition have become the new branch of exploration in the adoption of newer techniques in terms of security, higher accuracy, and high speed [3]. Unimodal biometric authentication structures got more interest from sensible programs [4] consisting of the Internet of Things (IoT), Automated Teller Machines (ATM), and cellular packages. Thus, one feature is commonly neither green nor enough to expect the proper subject, particularly for the accrued photos in diverse conditions such as illumination, rotation, and occlusion conditions. Therefore, most researchers pay more attention to multimodal biometric recognition to grow identity performance and provide greater protection. Most of the latest human-popularity works [5] utilized function-degree fusion to overcome the challenges of confined assets and to boom device security and device overall performance.

Artificial intelligence is the way of creating an intelligent system that thinks and acts like a human being. It is a way of using computer machines as a power of humans [6]. A system to be an intelligent system should have six disciplines of AI (NLP, computer vision, machine learning, knowledge representation, robotics, and logical reasoning). In the current era, AI is used in



different areas like healthy cars, agriculture, education, and industry. In industry IoT and AI systems are commonly used to improve services and produce more products for customers.

In the IoT ecosystem, complex structures and heterogeneous components are interconnected. In the current era of globalization, most of the systems in industrial companies are migrating to IoT technology. Edge devices in IoT can exchange data with less human interaction. Ensuring security for the IoT ecosystem is necessarily needed to avoid unauthorized access to IoT systems.

Researchers did different security mechanisms to ensure security in IoT systems. In the last decades, traditional security mechanisms were applied to secure edge devices in an IoT ecosystem. Traditional security mechanism has a drawback because the key used for the security method may get stolen, forgotten, or forged key may be created by intruders or a man in the middle, but in biometric security mechanism the character or the key can't be stolen by theft, forgotten, and fake character cannot be generated by the intruders. The biometric character may be physiological (face, fingerprint, iris, hand geometry, hand gesture) or behavioral (walking, typing, touchpad). Most researchers applied either of these biometrics to improve security issues in IoT.

Researchers were applying biometrics in two ways. The first one is a unimodal biometrics system. In unimodal biometrics, only one biometrics character was applied which does not apply to ensuring security in IoT systems. The second one is multimodal biometrics systems that can apply more than one biometrics characteristic.

II. Literature Review

Research by Mohammed Ali Al-Garadi, Amr Mohamed, and Abdulla Al-Ali [7] proposed a review of the machine learning and deep learning methods and algorithms applied to the Internet of Things IoT security which is titled "Survey of security issues Machine and deep learning knowledge of techniques for Internet of Things". In this paper, the researchers tried to address all the methods and algorithms of machine learning and deep learning and how they are applied for ensuring the security of IoT.

Another study by Jasmeen Sharma, and Dharam Veer Sharma [8] proposed a multimodal biometrics authentication using face and fingerprint. They tried to address the drawback of unimodal biometrics and how the multimodal biometric system was very advanced than the

Received: 19 March 2022; **Revised:** 23 March 2023; **Accepted:** 27 March 2023; **Published:** 30 April 2023.

Corresponding author- **Gergito Kusse**



unimodal biometrics. The researchers used principal component analysis (PCA), Bacterial Foraging Optimization algorithms (BFOA), Minute Extraction, and multilayer (MLNN).

In another paper, Sudip Vhaduri and Christian Poellabauer [9] proposed “Multimodal biometric-based implicit authentication of wearable devices users”. They applied authentication mechanisms using combinations of three types of coarse-grain minute-level biometrics: behavioral (step counts), physiological (heart rate), and hybrid (calorie burn and metabolic equivalent of task). Their findings show that hybrid biometrics perform better than other biometrics and behavioral biometrics do not have a significant impact, even during non-sedentary periods.

Very important research by Mohamed Hammad, Yashu Liu, And Kuanquan Wang [10] proposed a “Multimodal biometric authentication system using CNN based on a different level fusion of ECG and fingerprint”. They developed two authentication systems with two different level fusion algorithms: feature-level fusion and decision-level fusion. The feature extraction for users’ modalities is done through the usage of CNN.

III. Research Design and Methodology

A comprehensive overview of multimodal biometric authentication for enhancing IoT security systems with face recognition and fingerprint biometric data was discussed. For the experimental investigation, images were collected through the pi-camera and fingerprint sensor.

A. Proposed Model Architecture

The proposed model contains two phases, the enrollment phase, and the authentication phase. Both phases have the same image-processing tasks. First digital face image and fingerprint images are acquired by using the Pi camera module and fingerprint sensor devices respectively. Then the image preprocessing technique is applied. The segmentation process was applied to the image which is then ready for the feature extraction process. The following Fig.1 shows the proposed model architecture.

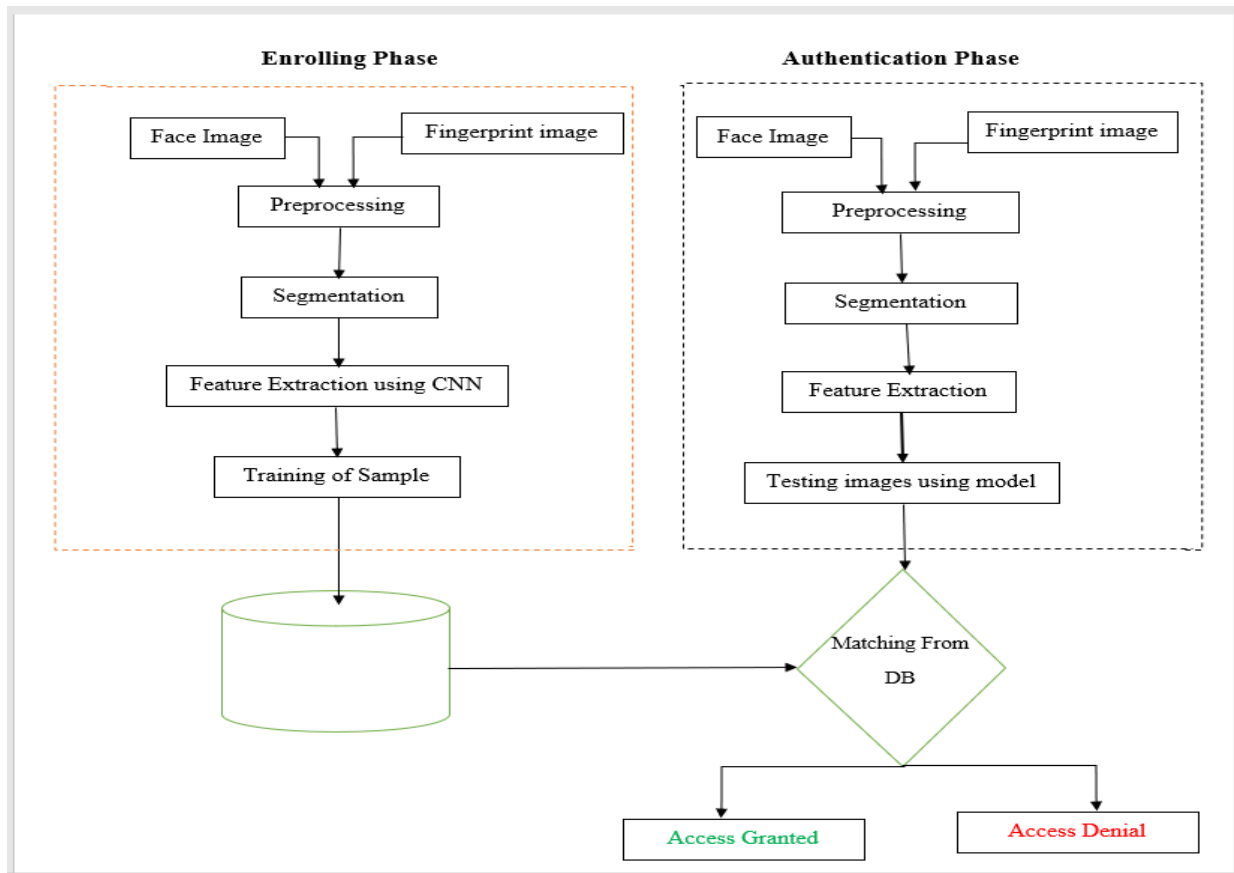


Fig. 1. Proposed Model Architecture

IV. Experimental Setup, Result, and Discussion

A. The Tool Used for the Study

In this research study software and hardware tool was used for conducting an experimental activity. Software tools like Anaconda navigation and Jupiter notebook for the code editor, open-cv library for capturing images and then image processing tasks, Tensor flow, and CNN algorithms for creating the proposed model.

Different hardware tools are also used for experiments. Raspberry Pi is for implementing and controlling the research result, a Pi camera for capturing the user's facial image, fingerprint sensor devices for capturing fingerprint images, and jumper cables for assembling edge devices with a raspberry pi controller. The following Fig.2 shows a highlight of the hardware tools used.

Received: 19 March 2022; Revised: 23 March 2023; Accepted: 27 March 2023; Published: 30 April 2023.

Corresponding author- Gergito Kusse

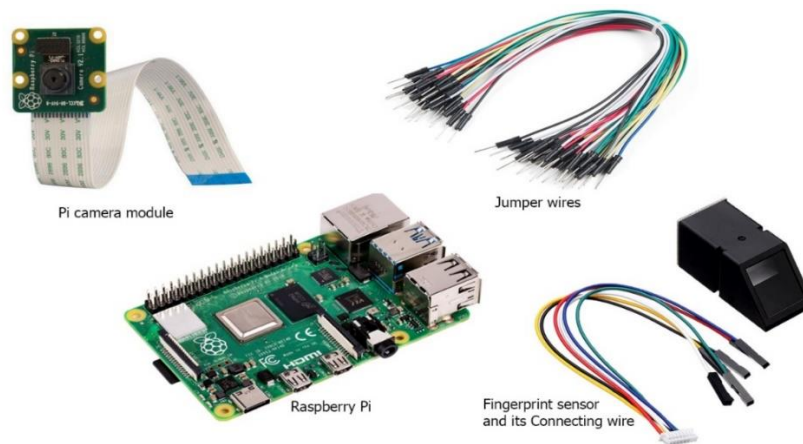


Fig. 2. Hardware tool used for the experiment

B. Experimental Setup

In the previous section tools used for experimenting were discussed in detail. In this section, experimental activities were discussed in the following subsections.

1) *Assembling hardware tools:* As presented in Fig. 3, Jumper wires were used to connect edge devices with Raspberry Pi, the fingerprint sensor has four/six-pin wire (ground, voltage, transmitter, and receiver) was connected to the corresponding pin of Raspberry Pi, camera module was connected to the camera port of raspberry Pi, HDMI cable to connect Raspberry Pi to displaying desktop screen and the USB cable connects raspberry Pi with direct current to provide power.

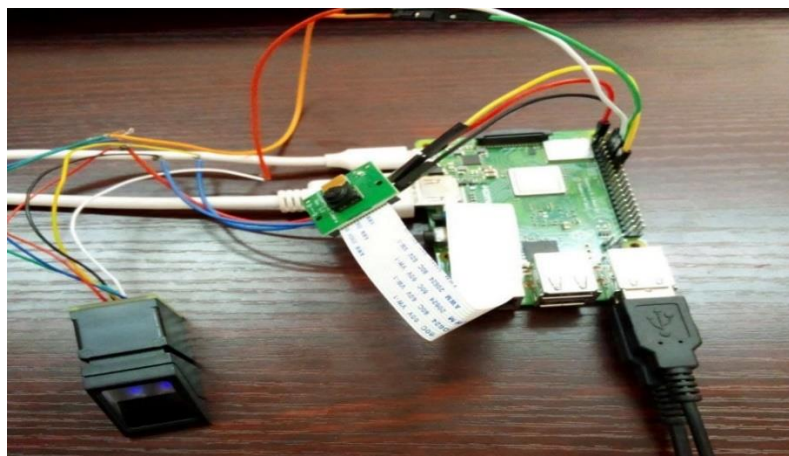


Fig. 3. Assembled hardware tools

C. Enrollment Phase

The main aims of the study were addressed in this enrollment phase. In this phase, how users' image was collected as a dataset of the study, image processing steps, and CNN layer were discussed in detail: -

1) *Datasets (image acquiring)*: Datasets used in this research study were the image of the user's facial image and fingerprint image as presented in Fig. 4 and 5. Those images are captured by the Pi camera module and fingerprint sensor devices which means all the data sets used for the experiment were primary data. To get high accuracy in the proposed model prediction during the enrollment phase 50 users' face image with different (20) angle position was captured by the Pi camera module and two fingerprint images were captured by fingerprint sensor devices. The sample size of data is $50 \times 20 = 1000$ face images and $2 \times 50 = 100$ fingerprint images. The following Fig. 4 shows the collected data set of users.



Fig. 4. Sample dataset user's face image



Fig. 5. Sample dataset of user's fingerprint image



2) *Pre-processing*: first activity of image processing is capturing the image as a dataset. The face region was detected and cropped then resized to 200 X 200 on the face image. Image enhancement and minutiae extraction was applied as a preprocessing task on the fingerprint image.

3) *Segmentation*: segmentation task on the face image is responsible for converting a colored image (RGB) into a grayscale image and then transforming the image into a numerical data array by using the NumPy library. The segmentation process in the fingerprint image was responsible to remove unnecessary or unwanted data from the image. And then ridge flow estimation and region of interest of minutiae were considered under this task.

3) *Feature Extraction*: The feature extraction process was done by using a supervised deep learning method called CNN. The collected dataset of the user's image was split into 70% of the dataset as a training dataset and 30% used as a test dataset. To train the model CNN passes the following four layers: -

a) *Convolution layer*: In this layer, the preprocessed image with 200 X 200-pixel resolution was multiplied by 30 X 30 filter images magically generated by CNN. In this case, 1st filtered image output becomes 171 X 171.

b) *Normalization/Activation layer*: In this layer, non-linear functions called RELU were used to train the dataset and speed up the training process and reduce computational time.

c) *Pooling layer*: The main aim of this layer in CNN is to reduce the dimension of an image which highly probably reduces computational time and avoids overfitting of a proposed model. The max-pooling method was applied to a normalized image. To reduce the dimension of an image, 20 X 20 Max-pooling was applied. So, the first-round max-pooling result was 152 X 152 pixels.

d) *Fully connected layer*: The output of the pooling layer which is a 3D image was converted to a 1D image by applying the flatten method on the image. The output of this layer was used as the input layer for a neural network. The following Fig. 6 shows the summary of feature extraction.

D) Authentication Phase

The main responsibility of this phase is to check whether the captured face image and fingerprint was matching it from the created mode during the enrollment phase and then make a decision



based on the output result. In this authentication process, the first three steps of the image processing task are similar to that of enrolling phase, but the difference is that there is no need to train the captured image rather it tests and then matches it from the trained model. Another difference is that in the case of enrolling phase RELU functions were used as activation functions for training the model, but in the authentication phase Regression function as optimizer and SOFT-MAX were used as the activation function for classifying images to corresponding users.

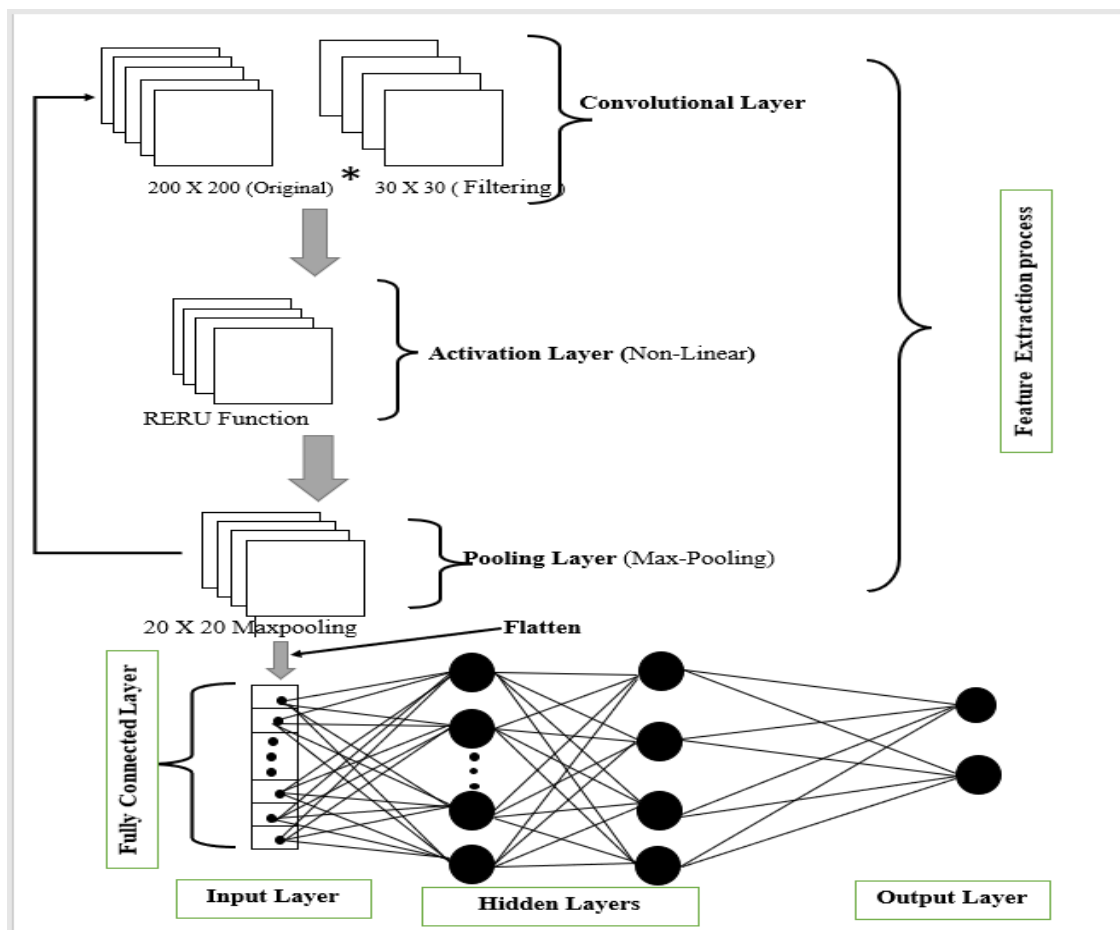


Fig. 6. Feature extraction using CNN

V. Conclusion

IoT system is a highly growing technology that improves the quality of our daily life. So, to ensure the physical security of IoT systems and their operating technology, multimodal biometric authentication systems were designed. In this research work, the unimodal and multimodal



biometric system is discussed in detail after the multimodal system is implemented by using CNN algorithms on both face and fingerprint images. The Relu function was used as an activation function and a max-pooling method for dimension reduction on both images. The softMax function was applied for classification. Three parameters of performance analysis were considered (Accuracy, FAR, and FRR). The result shows that accuracy is 92% and 89% for the face and fingerprint respectively, FAR is 1.35%, and FRR is 1.5%.

Future works: From the results of the experiment, it shows that the accuracy of the fingerprint image is 89%, which still has scope to enhance. So, this research work may be extended for improving the existing accuracy of results or by adding another biometric system.

References

- [1] M. Abomhara, "Cyber security and the Internet of things vulnerabilities, threats, intruder and attacks," *Journal of Cyber security and mobility*, vol. 4, no. 1, pp. 65-88, 2015.
- [2] "TeachTarget," [Online]. Available: <https://www.techtargget.com/searchsecurity/definition/biometric-authentication>, 2022.
- [3] S. Prabu, M. Lakshmanan & V. Noor Mohammed "A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques," *Journal of the medical system (Springer)*, vol.43, no. 249, p. 2, 2019.
- [4] A. H. S. C. Ibrahim Omara, "A Hybrid Model Combining Learning Distance Metric and DAG Support Vector Machine for Multimodal Biometric Recognition," *IEEE Access*, vol. iii, no. 43, p. 3, 2020.
- [5] M. T. M. B. a. N. C. M. Regouid, "Multimodal biometric system for ECG, ear and iris recognition based on local descriptors," *Multimedia Tools Appl*, vol. 78, no. 16, 2019.
- [6] S. J. R. a. p. Norvig, "Artifitial Intelligent in moderen Approach," second edition, United stat of america, 2003.
- [7] Y. B. Y. Lecun, "Deep Learning nature," vol. 521, p. 436, 2015.
- [8] A. M. A. A.-A. Mohammed Ali Al-Garadi, "Servey of Machine and Deep Learning methods for IoT security," *IEEE Communications Surveys & Tutorials*, 2020.

Received: 19 March 2022; **Revised:** 23 March 2023; **Accepted:** 27 March 2023; **Published:** 30 April 2023.

Corresponding author- **Gergito Kusse**



-
- [9] D. V. S. Jasmeen Sharma, "Multimodal biometric authentication using face and fingerprint," *IOSR Journal of Engineering*, vol. 08, no. 4, 2018.
- [10] S. V. a. C. Poellabauer, "Multimodal Biometric-based implicit authentication of wearable devices for the users," *IEEE Transactions on Information Forensics and Security*, 2019.