Face Mask Detection using CNN: A Fusion of Cryptography and Blockchain

Imen Hagui
Laboratory of Micro-Optoelectronics and Nanostructures, University of Monastir, Tunisia
imen.haggui.94@gmail.com (corresponding author)

Amina Msolli
Laboratory of Micro-Optoelectronics and Nanostructures, University of Monastir, Tunisia
amina.msolli@yahoo.fr

Abdelhamid Helali
Laboratory of Micro-Optoelectronics and Nanostructures, University of Monastir, Tunisia
abdelhamid.helali@gmail.com

Hassen Fredj
Laboratory of Micro-Optoelectronics and Nanostructures, University of Monastir, Tunisia
hassenfredj@gmail.com

Received: 13 May 2024 | Revised: 28 May 2024, 3 June 2024, and 4 June 2024 | Accepted: 12 June 2024

 DOI: https://doi.org/10.48084/etasr.7827

ABSTRACT

The global COVID-19 pandemic has led to an urgent need for government intervention to prevent its spread. Scientific evidence has confirmed the effectiveness of mask-wearing in reducing virus spread. However, enforcing mask mandates in public spaces presents notable monitoring hurdles, particularly as facial recognition technology is impeded by face coverings. With many organizations relying on facial recognition for employee authentication, security and authentication become critical, especially for IoT systems. This article uses a Convolutional Neural Network (CNN) model to accurately identify mask-wearing individuals and introduces a secure user authentication mechanism between the node and the access point. This authentication mechanism consists of three phases. (i) Identification Phase at the Access Point Level: A novel hybrid biometric pattern, merging password and image features, is employed to strengthen user authentication security through a fusion approach. (ii) Secure Communication: Utilizing blockchain technology and AES cryptography ensures the secure transmission of these patterns between the node and the access point. (iii) Matching Phase at the Node Level: A newly proposed method verifies authenticity by comparing the combined image and password features with database records during the development phase. The experimental results demonstrate its outstanding performance, achieving 99% accuracy, 99% recall, 100% precision, and 98.9% F1 score. These results suggest that the proposed approach holds promise as an effective and secure solution for identifying individuals wearing masks while ensuring reliable authentication in various environments.

Keywords-Internet of things (IoT); Advanced Encryption Standard (AES); Convolutional Neural Networks (CNNs); blockchain; face recognition

I. INTRODUCTION

Ensuring data security in IoT networks is critical, particularly in the COVID-19 pandemic, where IoT devices play a crucial role in monitoring and enforcing hygiene measures such as mask wear. These devices collect and transmit sensitive information, including personal health data and location details, responding to pressing concerns about data security to prevent privacy breaches and potential misuse. However, as IoT devices become more prevalent, they also become prime targets for cyberattacks, necessitating measures to ensure the integrity and confidentiality of transmitted and stored data. Encryption, authentication, and regular software updates are vital security measures to protect data within the network. In addition, establishing access control protocols allows authorized individuals or systems to monitor the data generated by these devices. As people rely more on technology to combat the pandemic and improve health efforts, prioritizing data security becomes both a technological necessity and a moral obligation to protect individuals' privacy and safety.

In this context, the objectives of this study are outlined as follows:

- Presents a novel process for identifying whether an individual is wearing a protective mask, achieved through the creation, training, and deployment of a CNN for computer vision.
- Proposes an innovative user authentication method to secure communication between the node and the access point, divided into three stages. Initially, a unique hybrid biometric pattern is crafted by blending password and image features, enhancing user authentication security. Subsequently, AES cryptography and blockchain technology are utilized to secure the communication of patterns between the node and the access point. Lastly, a matching procedure is employed to verify the user's authenticity by cross-referencing their password and image features with the data stored in the database.

The main contributions of this study are as follows:

- Use CNN and the Haar cascade classifier to detect faces with and without masks.
- Improve the security of the authentication process, using an image and password merging approach.
- Employ the AES algorithm to provide an additional security layer to the hybrid pattern.
- Use blockchain to secure transmissions between the node and the access point.
- Finally, devise a matching approach to assess the correspondence of the access point's password and image features with those saved in the node database. The proposed method achieves impressive accuracy (99%), recall (99%), and F1 score (98.9%).

II. RELATED WORKS

Protecting data is crucial today, especially with the rise of technologies such as cryptography, blockchain [1], and CNNs, particularly in IoT. Encryption techniques aim to secure sensitive data along with key management to prevent unauthorized access. Technology can implement these security techniques and add a security layer at the same time. Blockchain is the most powerful technology used to protect data in a decentralized and immutable network. Cryptography secures data exchange among IoT devices and forms a distributed ledger. Previous studies have highlighted the importance of advanced security measures to mitigate security risks in IoT.

Biometric systems are susceptible to external attacks [2]. In [2], various attack and vulnerability scenarios were explored within conventional biometric authentication processes, encompassing the input, point, match, and decision stages. Preventing and detecting attacks at entry points have been the subject of extensive research [3]. In [4], a transparent method was presented to handle a point-based sensor system. This method can facilitate the integration of these technologies while improving security measures. Blockchain technology has shown significant benefits in various fields. The proposed biometric identification system used an exclusive blockchain, improving protection actions and creating consensus even within a tumultuous environment. A Merkle tree structure was used for decentralized functionalities and secure pattern matching. This investigation included the development of a secure implementation mechanism, employing biometrics and blockchain technology, acquiring model parameters for informed decision-making through both visual and auditory modalities.

In [5], an approach was presented to secure sensor data saved on a cloud server in an IoT-based smart agriculture system. This approach merged RNN and ECC with blockchain. This method increased security and performance, achieving 2.57% better accuracy, hinting ability, and decreasing encryption and decryption times by 2.7 and 2.6 ms, respectively. In [6], the Public Key Encryption with Equality Test (PKE-OET) was proposed to secure outsourcing scenarios in cloud-based IoT settings, involving an additional reclamation attack signature scheme. In [7], a flexible authentication and key management approach (EKAFAS) based on ECC was proposed for cloud-based wireless sensor networks in the IoT context. This technique includes two levels of security measures: an angular-based CFG rule technique at the node level for identifying certain nodes, and an ECC key-matching verification process for user-level security to swiftly detect and exclude any malicious users from the communication system. In [8], an innovative critical consensus method was developed based on blockchain, named AgroMobiBlock, specifically designed for mobile agricultural vehicles in precision agriculture IoT networks. This innovative method incorporates elliptic curve functions to reduce completion time and cost. In [9], a detection work on a Blockchain IoT (BIoT) structure was presented. The decision-making process was based on data obtained by IoT devices on the blockchain. The possibility of performing such things within a limited time and a finite blockchain block was also examined. Kullback-Leibler Divergence (KLD) is a crucial statistical test to evaluate detection performance.

In [10], a face mask recognition algorithm was proposed using transfer learning. This study focused on utilizing CNNs to extract highly accurate information from various facial images. Then, various machine learning classifiers were used to evaluate the extracted features. In [11], a model was introduced to recognize masked faces, combining deep transfer learning with conventional machine-learning classifiers. This model was built to examine the identity of individuals who do not adhere to face mask use and be applied to surveillance cameras as a proactive measure against COVID-19 spread. This algorithm used a hybrid method, combining deep transfer learning with conventional device learning algorithms. In [12] a swift and precise face mask detection model was introduced for edge computing. The model uses the MobileNetV2 structure to extract significant features from the input data and transmit them to an autoencoder to create more abstract representations.

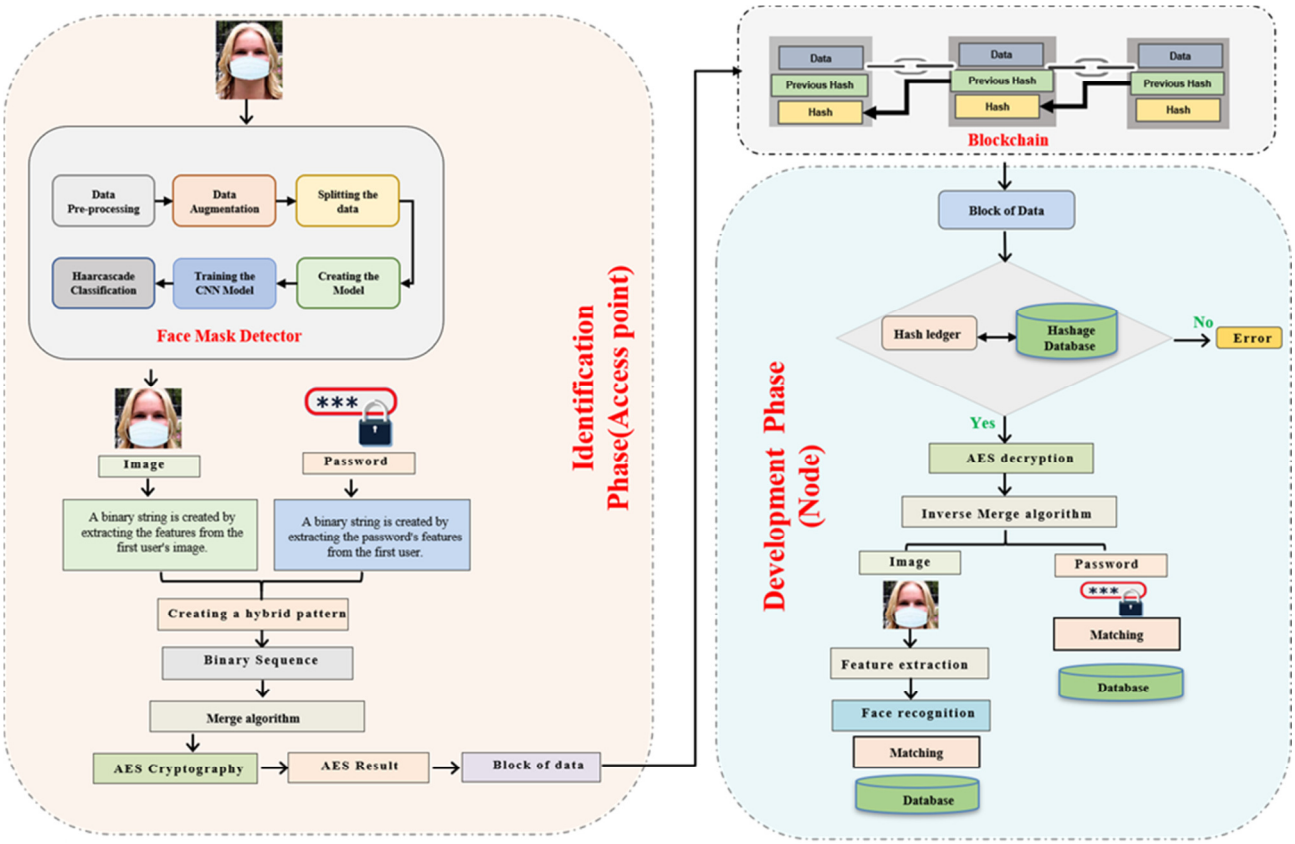

Fig. 1. The proposed secure authentication framework.

III. PROPOSED APPROACH

During the COVID-19 pandemic, issues such as alteration of image content and masked images emerge, requiring more robust security verification methods. The first phase uses an innovative strategy based on a password and image to improve randomness, presenting matching technology that uses both features. Integration with blockchain in the second step adds an encryption function that is critical for system security during authentication. Figure 1 shows the structure of the proposed method as it is implemented at access points and nodes.

A. Flowchart of the Face Mask Detector

Figures 1 and 2 show the procedures necessary to identify a face mask.

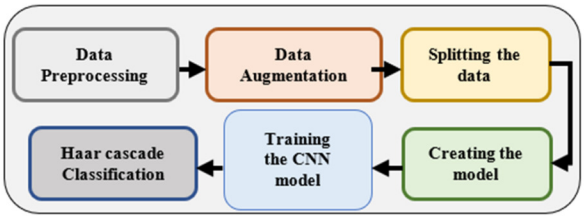

Fig. 2. Flowchart of the face mask detector.

1) Data Preprocessing

Two preparatory steps were followed. Initially, each image was converted from RGB to grayscale. In a color image, there are three channels (one for each color), whereas a grayscale image has only one channel, representing the gray level for each pixel. Subsequently, the image was resized to decrease the complexity of the CNN model and reduce the computational power needed for training the model. Figure 3 illustrates the data preprocessing steps.

Fig. 3. Data preprocessing.

2) Data Augmentation

Data augmentation is a technique for creating new training images that preserve the original class labels. It is performed by inserting random changes and distortions into existing training images. Its goal is to increase the model's ability to generalize effectively. Typically, an image data generator is used to enhance the dataset before testing, taking the original data and applying arbitrary modifications to produce augmented data.

This procedure involves rotating and flipping each image to increase the dataset size for training purposes. Following data augmentation, the dataset now contains 2751 photos, with 1380 in the "with mask" class and 1371 in the "without mask" class.

3) Creating the Model

The model design includes the following:

- Incorporates two convolutional layers that utilize a 3×3 convolutional window and employ a ReLU activation function. The initial convolutional layer generates 200 feature maps, while the second layer produces 100 feature maps. Stride and padding configurations remain unchanged.
- Integrates two max-pooling layers with a 2×2 window size.
- Features two fully connected layers: a hidden layer consisting of 50 neurons and an output layer with two neurons, each corresponding to a specific class. To compute class probabilities, a softmax activation function is applied. Figure 4 illustrates the architecture of the CNN model.

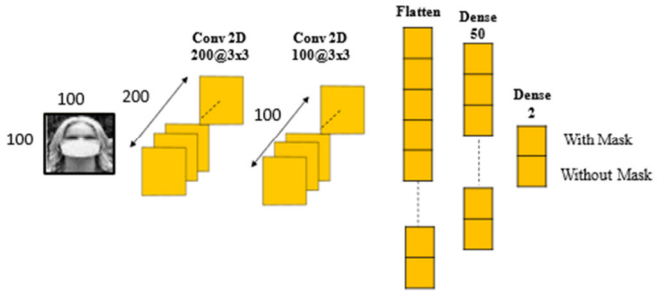

Fig. 4. CNN architecture.

The model was trained for 20 epochs to achieve higher accuracy and avoid overfitting.

4) Haar Cascade Classification

The Haar cascade classifier utilizes the Haar wavelet approach to divide pixels in an image into squares based on their functions. Detected features are computed using integral image principles. This classifier uses the AdaBoost learning algorithm, selecting a small number of critical features from a large set to produce effective results. Classifiers then use cascading techniques to recognize faces in images, resulting in a cascade of increasingly sophisticated classifiers. This cascade focuses computation on regions resembling potential objects by eliminating all nonface regions from an image. Figure 5 illustrates the Haar cascade classifier functionality in this study.

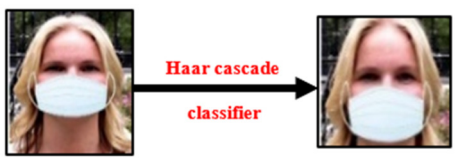

Fig. 5. Haar cascade classifier.

B. Secure Verification Framework

The secure authentication mechanism is divided into two main phases: identification and development. The identification phase encompasses a variety of actions. Initially, it involves creating a hybrid pattern by combining password and image features. The hybrid pattern is then encrypted using AES. The methods in the identification phase are inverted to extract image features from password characteristics. Finally, a matching procedure occurs, where the retrieved characteristics are matched to related entries in the database.

1) Access Point

The initial phase, known as the identification phase, is the system's entrance point and aims to establish the requirements for the hybrid model, such as feature extraction methods and information security standards. This phase establishes the basis for introducing a novel hybrid model within the verification framework, which uses a combination of password and image features to improve randomization and security within the pattern structure. This phase includes detailed processes that display primary data entry results and the necessary data types for each processing stage. Key processes involve creating a hybrid pattern and encrypting it using AES.

a) Creation of a Hybrid Pattern

The proposed fusion method is crucial in combining two crucial features, image and password characteristics, associated with users. It serves as the basis for creating duplex configurations, showcasing the hybrid approach's flexibility. This method involves real-time image features, precisely tailored to image dimensions, alongside a 34-bit word point, enhancing model complexity and precision. This detailed model includes an initial layer of protection that acts as the first line of defense against security risks. The fusion of image and password features is delicately managed to exceed strict random number requirements, ensuring system security and performance. This rigorous approach ensures the highest degree of randomness and unpredictability, bolstering the system's resilience.

b) Hybrid Pattern Encryption with AES

The AES encryption algorithm is employed to secure the hybrid pattern, providing an additional layer of protection. This encryption ensures the secure transmission of the encrypted pattern using blockchain technology. Processing takes place on the access point device, where the encrypted pattern is prepared for transmission to the node side. This process encompasses both the processing and preparation phases.

c) Transfer to the Node Side

Blockchain is employed to segment the data into distinct blocks, each subsequently undergoing encryption. The user pattern, originating from the node and the access point, forms an encrypted pattern that is improved with hashes. Within this chain, each successive user, excluding the first, summarizes the information of the preceding user. Consequently, a continuous data blockchain is established, forging an uninterrupted connection from source to destination.

2) Node

In this stage, a new hybrid authentication method is proposed, which combines passwords and images. For cloud users, the identity verification process, using hash values and encrypted patterns, is recommended for authorized block-level access to the data. An e-ledger, using blockchain, is recommended for hash comparisons to validate the originality of the data. Successful verification using AES ensures that only authorized persons can access the system. Using this system, users have two-level protection. The first level of protection is a user-defined hybrid pattern. This hybrid pattern will mostly contain biometric models and creative matching methods to protect the original user from an impersonator. In the context of matching between the two images, the user process begins with the image obtained by the inverse merge algorithm, from which the LBP features are extracted. These features capture critical texture information and are then used in the face recognition phase to compare and match the extracted features with those stored in the database. This method ensures accurate verification of the user's identity by effectively distinguishing between different facial textures. In this way, this meticulous verification process increases the integrity of the security system.

IV. VALIDATION

A. Datasets

1) Mask Dataset

This study utilized an open-access dataset including 1279 images [13]. These images are divided into two main categories: with mask and without mask.

2) Password Dataset

A dataset of passwords was generated, comprising their first names, last names, emails, passwords, and gender. Table I presents a sample of the password dataset.

TABLE I. PASSWORD DATASET

First name	Last name	Email	Gender	Password
Stannislas	Munndle	ssmundle00@mail.com	Male	AtqL3qeyYX7
Shaarona	Pedraacci	shpedracci12@diigo.com	Female	aEDg5TTkmKpaZ
Gustavv	Elldersha w	gueldershaw25@ucoz.edu	Male	9dmeJM3r8Gk6
Waasha	Abigail	washaAbig38@cmu.edu	Male	p04IB0b59wt

B. Validation

The proposed framework was evaluated to determine whether the objectives were met. The model was trained over 15 epochs to measure loss and sensitivity. The efficiency of the model was evaluated with 20% of the data. The proposed method was developed using Python 3.8.7. The experiments were carried out on a PC with an Intel Core i7-4790 CPU, operating at 3.60 GHz with 8.00 GB of RAM. Computational costs were assessed in terms of processing time and resource utilization. During deployment, the average time to process and classify an image was measured at 0.05 s. This rapid processing time ensures that the system can operate efficiently in real-time applications. Furthermore, the energy consumption of the system confirms its suitability for resource-constrained IoT environments. The techniques implemented ensure minimal energy usage while maintaining high performance, making the system both effective and efficient for practical deployment. Figure 6 illustrates the training and validation loss.

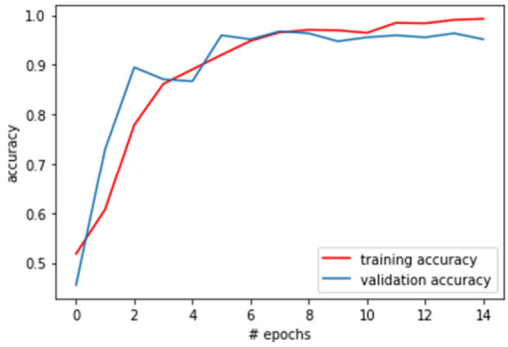

Fig. 6. Training and validation accuracy.

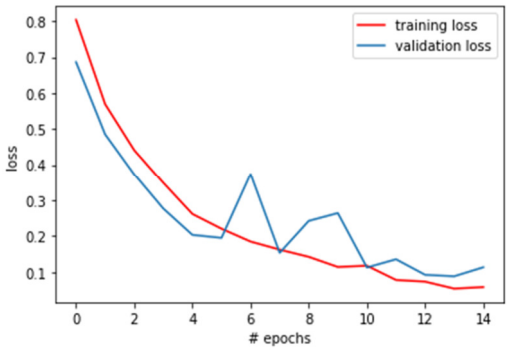

Fig. 7. Training and validation loss.

These results indicate that the model may be fitting the training set precisely. Considering the dataset's dimensions used for training the model, accuracy consistently approaches a total of approximately 97% within the validation set. When evaluated in the test dataset, the model achieved a score of 97.10 with a loss of 0.09, indicating performance improvement.

C. Performance Evaluation

Throughout the training and testing phases, the model's performance was measured using precision, recall, F1-score, and accuracy, using the following equations. True positives, false positives, true negatives, and false negatives are all abbreviated as TP, FP, TN, and FN, respectively.

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$F1 - score = 2 \times \frac{precision \times recall}{precision + recall} \quad (3)$$

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \quad (4)$$

Table II provides a detailed comparison of two datasets, one with and one without a mask.

TABLE II. COMPARISON BETWEEN TWO DATASETS; WITH AND WITHOUT MASK.

	Accuracy	**Recall**	**Precision**	**F1-score**
Dataset with and without masks	0.992	0.99	1.00	0.989
Dataset without masks	0.989	0.976	1.00	0.978

Many studies focused on face mask detection, underscoring the increasing importance of enhancing detection accuracy as a preventive measure against the spread of the COVID-19 virus. Table III compares the performance of the proposed with other models [10-12] to assess its efficacy.

TABLE III. COMPARISON BETWEEN THE PROPOSED MODEL AND OTHER STATE-OF-THE-ART MODELS.

	Accuracy	**Recall**	**Precision**	**F1-score**
[10]	0.9711	0.9508	0.9484	-
[11]	0.9964	0.9963	0.9963	0.9945
[12]	0.9998	0.9997	0.9996	0.9997
Proposed model	0.992	0.99	1.00	0.989

In general, compared to other methods that combine image-based passwords in the authentication process, the proposed method appears promising in terms of performance.

V. CONCLUSION

This paper presented an automated procedure using computer vision and CNNs to recognize mask-wearing individuals, which is critical for public health and security monitoring, and a security model that incorporates password and image elements into an authentication framework based on blockchain and cryptography, fulfilling high-security requirements. The challenge of regulating data flow is handled, with excellent metrics such as 99% accuracy, 99% recall, 100% precision, and 98.9% F1 score. In addition, the proposed approach ensures the hybrid pattern's security during data transfer. In the future, algorithm efficiency and security will be improved by examining other encryption algorithms, such as Shift AES, and the proposed method will be implemented on an FPGA platform.

REFERENCES

[1] N. K. Al-Shammari, T. H. Syed, and M. B. Syed, "An Edge – IoT Framework and Prototype based on Blockchain for Smart Healthcare Applications," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7326–7331, Aug. 2021, https://doi.org/10.48084/etasr.4245.

[2] G. Held, "Enhancing Security," in *The ABCs of TCP/IP*, 2nd ed., Auerbach Publications, 2003.

[3] N. Akhtar and A. Mian, "Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey," *IEEE Access*, vol. 6, pp. 14410–14430, 2018, https://doi.org/10.1109/ACCESS.2018.2807385.

[4] M. Qiu, Ed., Smart Blockchain: First International Conference, SmartBlock 2018, Tokyo, Japan, December 10–12, 2018, Proceedings, vol. 11373. Cham, Switzerland: Springer International Publishing, 2018.

[5] N. Mahalingam and P. Sharma, "An intelligent blockchain technology for securing an IoT-based agriculture monitoring system," *Multimedia Tools and Applications*, vol. 83, no. 4, pp. 10297–10320, Jan. 2024, https://doi.org/10.1007/s11042-023-15985-8.

[6] S. Ma, Y. Zhong, and Q. Huang, "Efficient Public Key Encryption With Outsourced Equality Test for Cloud-Based IoT Environments," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3758–3772, 2022, https://doi.org/10.1109/TIFS.2022.3212203.

[7] V. Thirunavukkarasu, A. S. Kumar, P. Prakasam, and G. Suresh, "Elliptic curve cryptography based key management and flexible authentication scheme for 5G wireless networks," *Multimedia Tools and Applications*, vol. 82, no. 14, pp. 21131–21145, Jun. 2023, https://doi.org/10.1007/s11042-023-14539-2.

[8] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023, https://doi.org/10.1109/TIFS.2022.3231121.

[9] Y. Jiang and J. Zhang, "Distributed Detection Over Blockchain-Aided Internet of Things in the Presence of Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3445–3460, 2023, https://doi.org/10.1109/TIFS.2023.3279984.

[10] A. Oumina, N. El Makhfi, and M. Hamdi, "Control The COVID-19 Pandemic: Face Mask Detection Using Transfer Learning," in *2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS)*, Kenitra, Morocco, Dec. 2020, pp. 1–5, https://doi.org/10.1109/ICECOCS50124.2020.9314511.

[11] M. Loey, G. Manogaran, M. H. N. Taha, and N. E. M. Khalifa, "A hybrid deep transfer learning model with machine learning methods for face mask detection in the era of the COVID-19 pandemic," *Measurement*, vol. 167, Jan. 2021, Art. no. 108288, https://doi.org/10.1016/j.measurement.2020.108288.

[12] S. Habib, M. Alsanea, M. Aloraini, H. S. Al-Rawashdeh, M. Islam, and S. Khan, "An Efficient and Effective Deep Learning-Based Model for Real-Time Face Mask Detection," *Sensors*, vol. 22, no. 7, Jan. 2022, Art. no. 2602, https://doi.org/10.3390/s22072602.

[13] "Covid-19-PIS Classification Dataset by PyImageSearch." Roboflow, [Online]. Available: https://universe.roboflow.com/pyimagesearch/covid-19-pis.