Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1901–1909
DOI : 10.47974/JIOS-2019

Facial authentication-based smart door lock system and anomaly detection using machine learning architectures integrated with IoT

Morched Derbali *
Mutasem Jarrah †
Department of Information Technology
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah
Saudi Arabia

Ahmed Harbaoui §
Department of Computer Science
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah
Saudi Arabia

Kamel Taher khoualdi ‡
Department of Management Information Systems
Faculty of Economics and Administration
King Abdulaziz University
Jeddah
Saudi Arabia

This manuscript contains self-plagiarism, which is from a preprint publication authored by the corresponding author (Morched Derbali) itself.

* *ORCID-ID:* **0000-0001-9965-8184**
† *ORCID-ID:* **0000-0002-4260-8407**
§ *ORCID-ID:* **0000-0002-0764-8438**
‡ *ORCID-ID:* **0000-0002-8499-6153**

* *E-mail:* **mderbali@kau.edu.sa (Corresponding Author)**
† *E-mail:* **mmjarrah@kau.edu.sa**
§ *E-mail:* **aharbaoui@kau.edu.sa**
‡ *E-mail:* **kkhoualdi@kau.edu.sa**

© Taru Publications

Abstract

This work comprises two components: home security and reconnaissance, as well as remote entryway exchange with a greeting framework. The first step for the user is to install the security and surveillance hardware components of the system. A growing number of people are considering installing smart home systems as a result of the proliferation of IoT devices. Security and access control are important components of the smart home system. This paper details the development of a facial recognition security framework that makes use of Raspberry Pi, which is regularly integrated with smart home systems. An SDL system that relies on face authentication and intrusion detection is the goal of this project, which intends to use machine learning architectures and the internet of things (IoT). To secure this smart door, biometric authentication based on face recognition is utilized. Next, we employ the DeSGCBQNN, which stands for distributed encoder Shannon-Gaussian Correlation Bayesian Q-neural networks, to spot outliers. We completed the trial examination for several smart entrance face datasets in terms of mean square error, false acceptance rate, false rejection rate, mean average precision, and accuracy. The proposed approach achieved a 98% success rate, a 66% mean average precision, a 65% false acceptance rate, a 55% false rejection rate, and a 53% mean square error.

Subject Classification: *68T10, 68T45, 94A62.*

Keywords: *Smart door lock, Facial authentication, Intrusion detection, Machine learning, Internet of Things.*

1. Introduction

Human life has always prioritized safety and security, with traditional physical locks providing peace of mind. However, keys and locks are now considered vulnerable, as they can be lost, stolen, or duplicated, leading to unauthorized access [1]. Advances in technology, particularly artificial intelligence, have enabled modern security systems, such as smart locks, which allow remote access and control. Relying on unimodal systems, like a single biometric trait, remains insufficient for reliable monitoring and identification, highlighting the need for intelligent, multi-layered security [2]. This research proposes a smart door lock (SDL) system that integrates facial authentication with machine learning-based intrusion detection. The design is cost-effective, flexible, and suitable for various indoor and outdoor settings. A key feature is remote access via the internet, while the prototype simulates real-time entry using an LCD-based greeting system [3]. Facial recognition enhances security, leveraging the uniqueness of individual faces to prevent forgery and unauthorized access, ensuring robust, intelligent protection for users.

2. Existing SDL based on Machine Learning Techniques

Modern home security technologies include RFID cards, biometrics, OTP-based unlock systems, and more. While effective in specific scenarios, these approaches do not provide complete security. Although home security systems have been widely researched, only a few have adopted facial recognition [4],

which holds significant potential for reliable authentication [5]. A framework using Local Binary Patterns (LBP) and Support Vector Machine (SVM) demonstrated promise but lacked reliability during power failures [6]. Digital door locks with key sharing and mobile-based remote control were studied [7], while other models transmitted images of accessing individuals for detection [8]. Voice recognition-based locks without internet reliance were explored [9]. Bluetooth-enabled Android applications [3], or inter-device communication for alarm signaling [1], were proposed. Face recognition-based unlock systems [2] often lacked remote control, limiting IoT applicability. Additional studies integrated security with home automation, webcam-based intruder alerts, and Raspberry Pi-based facial recognition, though performance declined in poor lighting. Multi-layered PCA-based face recognition systems and MATLAB-based biometric security solutions were also developed for secure access.

3. Proposed Facial Authentication-based Anomaly Detection using Machine Learning

We began by researching new ideas and selecting an energy-efficient, cost-effective method. Based on our goals and requirements, we identified the necessary components. Instead of using Arduino, we experimented with the Bolt IoT Wi-Fi module. We then designed a rectangular-shaped lock to fit all key parts and attach securely to a door. Finally, we considered real-time environmental factors during the simulation phase to ensure the design's practical effectiveness and reliability.

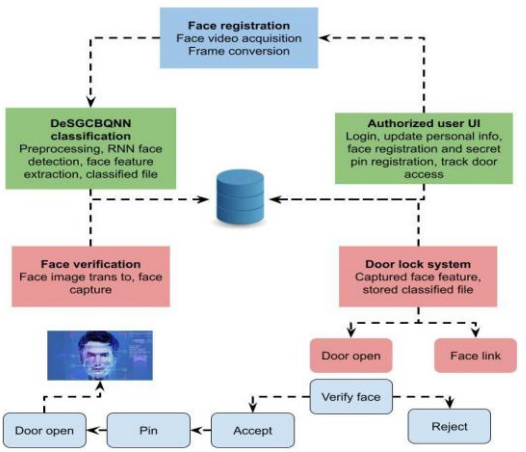


Figure 1
System for smart door locks that rely on facial recognition

2.1 *Facial authentication based smart door lock system with IoT*

This method improves security by using facial recognition instead of keys, which can be lost or misused. It automatically detects and matches a person's

face from live video with stored images of authorized users. Figure 1 illustrates the main procedures for real-time deployment. The prototype uses a Raspberry Pi 3B+ running Raspbian Stretch OS, accessed via SSH with a VNC server for remote desktop control. The Pi manages multiple tasks, including monitoring a proximity sensor, triggering the camera to capture images, sending them to the cloud, and receiving commands to control the door lock. When access is granted, the user ID is displayed on an LCD screen.

A camera module captures images based on two triggers: a push-button doorbell or detection by an IR-based proximity sensor. A LED bulb represents the door switching mechanism, activated via mobile app commands sent through the cloud. Figure 2 shows the LCD module.

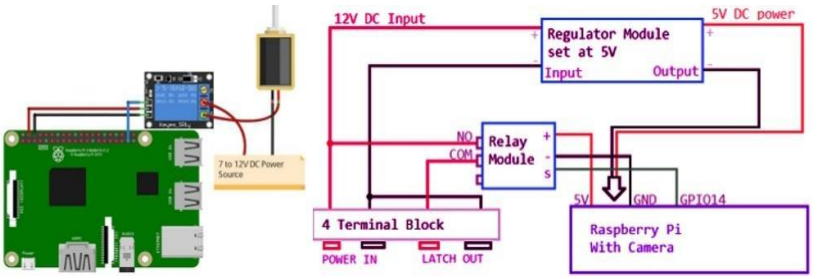


Figure 2
Proposed Facial authentication based smart door lock module

In the proposed system, the Raspberry Pi acts as the central controller, managing sensors and a camera. When an IR sensor detects someone near the door for over ten seconds, the Pi activates the camera to capture an image. This image is uploaded to an S3 bucket named "Visitors," triggering a Lambda function that uses AWS Recognition to compare the image with a "Known" database. If the match confidence is 90% or higher, the person's ID is returned; otherwise, they're labeled "unknown." A notification, along with the image and label, is sent to the registered app. When the doorbell is pressed, the Pi captures another image with a five-second delay to avoid duplicates. If the user chooses to unlock the door, a confirmation prompt appears. Upon approval, a status value (0 or 1) is updated in DynamoDB and read by a Lambda, instructing the Pi to toggle the lock and display a welcome message on the LCD if the visitor is known.

2.2 *Distributed encoder Shannon Gaussian Correntropy Bayesian Q-neural networks (DeSGCBQNN) based face detection of anomaly analysis*

The encoder maps input data x to latent space z using $E(x) = f(W_E x + b_E)$, with W_E of size $N_z \times N_x$ and bias b_E. The generator G reconstructs x from z, minimizing L2 reconstruction loss $L_{rec} = E_{x \in X} \parallel x - G(E(x)) \parallel^2$. To reduce Jensen-Shannon Divergence $JSD(p_G \parallel p_{X_{nor}})$, the generator and discriminator are parameterized as $G = (W_G, b_G), D(x) =$

$f_D(W_D x + b_D)$, where f_D is a non-linear function like sigmoid. Discriminator parameters θ_D are optimized using a gradient-based method before updating generator parameters θ_G.

$$\theta_D^{(k)} = \theta_D^{(k-1)} + \eta \cdot Adam\left(\nabla_{\theta_D} F\left(\theta_D^{(k-1)}, \theta_G\right); \beta_1, \beta_2\right) \quad (1)$$

$$\theta_D^*(\theta_G) = \lim_{k\to\infty} \theta_D^{(k)} \quad (2)$$

$$\theta_E = \theta_E - \eta \cdot Adam\left(\nabla_{\theta_E} L_{rec}(x; \theta_E, \theta_G^*); \beta_1, \beta_2\right) \quad (3)$$

The gradient of loss function F with respect to G is updated using Adam. For every θ_G update, there are multiple updates for θ_D, reducing reconstruction error through an additional auto-encoder.

$$L_{rec}(x; \theta_E, \theta_G^*) = E_{x\in X_{nae}} \parallel x - G(E(x; \theta_E); \theta_G^*) \parallel^2 \quad (4)$$

from which we obtain by eq. (5)

$$\theta_E^* = argmin_{\theta_E} L_{rec}(x; \theta_E, \theta_G^*) \; and \; z_{oprimal} = E(x; \theta_E^*) \quad (5)$$

Here, the encoder's ideal parameter is denoted by θ ∗ E. The encoder parameter ΘE is optimized by applying equation (6).

$$\theta_G = \theta_G - \eta \cdot Adam\left(\nabla_{\theta_G} F\left(\theta_D^{(k)}, \theta_G\right); \beta_1, \beta_2\right) \quad (6)$$

$$X_k^{'r}(i) = X_k^r(i) + \epsilon_k(i) \quad (8)$$

$$R(s, a) = \sum_{s'\in S} \quad P_a(s \mid s', a) R(s', a) \quad (9)$$

$$P_a\left(s_{t+1} = s_j \mid s_t = s_i, a\right) = \sum_{j=1}^{3} \quad \alpha_{i,j} \beta_{i,j}^{(a)}, i = 1,2,3 \quad (10)$$

$$Q^\pi(s, a) = E_{s,a,s'}\left[R(s, a) + \gamma \max_{a'\in A}\left(Q(s', a')\right)\right] \quad (11)$$

A particular distributional Bellman equation is depicted in Equation (12).

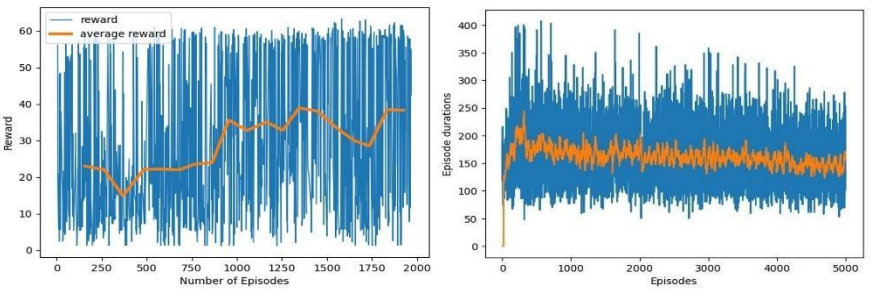
$$Z(s, a) =^D E_{s,a,s'}\left[\left(R(s, a) + \gamma \max_{a'\in A} Z^\pi(s', a')\right)\right] \quad (12)$$

$$\tau^* Z(s, a) =^D E_{s,a,s'}\left[\left(R(s, a) + \gamma Z\left(s', \pi^*(s')\right)\right)\right] \quad (13)$$

In the reinforcement learning (RL)-based Intrusion Detection System (IDS) engine, several key parameters and symbols are defined. $\in_{K(i)}$ represents normally distributed adaptive noise added to the k-th feature at the i-th time stamp of the r-th healthy component. The set S denotes the states in the IDS, including s0 (normal), s1 (detection), and s2 (no detection). Based on the attack probability, the IDS has four alternative actions (low, medium, high, and critical). $R(s, a)$ is the system-optimized reward function that shows the return for action an in-state s. The likelihood of going from state s_j to s_i after doing action an is specified by the transition probability matrix, Pa, which is $P(s_i \mid s_j$, a). The relevance of future benefits is controlled by the discount factor, γ, which can be anywhere from 0 to 1. Qπ represents the estimated value function for a policy π, while $Z(s, a)$ is a random variable that captures the return of taking action a in state s, calculated as the discounted sum of rewards. The transition probability matrix B_a is normalized by the condition $\sum_{(j=1)}^{3} \beta(\mathrm{i,j})^{\mathrm{a}} = 1$.

4. Experimental Analysis

We propose a Raspberry Pi-based face recognition door lock system using OpenCV and Python to identify unknown individuals. The DAD system was evaluated using NSL-KDD, UNSW-NB15, and DS2OS datasets. A DRL agent with a 0.0001 learning rate achieved optimal convergence, while the Corr entropy method dynamically estimated adaptive baselines, improving anomaly detection and attack-type differentiation.

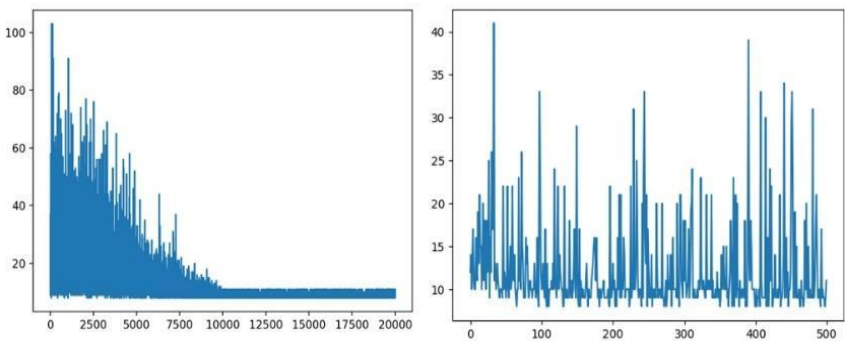


(a) (b)

Figure 3

(a) DRL agent training penalties, (b) kurtosis values of a subset of feature vectors drawn from the NSL-KDD dataset.

The evaluation of the proposed intrusion detection system was conducted on three benchmark datasets: NSL-KDD, UNSW-NB15, and DS2OS, each using 350,000 data samples.



(a) (b)

Figure 4

(a) The kurtosis values of a subset of the feature vectors drawn from the UNSW-NB15 dataset, and (b) the kurtosis values of a subset of the feature vectors drawn from the DS2OS dataset.

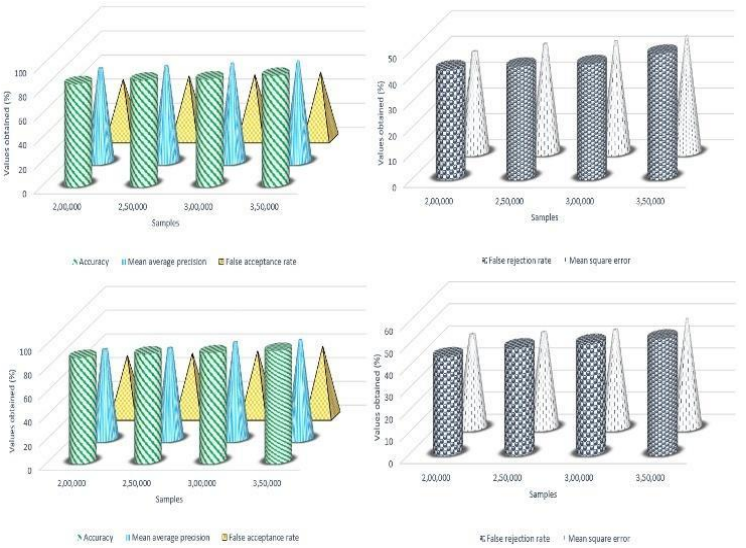


Figure 5
Evaluation standards for the NSL-KDD and UNSW-NB15 datasets based on proposed techniques

Figure 5 presents the evaluation criteria for the NSL-KDD dataset, where the system achieved 92% accuracy, 83% mean average precision, 55% False Acceptance Rate (FAR), 49% False Rejection Rate (FRR), and 45% Mean Squared Error (MSE). Table 1 compares the performance across these datasets. The proposed system effectively detects rare and complex attacks such as R2L and U2R in NSL-KDD and Worms, Shellcode, Fuzzers, and Backdoors in UNSW-NB15. Common attacks like DoS and Probing are detected with near 100% accuracy. This effectiveness is due to the dynamic estimation of normal profiles and Correntropy boundaries under the Gaussian Mixture Model (GMM). As shown in Figures 3 and 4, Correntropy values differ notably between normal and attack vectors. The system can process ten records per second and requires about 72 seconds to train 350,000 samples.

Table 1
Evaluation criteria across multiple cyber-attack datasets.

Samples (S)		**200,000**	**250,000**	**300,000**	**350,000**
NSL-KDD dataset	Accuracy	85	88	89	92
	Mean average precision	77	79	81	83
	FAR	49	52	53	55
	FRR	43	44	45	49
	MSE	39	42	43	45
UNSW-NB15 dataset	Accuracy	89	92	93	95
	Mean average precision	75	76	81	83

Contd...

	FAR	51	53	55	59
	FRR	45	49	51	53
	MSE	42	43	44	49
DS2OS dataset	Accuracy	92	95	96	98
	Mean average precision	61	63	65	66
	FAR	55	61	63	65
	FRR	48	51	53	55
	MSE	45	48	51	53

5. Conclusion

This study presents a novel facial verification system using an SDL-based framework and AI-driven intrusion detection. It integrates a remote door lock mechanism and home surveillance architecture using Python and OpenCV. The prototype, tested across various scenarios, achieved 98% accuracy, 66% mean average precision, 65% FAR, 55% FRR, and 53% MSE. The facial recognition output controls a relay to lock/unlock a magnetic door lock, ensuring high reliability and real-world applicability for multi-door security and surveillance systems.

Acknowledgement

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number 262684 - GPIP: 1697-611-2024 and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

References

[1] T. K. Mohammed, D. N. Vasundhara, S. H. Mehanoor, E. Sreedevi, P. R. Kumar, C. Manihass, and S. F. Baba, "A novel fusion approach for advancement in crime prediction and forecasting using hybridization of ARIMA and recurrent neural networks," *Journal of Information Systems Engineering and Management*, vol. 10, no. 38, pp. 404–420 (2025).

[2] M. Hanif, U. Shahzad, I. Shahzadi, and N. Koyuncu, "Stochastically increasing grouped data using the MLE of mean of the generalized exponential distribution," *TARU J. Organ. Behav. & Analytics*, vol. 1, no. 1, pp. 65–82 (2019).

[3] D. Goyal, A. Kumar, and D. S. Jat, "Special issue on advancements in intelligent systems for information optimization in cyber security: Challenges and innovations (Part-B)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. i–viii (2025).

[4] H.-C. Cheng, M.-C. Chiu, and C.-M. Chiu, "A lighting system using multiple climate sensors in conjunction with remote monitoring network," *TARU J. Comput. Dyn. Technol. Adv.*, vol. 1, no. 1, pp. 21–38 (2019).

[5] S. Sharma, A. K. Patel, and N. Menaria, "Integral transform of product of generalized k-Bessel function and generalized Hurwitz-Lerch Zeta function," *Journal of Interdisciplinary Mathematics*, vol. 27, no. 8, pp. 1757–1764 (2024).

[6] B. Shilpa, P. R. Kumar, and R. K. Jha, "Spreading factor optimization for interference mitigation in dense indoor LoRa networks," in Proc. IEEE IAS Glob. Conf. Emerg. Technol. (GlobConET), pp. 1–5 (2023).

[7] P. R. Kumar and B. Shilpa, "An IoT-based smart healthcare system with edge intelligence computing," in *Reconnoitering the Landscape of Edge Intelligence in Healthcare*, CRC Press, pp. 31–46 (2024).

[8] P. Dass, V. Gupta, S. Dhingra, R. Arora, P. Katariya, and A. Kumar, "A deep learning model to predict and classify crime rate using tweets," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 8, pp. 2255–2271 (2024).

[9] G. B. Mohammad, Shitharth, and P. R. Kumar, "Integrated machine learning model for URL phishing detection," *International Journal of Grid and Distributed Computing*, vol. 14, no. 1, pp. 513–529 (2021).

Received December, 2024