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

Morched Derbali (mderbali@kau.edu.sa)
King Abdulaziz University (KAU)- Jeddah

Research Article

Keywords: smart door lock, Facial authentication, intrusion detection, machine learning, internet of things

Posted Date: August 23rd, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3247506/v1

Abstract

Home security and reconnaissance, as well as far off entryway exchanging with a hello framework are two parts of this work. Process of installing system's hardware components for security and surveillance begins the user's journey. With advent of Internet of Things (IOT), there is an increase in interest in smart home systems in recent years. One of the significant parts of the brilliant home framework is the security and access control. In this paper, a facial acknowledgment security framework was planned utilizing Raspberry Pi which are consistently coordinated to savvy home framework. Using machine learning architectures and IoT, this study aims to develop a smart door lock (SDL) system based on facial authentication and intrusion detection. Biometric authentication that is based on facial recognition is used to lock this smart door. The distributed encoder Shannon Gaussian Correntropy Bayesian Q-neural networks (DeSGCBQNN) are then used to detect anomalies. The trial examination is completed for different savvy entryway facial dataset as far as accuracy, mean average precision, False Acceptance Rate, False Rejection Rate and mean square error.Proposed technique attained accuracy of 98%, mean average precision of 66%, False Acceptance Rate of 65%, False Rejection Rate 55%and mean square error of 53%.

1. Introduction

Human life is characterized by security and safety. Humans frequently put in a lot of effort, seize every opportunity, and earn and save money. For many generations, this was a routine. It is likewise essential to save what we have acquired, barely any put their cash in banks, scarcely any purchase resources, few put away their cash and other spend on necessities or gift to their friends and family. But does that apply to our homes as well? People forever are dreaded they get terrified effectively to alleviate them from their apprehension they need security, and that security is locks [1]. It is astonishing how a gadget, for example, a lock places a help to individuals that they are protected. According to research, people work more than half of their lives to provide for themselves and their families, so locks are the only hope for safeguarding such valuables. There has been a lot of innovation in locks over the years. Nowadays, locks can be unlocked from any location in the world. Presently, we will foster our form of brilliant lock that meets our goals. The means by which systems can be sabotaged are also expanding simultaneously as artificial intelligence technologies are incorporated into their development [2]. Particularly, it is not recommended to rely on a uni-modal method for reliable monitoring in applications related to security and surveillance. Problems with security are given a high priority because every business owner tries to keep their workplace, assets, and homes as safe as possible [3]. Security is important in daily life. One of the principal explanations behind split the difference of safety is the unapproved admittance to outsiders. Keys, locks, and chains were the components of the old door security systems. Nonetheless, the locks can be effortlessly broken. There are times when using keys to unlock doors is inefficient due to the possibility of keys being misused, stolen, or duplicated [4]. Then came the era of uni-modal systems and shallow learning algorithms that could handle a single biometric trait at a time to guarantee authorized access. The precise identification of those who wish to enter the door is the most critical component of any door security system. However, that standard is not met by unimodal systems [5]. Detecting who enters or exits a house is a home security control system's most crucial function. Unique faces, which are a person's biometric characteristic, can be used instead of passwords or pins to monitor that. These are inherent and cannot be easily altered or stolen. Using face detection can raise the level of security [6].

The research aims to propose a novel facial authentication-based SDL system and machine learning-based intrusion detection method. By connecting all methods to the system database as well as developing an open-source Python-based home automation method for a variety of indoor and outdoor settings, the proposed system aims to design a system that is both cost-effective and flexible. The presence of the door is assumed for the purpose of the remote door unlocking feature, and our prototype lacks a physical lock. However, the house's greeting system is provided by an LCD screen. The web can be utilized for the controller of gadgets. For the far off entryway lock exchanging viewpoint, the principal task in this work is to propose a protected and dependable component; It requires locks that are extremely advanced and sophisticated to implement.

2. Existing SDL based on machine learning techniques

The most recent security technologies include RFID card technologies, biometrics, an OTP-based unlock system, and many others. Each of these works in some situations, but they don't provide the entire security system. Home security systems have been proposed by many researchers, but face recognition has only been used by a small number [7]. Face acknowledgment brings the great potential to the table for areas of strength for a framework to the home. A Framework for Face Acknowledgment The Home Security Administration Robot's developers' Nearby Paired Examples and Backing Vector Machine have clarified how LBP works in the face identification module, however they fall short in the situation of force disappointment. The author [10] investigated useful digital door lock features like key sharing and remote control via mobile device integration. A method for transmitting the image of an accessing object and detecting it was proposed in Work [11]. Creator [12] read up a technique for opening and shutting the entryway lock utilizing voice acknowledgment, without utilizing an organization. Work [13] proposed a security framework that points of interaction with an Android cell phone. Bluetooth allows for quick communication between the mobile device and security system. An application for communicating between devices was created by the author in [14] for the purpose of transferring the state of the alarms that are set off in a house through a neighbor's door lock. Work [15] investigated face recognition in order to unlock the door. Specifically, the utilization of [16] moves the SMS about the authenticity of the client to the cell phone. However, because the door locks cannot be remotely controlled by the mobile device, neither of them can be an ideal IoT application. Investigations of [17] are connected with security applications for home robotization. Work [19] has developed a method in which the system uses a webcam to identify intrusive person who was using a computer programme and it uses the internet for communication. When a gatecrasher is detected by a camera, recognition software alerts the home owner through the Internet, plays a warning tone, and also sends an SMS to the addressee. The studies of [18] are the first studies for remotely controlling a door lock, which cannot be classified also into application of the entire Internet of Things. Author [20] proposed a system that used RaspberryPi to take pictures from the camera and compare them to a database that was available. However, his model was limited because it couldn't work well in poor lighting. Work [21] presented a doorway lock framework which involves three subsystems: face acknowledgment, face distinguishing proof and last is entryway section. Acknowledgment is finished by utilizing PCA calculation. Entry door will open naturally for approved individual and watchfulness will ring for the unapproved person. A security framework with the face as biometric trait was proposed by author [22]. The MATLAB package's PCA was utilized by the authors.

3. Proposed facialauthentication based anomaly detection using machine learning

At first, researched and investigated the new ideas and concepts that were available. We chose a method that was both energy efficient and cost effective based on the information we gained. Then, at that point, we recorded our necessities and targets and chose the parts that it required. We decided to try something new with the microcontroller, so instead of sticking with the Arduino, we chose something new like the bolt IoT WIFI module. The next thing we decided to do was design the lock so that it could be attached to the door. We chose a model with a rectangle shape for this project so that it could hold all of the main parts. A real-time environment must be taken into account during simulation after design.

Facial authentication based smart door lock system with IoT:

In contrast to the conventional technique, it works directly with the face rather than the key, which allows anyone with the key to enter even if they are not authorised to do so. This technique is regarded as an additional security measure to keep intruders out of a certain area. Face recognition is a method for automatically recognizing, comparing, and matching a human face from a live video feed with other images from a database of authorized individuals. Figure 1 depicts the primary steps involved in putting this concept into action in real time.

At home, the primary computer at the site is a Raspberry Pi model 3B+. It runs Raspbian Stretch OS in the prototype that was shown to you. The Secure Shell (SSH) protocol is used to access Pi before it is used in the development process, and its Virtual Network Computing (VNC) server is enabled. After that, the VNC viewer software is used to access this Pi whenever it is needed for work. The primary benefit of this is that Pi can be utilized with the peripherals of a PC or a PC, without having to remotely join a HDMI screen, a mouse, and a console to it. The Pi performs multiple functions within the security system. It is in charge of keeping an eye on the proximity sensor and triggers that cause the Pi camera to take an image. A suitable cloud service will receive the image. Other than these undertakings, it needs to stand by listening to another cloud administration that illuminates Pi regarding whether to open or close the door s lock and on the off chance that the entryway is to be opened, it needs to bring an ID to be shown on the LCD screen message. The Raspberry Pi continually should be associated with the web. A camera module associated with the Pi is liable for catching a picture on both of the two triggers - the first is the squeezing of the doorbell which is likewise interacted with the Raspberry Pi. A push-button doorbell is used to represent the prototype. The second trigger is when someone stays near the house (via a proximity sensor) for more than a certain amount of time. The proximity sensor in the prototype shown here is an infrared sensor. For the entryway exchanging framework, a Drove bulb addresses the exchanging of the entryway that occurs after the order is transferred to the Raspberry Pi from the versatile application through the cloud. Figure 2 depicts an LCD module used to represent the LCD screen.

Raspberry pi, which fills in as the primary gadget regulator in our framework. Raspberry pi arranges the camera to catch and store the picture. Additionally, sensors are directly connected to a door-motion-equipped Raspberry Pi. To comprehend how the facial recognition and alert system works, let's say a person stays in the house for more than ten seconds, which is the predetermined time limit. This is detected by the IR sensor, and the Raspberry Pi checks to see if a presence has been detected for more than ten seconds before activating the camera to take a picture. A Lambda detects this and sends the image to Rekognition as soon as it is uploaded to an S3 bucket called "Visitors." The image is given a name and a time stamp. A second Lambda compares the features extracted by Rekognition to those in the "Known" database. A match is made and the name-tag of the match is extracted if a confidence value of at least 90% is reached. There is no match if the confidence value is less than 90%. One way or the other, the outcomes are shipped off the enlisted email/s. On the application, a warning is sent, and in a window the client can see the photograph taken by the Raspberry Pi camera, as well as the related label which is either „unknown or the ID in the event that the individual external the house is known. The doorbell is rung by the same door. A picture is taken as soon as the doorbell switch is pressed, and a time buffer of five seconds is provided to prevent multiple pictures from being taken during the time the switch is pressed. Now, suppose Mr. X is the person at the door, and the users who were alerted want to let him in. For this, the client switches the slider button on the application. In order to prevent accidental errors, when the user tries to toggle it, a prompt appears asking if they are confident in the operation. Solely after the client consents to the brief, the button flips. A Lambda that takes the status value and updates it in another DynamoDB database with only a key-value pair is triggered when this button is toggled. The value is either 0 or 1, and the key is "door_status." Open means 1, and closed means 0. When this worth update happens, another Lambda takes this worth (1) from the information base and moves it to the Raspberry Pi, which turns the Drove bulb on, implying that the entryway lock is exchanged open. The same Lambda also carries the face-match result, or the string "unknown" if the door is unlocked for a person the system doesn't know. If the door is unlocked for a known person, the Lambda carries a name tag. The LCD module displays "Welcome, Mr. X" because the individual in this instance is known and has a name tag that reads "Mr. X." In the event that the individual at the entryway is obscure to the framework, however the entryway is opened for them, then no hello message would appear on the LCD module.

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

While generator reconstructs input data from latent variable z, encoder maps data space X into latent space Z. E (x; E) = f (WE x + bE), where the parameters are the weight matrix W E of size NzNx and offset vector bE of dimension Nz, is an example of an encoder. It consists of a nonlinear activation function f and an affine transformation. The generated latent variable z is mapped back into reconstructed Nx-dimensional vector by generator G. By reducing the reconstruction error Lrec, which measures the predicted separation between the input vector x and its reconstruction x, the Auto-Encoder is trained: $\widehat{x} : \mathcal{L}_{\text{rec}} = \mathbb{E}_{x \in \mathcal{X}} \parallel x - \widehat{x} \|^2 = \mathbb{E}_{x \in \mathcal{X}} \parallel \backslash\mathtt{varvec} x - G\left(E(\,x\,)\right) \|^2$, where "." stands for L2 norm.

to reduce Jensen Shannon Divergence $JSD\left(pG \parallel p_{\mathcal{X}_{\text{nor}}}\right)$, where Xnor is collection of patterns from components operating normally, pXnor is the probability distribution of those patterns, and pG is the probability distribution of generated patterns.

Let's define generator and discriminator parameters, as G = WG, bG and D = W D, bD. D (x; D) = fD(W D x + bD), where W D is a NzNx weight matrix, bD is an offset vector of size Nz, and fD is nonlinear activation function, for example, fD = sigmoid(), is formulated similarly to how the AutoEncoder (Section III-B) does.Prior to generator parameter θG'soptimisation, discriminator parameter θ ∗ D(θG) optimisation is established utilizing gradient-based technique based on Eq. (2).

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

1

$$\theta_D^{*}\left(\theta_G\right)=\lim_{k\to\infty}\theta_D^{(k)}$$

2

Additionally, Eq. (3) is used to optimise the generator parameter.

$$\theta_E=\theta_E-\eta\cdot\operatorname{Adam}\left(\nabla_{\theta_E}\mathcal{L}_{rec}\left(x;\theta_E,\theta_G^{*}\right);\beta_1,\beta_2\right)$$

3

where gradient of loss function F with respect to G determines the updating term $\operatorname{Adam}\left(\nabla_{\theta_G}\mathcal{F}\left(\theta_D^{(k)},\theta_G\right);\beta_1,\beta_2\right)$. Due to the fact that θ (k) D depends on θG, there are θk updating steps of θ (k) D for every updating step of θG (Eq. (4)). It is suggested to use an additional auto-encoder to effectively reduce the reconstruction error by Eq. (4):

$$\mathcal{L}_{\text{rec}}\left(x;\theta_E,\theta_G^{*}\right)=\mathbb{E}_{x\in\mathcal{X}_{\text{nae}}}\left\|x-G\left(E\left(x;\theta_E\right);\theta_G^{*}\right)\right\|^2$$

4

from which we obtain by Eq. (5)

$$\theta_E^{*}=\underset{\theta_E}{\operatorname{argmin}}\mathcal{L}_{\text{rec}}\left(x;\theta_E,\theta_G^{*}\right)\text{ and }z_{\text{oprimal}}=E\left(x;\theta_E^{*}\right)$$

5

where θ ∗ E is encoder's ideal parameter. By using Eq. (6), encoder parameter θE is optimised.

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

6

In order to obtain Eq. (7), we first add a normally distributed adaptive noise, $\epsilon_k\left(i\right)$, to the k-th feature at the i-th time stamp of the r-th healthy components, Xr k (i).

$$\backslash\text{varvec}X_k^{\prime r}\left(i\right)=\backslash\text{varvec}X_k^{r}\left(i\right)+\epsilon_k\left(i\right)$$

7

We briefly introduced idea of reinforcement learning (RL) based on a Markov decision process (MDP), which forms basis of our proposed method distributional reinforcement learning-based IDS engine, which relies on RL modelling from our earlier work [42]. Quintuple ideas of RL-based IDS by (S, A, R, Pa, γ) are concisely defined as follows: - S stands for the collection of states that IDS has recorded. We assume that S = s0, s1, and s2, where s0 stands for "normal00," s1 for "Detection00," and s2 for "NoDetection00." - A denotes the range of potential responses that IDS may employ. These responses may be classified as low, medium, high, or critical depending on likelihood of an attack.Placement of reward R(s, a) obtained in state s and action a by Eq. (8) allow us to express returns of IDS and to conduct an action immediately. R is objective function to be optimised in system.

$$R(s,a)=\sum_{s'\in S}P_a\left(s\mid s',a\right)R(s\prime,a)$$

8

Pa is the probability of changing states. It is represented by an Eq. (9) as a matrix of transition probabilities p(si ∣ sj, a) observed at time t for a ∈ A where i, j = 1, 2, 3 and V = 1(valid), 2(invalid).

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

9

In a 3×3 matrix B_a with $\sum_{j=1}^{3} \beta_{i,j}^{a} = 1$, transition probability from state sj observed at t to state si observed ats_i observed at t+1 is shown, indicating whether the anticipated data is legitimate or incorrect. - The discount factor is in the range of 0 < γ < 1. The agent performs an action in each s, records the reward of that action as well as the following state as s 0, and then updates the estimated value function of Qπ that satisfies the Bellman equation.

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

10

By modelling all potential returns in a dynamic manner and attempting to learn from their mean, this is done to provide more action predictions. Let R(s,a) be the return calculated by adding discounted rewards that agent has observed starting from state s and taking action an in accordance with the policy π, with random variable $Z(s,a) = \sum_{i=0}^{\infty} \gamma R(s,a)$. As a result, Eq. (11) provides the estimated value function for a given π.

$$Q^{\pi}(s,a) = \mathbb{E}\left[Z^{\pi}(s,a)\right]$$

11

Equation (12) is a representation of the distributional Bellman equation for a specific.

$$Z(s,a) \overset{D}{=} \mathbb{E}_{s,a,s'}\left[\left(R(s,a) + \gamma \max_{a' \in A} Z^{\pi}\left(s', a'\right)\right)\right]$$

12

$$\tau^{*} Z(s,a) \overset{D}{=} \mathbb{E}_{s,a,s'}\left[\left(R(s,a) + \gamma Z\left(s', \pi^{*}\left(s'\right)\right)\right)\right]$$

13

$$\text{where} s' \sim p(. \mid s,a) \text{and} \pi^{*} = \text{argmax}_{a' \in A} \mathbb{E}\left[Z\left(s', a'\right)\right]$$

Algorithm for anomaly detection

Input: Anomaly score valudation set, $V = \left\{A^{2}\right\}_{z=1}, N_{\infty}$, weak classifier $h : A \to \{-1,1\}$, percentile c.

Output: Ensembled classifier

$H(A) = \text{sgn}\left(\sum_{m=1}^{N_m} a_m \cdot h_m(A)\right)$

Initialize: Weights of validation set V anomaly scores $w_1^{(1)}, w_2^{(1)}, \ldots, w_{N_1}^{(1)}$ set to $\frac{1}{N_e}$initial error rate $\epsilon_m, m = 1, \ldots, N_m$ set as $\frac{1}{2}$

/ * Train AdaBoost Ensemble model // for $m = 1, \ldots, N_m$ do $A_{\text{rhreshold },m} =$ Percentile $e_c\left\{\left(A^{v}\right)^{T} \cdot o^{(m)}\right\}_{0=1,\ldots,N_\epsilon}$

Obtain error rate

$\epsilon_m = \sum_{v,1-h_m\left(A^{*}\right)} w_D^{(m)}, v = 1, \ldots, N_v$

Obtain weights of classifier $h_m, \alpha_m = \frac{1}{2} \ln\left(\frac{1-\epsilon_m}{\epsilon_m}\right)$

Update weights

$w_0^{(m+1)} = w_b^{(m)} e^{a_m h_m\left(A^{*}\right)}, v = 1, \ldots, N_{b.}$

7 Normalize weights

$w_{\mathrm{v}}^{(m+1)} = \frac{w_D^{(m+1)}}{\sum_{m=1}^{N_0} w^{(m+1)}}, v = 1, \ldots, N_0 -$

4. Experimental analysis

For security purposes, we have suggested a raspberry pi-based face recognition door lock system. Execution of the framework is done to see whether any unknown people are coming through the door. With the help of the Pi camera and Raspberry Pi platform, we have set up face recognition for communication with electronic devices. The Open CV libraries and Python are used for software development.

NSL-KDD and UNSW-NB15 benchmark datasets served as basis for evaluating proposed DAD system. From one viewpoint, NSL-KDD dataset is a superior variant of old KDD99 dataset for resolving a few issues. To address unbalanced issue, the NSL-KDD removes KDD99 dataset's repeated records. Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe are four attacks in each of 41 attributes and class labels of each vector. The normal and attacks records are mixed together in the UNSW-NB15 dataset. Each vector includes 47 qualities and the class mark, including typical records and nine assaults of Observation, Investigation, Worm, Secondary passage, DoS, Nonexclusive, Fuzzer, Shellcode as well as Exploit.

We utilized Distributed Smart Space Orchestration System (DS2OS) benchmark dataset that was collected from Kaggle as an open-source dataset offered by Pahl and Aubet [40]. A simulated IoT environment was built with DS2OS and utilised to gather a fake data set. This data collection contains traces of several IoT simulation sites' usage of a variety of services, including manipulation of smartphones and smart doors as well as light controls, thermometers, movement sensor readings, washing machines, battery and temperature status, and thermometers. TDataset typically contains 357,952 interesting data, which are divided into 347,935 and 10,017 common and uncommon pieces of information, respectively. Seven types of attacks—DoS, scan, malicious control, malicious operation, espionage, data probing, and improper setup attacks—as well as regular data are included in these categories.

Different learning rates were utilized to distinguish most sufficient for our review that gave stable figuring out how to the specialist. The blue curve in Fig. 3 indicates that learning rate of 0.0001 achieved best convergence. When DRL agent's learning curve stops growing and becomes flat, it has reached convergence.

The Correntropy method significantly affects the creation of an adaptive baseline from standard traffic records. It treats any deviation from legitimate profile as an anomaly as well as dynamically estimates its boundaries. as depicted in the figures. After estimating their Correntropy values, some records from NSL-KDD and UNSW-NB15 datasets are plotted in Figs. 4 and 5. There are contrasts in the worth scopes of ordinary and assault information on both datasets. As a result, DAD's ability to distinguish between the various attack types in both datasets is significantly improved.

Table 1

Evaluation criteria based on comparison for various cyber attack datasets.

Samples (S)	NSL-KDD dataset					UNSW-NB15 dataset					DS2OS	
	Accuracy	Mean average precision	False acceptance rate (FAR)	False rejection rate (FRR)	Mean square error (MSE)	Accuracy	Mean average precision	False acceptance rate (FAR)	False rejection rate (FRR)	Mean square error (MSE)	Accuracy	Mean averag precisi
200,000	85	77	49	43	39	89	75	51	45	42	92	61
250,000	88	79	52	44	42	92	76	53	49	43	95	63
300,000	89	81	53	45	43	93	81	55	51	44	96	65
350,000	92	83	55	49	45	95	83	59	53	49	98	66

The above table- 1 shows comparison analysis based on various cyber attack dataset for number of data samples. Here the dataset analysed are NSL-KDD, UNSW-NB15, DS2OS dataset in terms of accuracy, mean average precision, FAR, FRR and MSE based on number of data samples.

The above Fig. 6 shows Evaluation criteria for NSL-KDD dataset for number of data samples. Here the proposed technique attained accuracy of 92%, mean average precision of 83%, FAR of 55%, FRR 49%and MSE of 45% based on 350,000 number of data samples.

From above Fig. 7 shows UNSW-NB15 dataset evaluation criteria based on number of data samples for proposed techniques. the proposed technique attained accuracy of 95%, mean average precision of 83%, FAR of 59%, FRR 53%and MSE of 49% based on 350,000 number of data samples.

The above Fig. 8 shows Evaluation criteria for DS2OS dataset for number of data samples. Here the proposed technique attained accuracy of 98%, mean average precision of 66%, FAR of 65%, FRR 55%and MSE of 53% based on 350,000 number of data samples.

The R2L and U2R attacks can be effectively detected by the system in NSL-KDD. Worms, Shellcode, Fuzzers, and Backdoor are just a few of the rare events that the system in UNSW-NB15 is able to effectively detect. DoS and probing, two other events with numerous records in both datasets, are discovered with almost 100% detection accuracy. On the basis of dynamic estimations of normal profile as well as proposed baseline, proposed system is capable of detecting these kinds of attacks. The Correntropy method, which has a significant impact on estimating normal profile's boundaries under GMM, uses the vectors' posterior probabilities as its input. This demonstrates that attack vectors' Correntropy values over time differ from the normal profile's Correntropy boundaries. The proposed system can test data record-by-record in less than one second for every ten samples as well as took approximately 72 seconds to train 350,000 examples. For any information size, suggested framework can effectively evaluate limits of GMM as well asCorrentropy models. Its prospective design focuses on automatically adjusting some GMM and Correntropy settings, making it simple to apply on gateways of edge networks to monitor and observe suspicious events. Suggested system can successfully identify different attack vectors, but in order to provide high reliability during the training phase, it needs a lot of regular vectors.

5. Conclusion

This examination propose novel strategy in facial validation based SDL framework and interruption recognition utilizing AI procedures. In addition to offering a remote door lock switch mechanism, an architecture for a system that works with images to provide home surveillance has been proposed. Several test cases were used to successfully develop and evaluate a prototype built with the same architecture. The framework accomplished an elevated degree of unwavering quality. It can be extended to other use cases that involve safeguarding and/or surveillance, and it can be used for multiple door locks. The element extraction and classifier were carried out utilizing Python and OpenCV. The finalised prototype design is ready for use in the real world. The output of the facial recognition algorithm will control a relay circuit, which will lock or unlock the magnetic lock on the door. Proposed technique attained accuracy of 98%, mean average precision of 66%, FAR of 65%, FRR 55%and MSE of 53%.

Declarations

Transformative

I confirm that I understand journal Optical and Quantum Electronics is a transformative journal. When research is accepted for publication, there is a choice to publish using either immediate gold open access or the traditional publishing route.

Competing Interests

No, I declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Dual Publication

The results/data/figures in this manuscript have not been published elsewhere, nor are they under consideration (from you or one of your Contributing Authors) by another publisher.

Authorship

I have read the Nature Portfolio journal policies on author responsibilities and submit this manuscript in accordance with those policies.

Third Party Material

All of the material is owned by the authors and/or no permissions are required.

References

1. Alotaibi, A., Rassam, M.A.: Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. Future Internet. **15**(2), 62 (2023)
2. Idrissi, I., Azizi, M., Moussaoui, O.: A Stratified IoT Deep Learning based Intrusion Detection System. In *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)* (pp. 1–8). IEEE. (2022), March
3. Kayyidavazhiyil, A., Silic, M.: INTRUSION DETECTION USING DEEP (CNN) CONVOLUTIONAL NEURAL NETWORK FEATURE EXTRACTION WITH (EPCA) ENHANCED PRINCIPAL COMPONENT ANALYSIS FOR DIMENSIONALITY REDUCTION. Global journal of Business and Integral Security (2022)
4. Othmen, F., Baklouti, M., Lazzaretti, A.E., Hamdi, M.: Energy-aware IoT-based method for a hybrid on-wrist fall detection system using a supervised dictionary learning technique. Sensors. **23**(7), 3567 (2023)
5. Al Duhayyim, M.: Modified Cuttlefish Swarm Optimization with Machine Learning-Based Sustainable Application of Solid Waste Management in IoT. Sustainability. **15**(9), 7321 (2023)
6. Agha, M.F.M.S.: *A new biometric system based on human hand geometry using deep convolutional neural network* (Master's thesis, AltınbaşÜniversitesi/LisansüstüEğitimEnstitüsü). (2022)
7. Tan, Y.: Feature Recognition and Style Transfer of Painting Image Using Lightweight Deep Learning. *Computational Intelligence and Neuroscience*, *2022*. (2022)
8. Sadineni, L., Pilli, E.S., Battula, R.B.: ProvNet-IoT: Provenance based network layer forensics in Internet of Things. Forensic Sci. International: Digit. Invest. **43**, 301441 (2022)
9. Sinha, M., Chaurasiya, R., Pandey, A., Singh, Y., Goyal, S.: Securing Smart Homes Using Face Recognition. In *Advances in Micro-Electronics, Embedded Systems and IoT: Proceedings of Sixth International Conference on Microelectronics, Electromagnetics and Telecommunications (ICMEET 2021), Volume 1* (pp. 391–398). Singapore: Springer Nature Singapore. (2022), April
10. Kumar, A., Biswas, A.K., Kumar, A., Yadav, R.K.: Optimising IOT Based Smart Home Systems Using Machine-Learning Algorithm. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1133–1139). IEEE. (2022), June
11. Rajeshkumar, G., Braveen, M., Venkatesh, R., Shermila, P. J., Prabu, B. G., Veerasamy,B., … Jeyam, A. (2023). Smart office automation via faster R-CNN based face recognition and internet of things. *Measurement: Sensors*, *27*, 100719
12. Leim, J.H., Ng, K.W., Arpitha, S., Ng, S.L., Haw, S.C.: SAFE: Security Door Lock System Using Haar-Cascade and LBPH Method. Appl. Comput. Eng., 291–299. (2023)

13. Raizada, P., Gupta, S., Das, M., Rastogi, P., Arora, D.: Smart Lock System using IoT, Embedded & Machine Learning. In *2022 IEEE 7th International conference for Convergence in Technology (I2CT)* (pp. 1–8). IEEE. (2022), April

14. Tameemi, M.I.A.: Design and implementation of a Deep Learning-based Intelligent Electronic Lock Door Entry Control System. Iraqi J. Sci., 4079–4089. (2022)

15. Rahim, A., Zhong, Y., Ahmad, T.: A Deep Learning-Based Intelligent Face Recognition Method in the Internet of Home Things for Security Applications. J. Hunan Univ. Nat. Sci., **49**(10). (2022)

16. Paikaray, D., Parikh, S.: A new way of Smart Home Security using ML Face Recognition. In *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 1628–1632). IEEE. (2022), December

17. Puvaneswari, G., Ramya, M., Kalaivani, R., Ganesh, S.B.: Smart Home Security System Using Facial Recognition. In *Proceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022* (pp. 239–252). Singapore: Springer Nature Singapore. (2023), February

18. Edward, A.S., Jothimani, A., Akila, V., Vaishali, D.: Smart surveillance system using emotion detection. In *AIP Conference Proceedings* (Vol. 2427, No. 1, p. 020086). AIP Publishing LLC. (2023), February

19. Bhatlawande, S., Shilaskar, S., Gadad, T., Ghulaxe, S., Gaikwad, R.: Smart Home Security Monitoring System based on Face Recognition and Android Application. In *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 222–227). IEEE. (2023), January

20. Hemalatha, M., Priya, J.S., Porselvi, T.: An Intelligent Authentication System for Improved Security. In *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)* (pp. 1–5). IEEE. (2022), December

21. Sankar, S., Pradeep, D., Rangarajan, A.: Intelligent Door Assist system using Chatbot and Facial Recognition. In *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1–6). IEEE. (2022), July

22. Surla, G., Manepalli, S., Shaik, N.A., Gurram, N.S.: IoT and Face Recognition based Automated Door Lock System. In *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 648–651). IEEE. (2023), March

Figures

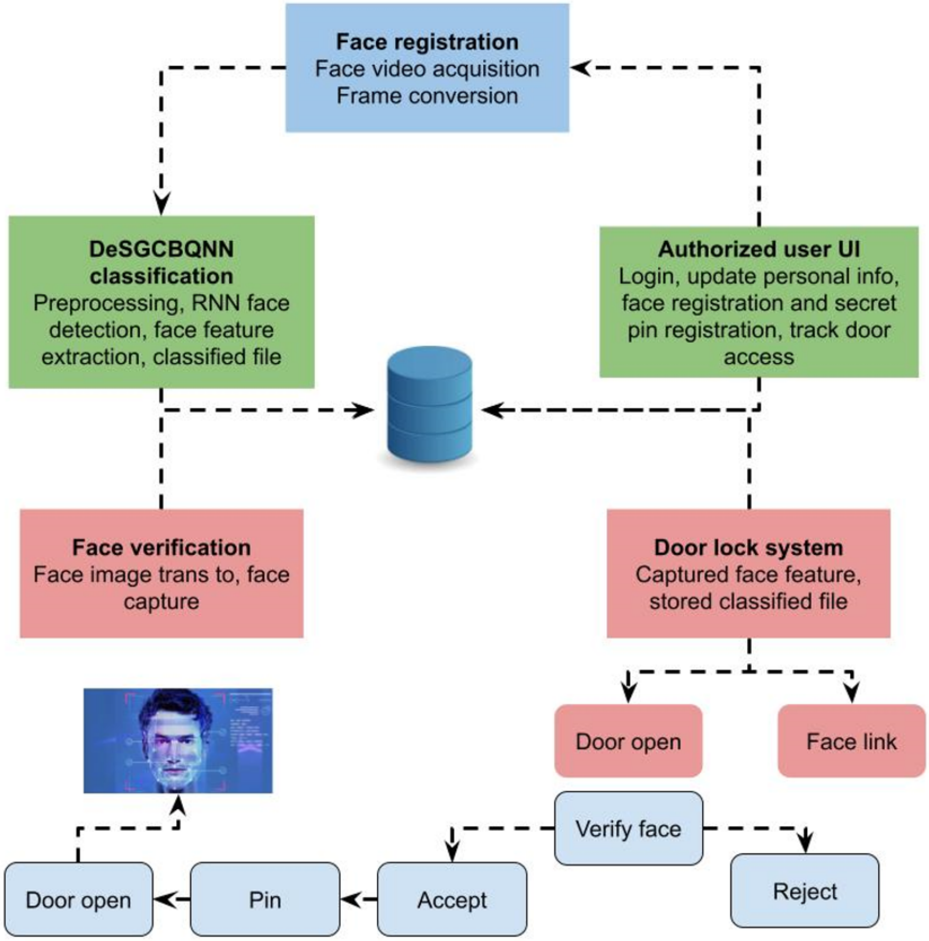
Face registration
Face video acquisition
Frame conversion
DeSGCBQNN classification
Preprocessing, RNN face detection, face feature extraction, classified file
Authorized user UI
Login, update personal info, face registration and secret pin registration, track door access
Face verification
Face image trans to, face capture
Door lock system
Captured face feature, stored classified file
Door open
Face link
Verify face
Reject
Accept
Pin
Door open

Figure 1

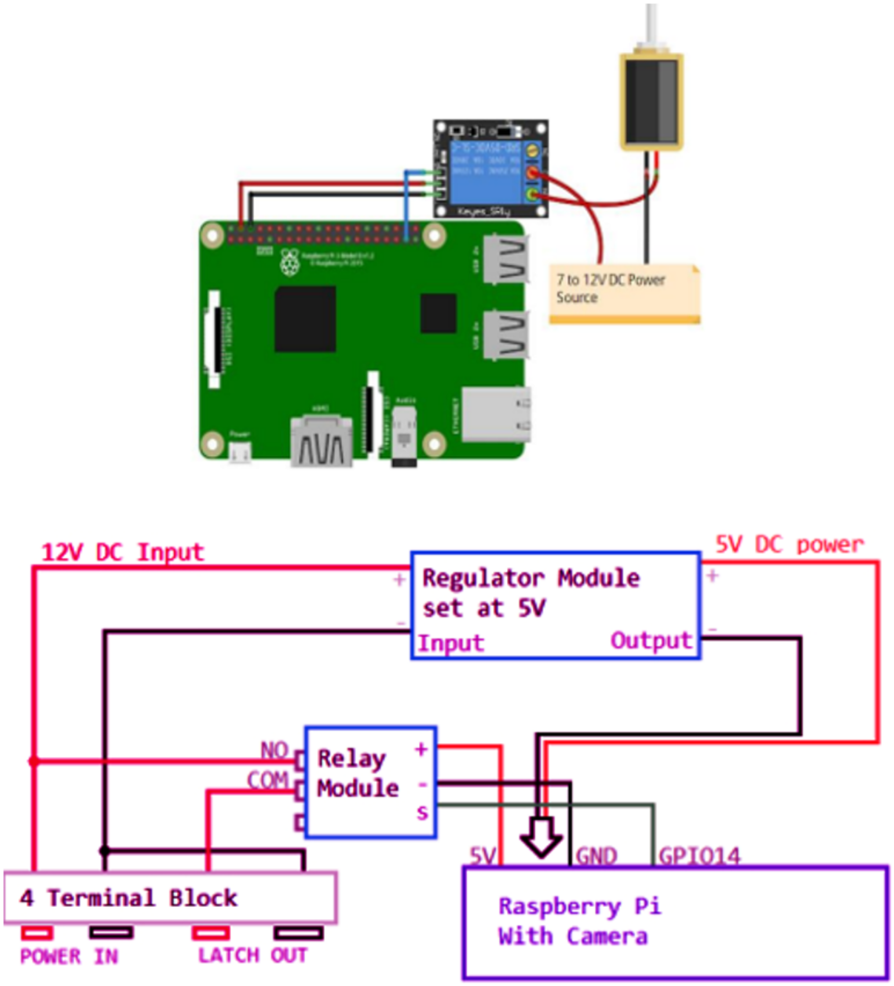

Figure 2

Proposed Facial authentication based smart door lock module

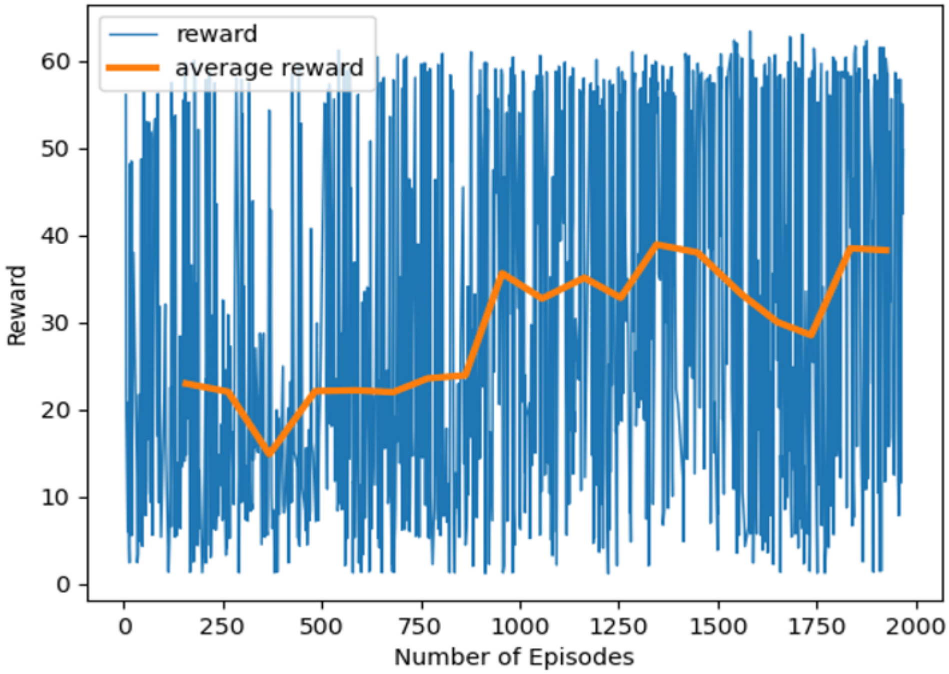

Figure 3

Training rewards of the DRL agent

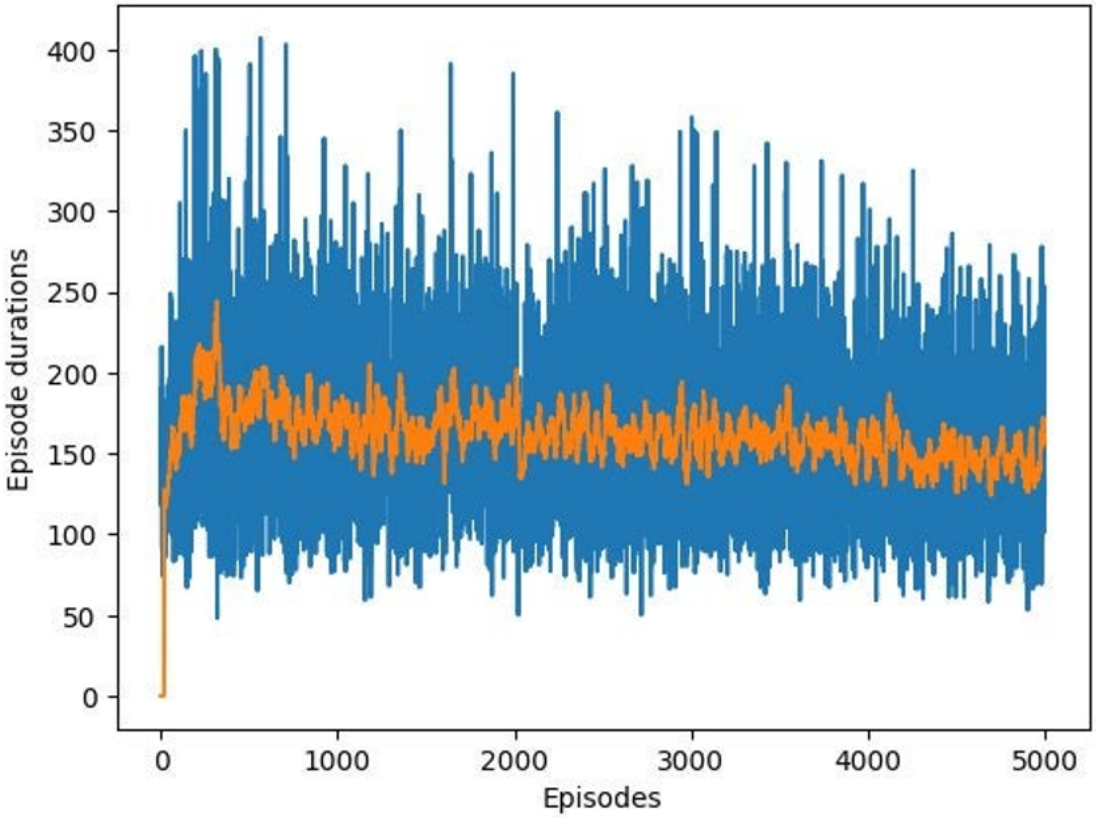

Figure 4

Correntropy values of some feature vectors selected from NSL-KDD dataset

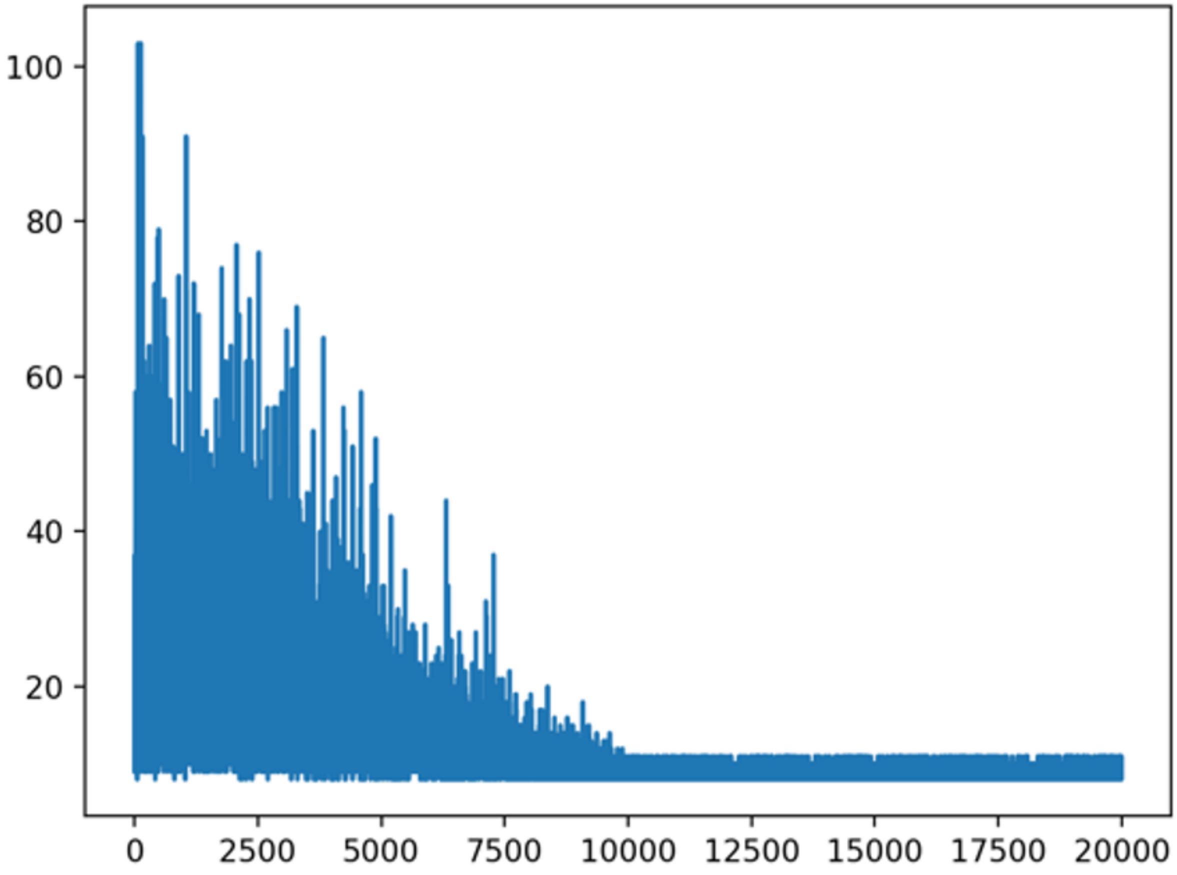

Figure 5

Figure 5. Correntropy values of some feature vectors selected from UNSW-NB15 dataset

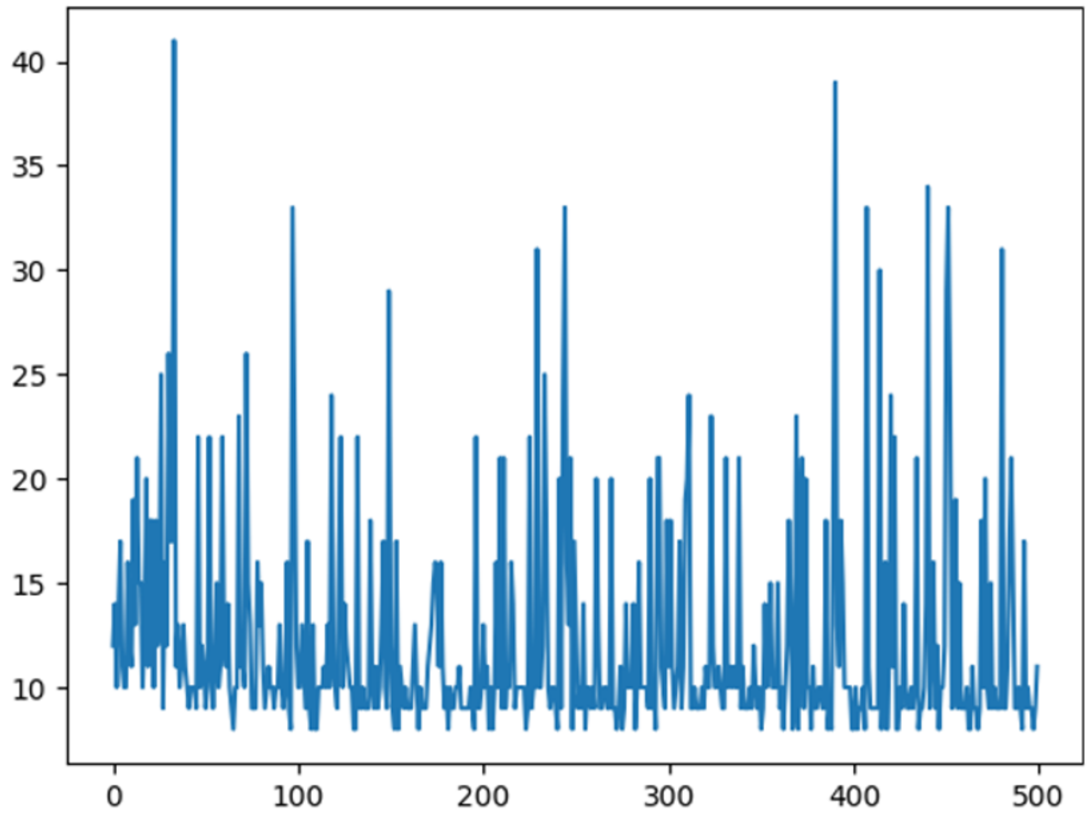

Figure 6

Figure 5. Correntropy values of some feature vectors selected from DS2OS dataset

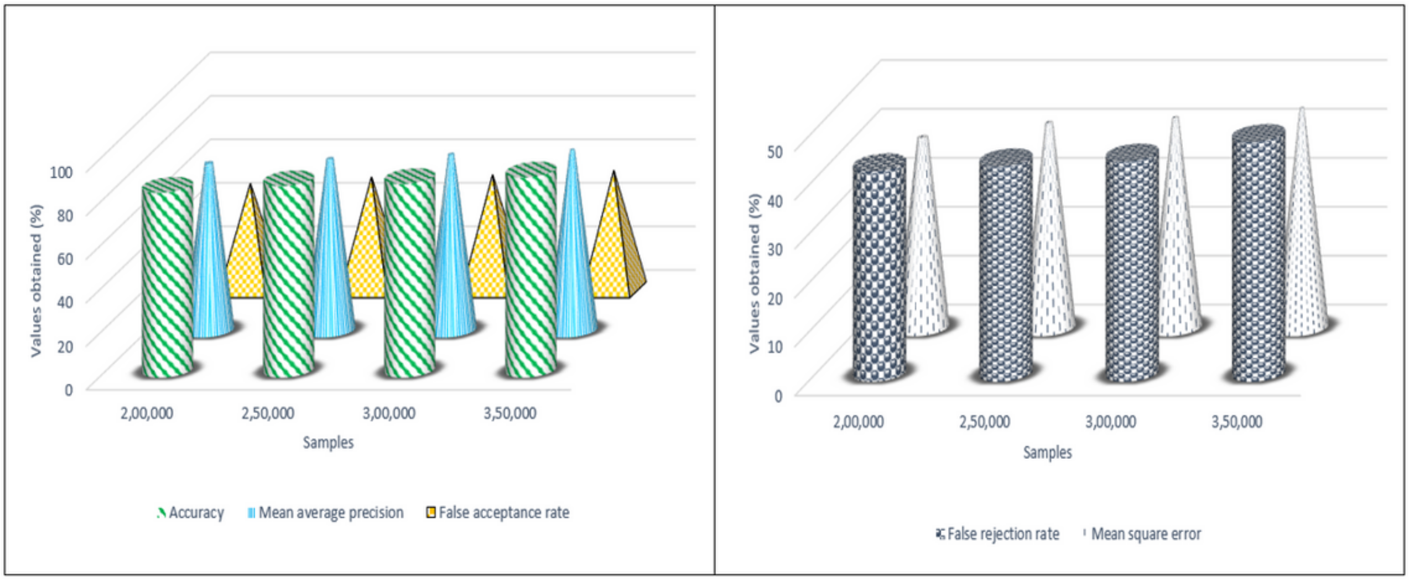

Figure 7

Figure-6 proposed technique based evaluation criteria for NSL-KDD dataset

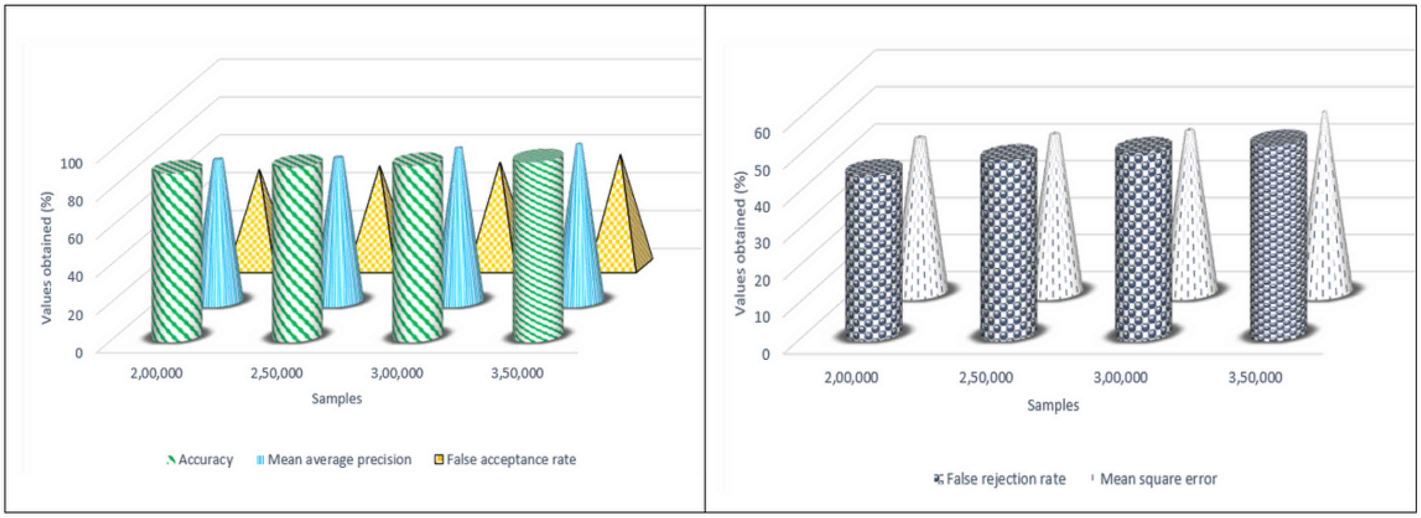

Figure 8

Figure-7 proposed technique based evaluation criteria for UNSW-NB15 dataset

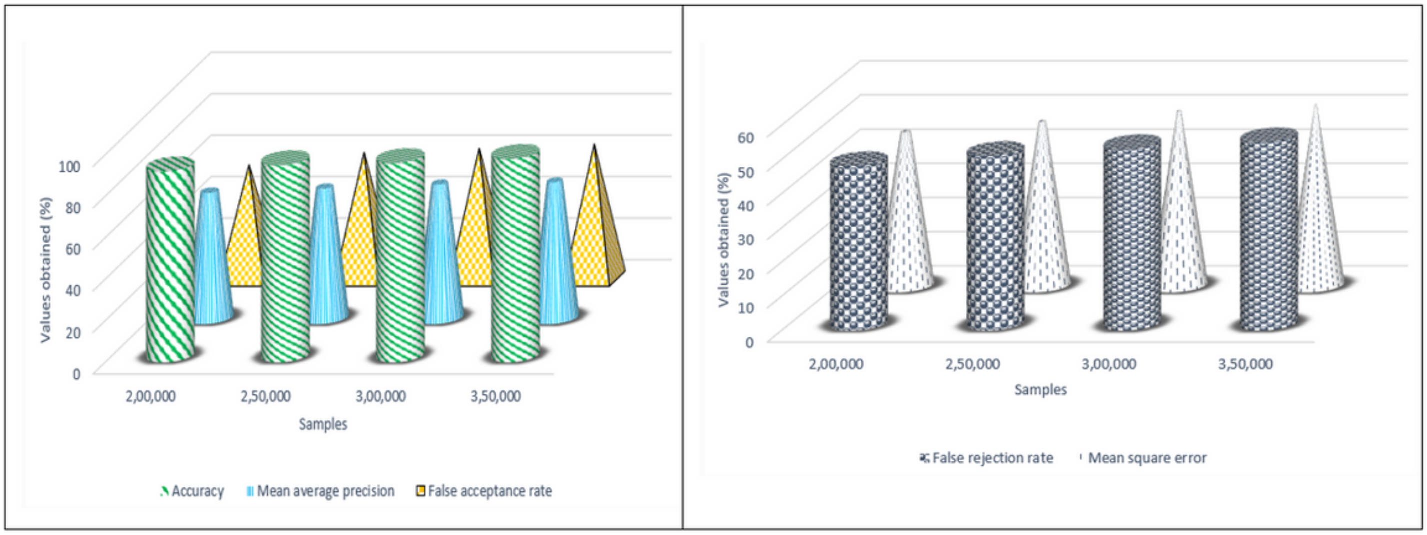

Figure 9

Figure-8 proposed technique based evaluation criteria for UNSW-NB15 dataset