IoT Powered Authentication for Smart Door Security

K.RAMYA ,
Assistant Professor,
Dhanalakshmi Srinivasan engineering college,
Perambalur.

M.MUTHAMILSELVI ,
Final year CSE,
Dhanalakshmi Srinivasan engineering college,
Perambalur.

R.NIVETHA ,
Final year CSE,
Dhanalakshmi Srinivasan engineering college,
Perambalur.

R.PRIYA DHARSHINI,
Final year CSE,
Dhanalakshmi Srinivasan engineering college,
Perambalur.

ABSTRACT–The visitor management is a modern world problem with its application a numerous fraud, privacy issues, etc. can be easily detected and avoided. The visitor management system using face recognition is one of the most secure systems even better than CCTV cameras and wake through gate methods. The main focus that has to made in project is whether the cost of the system compiles with the extent of the project. The scale of operations and the security requirements differ from place to place for instance domestic usage and industrial usage. Visitor Management System is mostly used by corporate, schools, colleges now but with great advancements can extent its scope to railway stations, airports, toll stations, etc. Almost all businesses with huge facilities are incorporating Visitor Management Systems in their overall security and is constantly growing a constant pace. Face recognition visitors' management system (FRVMS) is proposed to enhance the security of home to identify the unknown persons without manual interventions. Centralize system enable managing and monitoring process become more efficient. Cost of development is also taking into consideration as this system is not requiring any extra devices. Face recognition is using web camera that is already embedded with the computer. The detected detailed features are compared with the family of face data stored in the database of the monitoring system, and security is cancelled in case of a member, while an alarm notification is displayed to the user in case of an outsider. Then the user wear face mask means, specify the alarm to remove the mask to recognize the facial features. We can implement the framework using deep learning algorithm named as Convolutional neural network and experiment this system in real time environments and also open the door in hardware setup

KEYWORDS:CCTV cameras, Visitor Management, Convolutional neural network, Mask Detection, Face detection

1. INTRODUCTION

The Internet of Things (IoT) is revolutionizing the way we think about home security, with IoT-enabled devices providing enhanced security features for smart homes. Smart locks are a particularly promising application of IoT in home security. These locks can be controlled remotely through smartphones, tablets, or voice assistants, enabling users to grant or revoke access to their homes. Smart locks can also be programmed to provide access to specific individuals for a limited period, making them ideal for rental properties and short-term rentals. Smart locks can also be integrated with other IoT-enabled devices such as security cameras and motion sensors to provide enhanced security features. For example, when a smart lock is unlocked, it can trigger a security camera to start recording, providing users with a visual record of who enters their homes. Additionally, smart doorbells are another IoT-enabled device that provides enhanced security features for smart homes. Smart doorbells can provide motion detection, live video streaming, and two-way communication, enabling users to monitor their homes remotely and communicate with visitors. These devices can also be integrated with other IoT-enabled devices such as smart locks, enabling users to control access to their homes remotely. In conclusion, IoT-enabled devices such as smart locks and doorbells are transforming home security, providing enhanced features that were not possible with traditional security systems. An IoT-based home security system employs interconnected sensors, devices, and technologies to safeguard residential properties from security threats. These systems typically comprise motion sensors, door/window sensors, security cameras, smart locks, and other components strategically placed throughout the home. Central to this setup is an IoT hub or gateway that serves as the nerve centre, facilitating communication between devices and the cloud or mobile applications. Data collected by sensors are processed locally or in the cloud, where algorithms analyse patterns to differentiate normal activities from potential security breaches. When a threat is detected, alerts are promptly issued to homeowners via mobile apps, email, or other channels. Remote monitoring and control capabilities empower homeowners to manage their security system from anywhere, enabling tasks such as arming/disarming alarms or viewing camera feeds. Integration with other smart home devices and services further enhances functionality, while robust security measures safeguard user privacy and prevent unauthorized access. Regular maintenance and testing ensure the system remains reliable and effective over time, providing homeowners with peace of mind and comprehensive protection for their homes and loved ones.

2. RELATED WORK

Hyung-jin mun, et.al,…[1] developed deep learning technology in the field of image recognition is being applied as a core technology to autonomous driving and crime prevention monitoring systems, which are emerging as future industries. As for deep learning models in the field of image recognition, various algorithms that have improved and developed CNNs capable of image processing have been proposed. In this paper, we introduce various object detection algorithms including CNN. CCTV detects the face of a visitor and then recognizes 81 feature points in the face to create a set of vector values based on the features. Members of the family are registered in advance with face images. In this study, we designed and implemented a system that opens the front door after recognizing a new visitor as a member of the family when the difference in recognized facial feature vector values between the CCTV image and the image stored in the database is smaller than the threshold.

Aaesha aldahmani, et.al,…[2] defined as “An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face situations and changes in the environment”. IoT is a cutting-edge technology that is changing the way we live. An autonomous smart home is equipped with embedded devices that are designed to detect and respond to a person’s presence and needs such as light detection devices, fingerprint readers, gas detection systems, smoke sensors, temperature monitoring devices, motion detection systems, home surveillance cameras, etc. These devices are connected together for many purposes such as saving energy consumption, reducing the bill costs, and security of home occupants. Users are using interface devices such as a remote control, computer, or smartphone to manipulate different sensors and devices in these systems. Home security and safety are crucial for occupants’ well-being. A smart home automation system should integrate a security management strategy with alarms. With motion identification and detection, smart homes may be safeguarded against intruders while preventing false alarms. As walking patterns are unique to each person, IoT sensors can track human mobility and activity. The collected movement patterns offer biometric verification of humans

Muhammad qasim mehmood, et.al,…[3] consists of a paper-based hybrid geometry sensors keypad for locking/unlocking the door and resetting the password. The sensors are fabricated from cost-effective and disposable materials using the garage-based fabrication process. The system performed equally good for bare and invisible configuration. The invisibility of the sensors lessens the chances of password leak while entering the password. The proposed invisible sensors can find ready applications in cardless and non-keys-based door locking systems for security applications in homes, banks, and lockers. Nowadays, security is one of the living essentials, and there is a dire need for reliable, secure, and smarter locking systems. The stand-alone smart security systems are of great interest as they do not involve keys, cards, or unsecured communication in order to prevent carrying, loss, duplication, and hacking. Here, we report an invisible touch sensors-based smart door locking system (DLS). The passive transducer-based touch sensors are fabricated through a facile do-it-yourself (DIY) based fabrication process by pasting the hybrid geometry copper electrodes on cellulose paper. The employment of biodegradable, and non-toxic materials like paper and copper tape makes this configuration a good candidate for green electronics. For additional security, the keypad in the DLS is made invisible by covering it with paper and spray paint. One can only open the door by knowing the password as well as the location of each key on the sensor keypad. The system can efficiently recognize the exact pattern of passwords without any false values. Invisible touch sensors-based locking systems can easily contribute to the security applications in homes, banks, automobiles, apartments, lockers, and cabinets.

Zeeshan ashraf, et.al,..[4] different types of electronic smart devices such as IoT-based sensors are used to collect specific data and transfer the data to central systems. The data are collected from different citizens, devices, buildings, and assets. The data are used to analyse & monitor the traffic, manage transportation systems, monitor power plants, manage water supply networks, criminal investigations, weather stations, pollution monitors, vehicle networks, home automation systems, and other community services. The data helps to improve the operations across the city. The idea of a smart home has gained enormous popularity throughout the world because of the rapid growth of information and communication technologies (ICT) and the Internet of

Everything (IoE). In a smart home automation system, IoT-enabled smart devices such as smart TVs, smart security cameras, smart lights, smart ACs, smart locks, etc. are connected through wireless technology. A variety of wireless technologies are available for connecting smart home devices but 6LoWPAN is the most suitable protocol for IPv6 to enable IPv6 packets to be carried on top of low-power wireless networks. Users utilize different services by accessing these smart devices either inside the network or outside the network. Users can control smart devices with an application, check the status of smart devices, and perform on or off services on various smart devices through smartphones. Users can control smart devices easily and remotely within a smart home by connecting to the smart home network.

Iram arshad, et.al,…[5] ensure data security and intelligent models in SM to protect the digital industry from potential cyber threats. ML and DL algorithms are used in various applications to detect patterns and anomalies in SM systems' vast amounts of data. By analysing data, these algorithms can identify potential cyber threats in real-time and alert security teams, enabling them to take swift action and prevent harm to the system or data. However, these algorithms are susceptible to various types of attacks, making the security of these algorithms essential in SM to protect against general cyber threats and model attacks. Smart cyber defence is significantly important in SM because these systems are often interconnected and rely on data to make decisions. A single vulnerability in the system could have far-reaching consequences. Therefore, a comprehensive smart defence framework is essential to ensure the security and integrity of SM systems. By implementing advanced cybersecurity solutions and practices, manufacturers can protect their operations, customers, and bottom line from the growing threat of cyber-attacks. In SM security, evaluating a system involves continually identifying the categories of attacks, assessing the system's resilience against those attacks, and strengthening the system against those categories of attacks. This study introduces a novel framework for smart cyber defence analysis of DL model security. The framework also provides a threat model to identify potential security risks and vulnerabilities in designing and implementing DL systems that aim to make models robust and secure.

3. EXISTING METHODOLOGIES

One existing system for visitor authentication in smart door security using sensors is a proximity sensor-based authentication system. In this system, a proximity sensor is installed near the smart door, and when a visitor approaches the door, the sensor detects their presence and triggers a sequence of authentication checks. The first step in the authentication process involves facial recognition technology. A camera located near the proximity sensor captures an image of the visitor's face, which is then compared to a pre-stored image of authorized visitors. If the facial recognition process is successful, the visitor's identity is confirmed, and the door is unlocked. If the facial recognition process fails, the system can prompt the visitor to perform an additional authentication check, such as voice recognition or fingerprint scanning. The microphone and fingerprint scanner sensors are also installed near the proximity sensor and activated when required. Once all the necessary authentication checks are completed successfully, the door unlocks, allowing the visitor to enter the secured area. If any of the authentication checks fail, the system raises an alert, and the visitor is denied access. Overall, this system provides a secure and efficient way of authenticating visitors, ensuring that only authorized individuals gain access to the secured area. Another existing system is motion sensor-based system. In this system, a motion sensor is installed near the smart door, which detects the movement of the visitor as they approach the door. The sensor then triggers a sequence of authentication checks, similar to the proximity sensor-based system. The first step in the authentication process involves facial recognition technology. A camera located near the motion sensor captures an image of the visitor's face, which is then compared to a pre-stored image of authorized visitors. If the facial recognition process is successful, the visitor's identity is confirmed, and the door is unlocked.

4. PROPOSED METHODOLOGIES

Smart door security using face recognition with mask recognition using deep learning is a system that utilizes advanced artificial intelligence algorithms to provide accurate and reliable authentication. Deep learning is a subset of machine learning that uses artificial neural networks to analyse and learn from data. In this system, a deep learning model is trained to detect faces and masks from images captured by the camera installed near the smart door. Smart door security using face recognition with mask recognition is a system that has become increasingly relevant during the COVID-19 pandemic, where wearing a mask is a necessity. In this system, a camera equipped with facial recognition technology and mask detection capabilities is installed near the smart door. When a visitor approaches the door, the camera captures an image of their face and analyses it to detect the presence of a mask. If a mask is detected, the system performs facial recognition to authenticate the visitor's identity. If the facial recognition process is successful, the door is unlocked, and the visitor gains access to the secured area. If the system detects that the visitor is not wearing a mask, the system can prompt them to put one on before performing facial recognition to authenticate their identity. This step ensures that visitors comply with safety measures and reduces the risk of spreading contagious diseases. The face recognition with mask recognition system can also detect when a visitor removes their mask after gaining access to the secured area. In such cases, the system can alert the security team to investigate and take appropriate measures to ensure safety. Overall, the smart door security system using face recognition with mask recognition provides a convenient and secure way of authenticating visitors while enforcing necessary safety measures during the pandemic. This system can also be integrated with other security features, such as motion sensors, to provide a more comprehensive security solution.

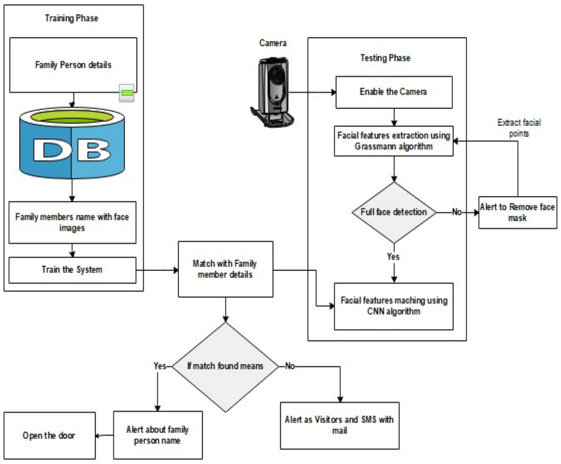
Training Phase
Family Person details
DB
Family members name with face images
Train the System
Camera
Testing Phase
Enable the Camera
Facial features extraction using Grassmann algorithm
Extract facial points
Full face detection
No
Alert to Remove face mask
Yes
Facial features maching using CNN algorithm
Match with Family member details
If match found means
Yes
No
Open the door
Alert about family person name
Alert as Visitors and SMS with mail

FIG 1: SYSTEM ARCHITECTURE

GRASSMANN ALGORITHM

For each frame in a video sequence, we first detect and crop the face regions. We then partition all the cropped face images into K different partitions. We partition the cropped faces by a Grassman algorithm type of algorithm that is inspired by video face matching algorithm. Sampling and characterizing a registration manifold is the key step in our proposed approach. The proposed algorithm presents a novel perspective towards frame selection by utilizing feature richness as the criteria. It is our assertion that quantifying the feature richness of an image helps in extracting the frames that have higher possibility of containing discriminatory features. In order to compute feature-richness, first the input (detected face) image I is preprocessed to a standard size and converted to grayscale. By performing face detection first and considering only the facial region, we ensure that other non-face content of the frame does not interfere with the proposed algorithm. Given a pair of face coordinates, we determine a set of affine parameters for geometric normalization. The affine transformation maps the (x, y) coordinate from a source image to the (u,v) coordinate of a normalized image.

Input: A set of P points on manifold

$\{X_i\}_{i=1}^{P} \in G(d,D)$

Output: Karcher meanμK

1. Set an initial estimate of Karcher mean $\mu_K = X_i$ by randomly picking one point in $X_i\}_{i=1}^{P}$

2. Compute the average tangent vector

A $= \frac{1}{P}\sum_{i=1}^{P} \quad log_{\mu K}(X_i)$

3. If $||A|| < \varepsilon$ then return μK stop, else go to Step 4

4. Move μK in average tangent direction $\mu K = exp_{\mu K}(\alpha A),$ where$\alpha > 0$ is a parameter of step size. Go to Step 2, until μK meets the termination conditions (reaching the max iterations, or other convergence conditions

Thus, the video is transformed on a trajectory that links different points on Grassmann manifold. The projection on Grassmann manifold requires decomposition. The main advantages of this projection are being reversible and have no loss of information. The next step consists on similarity computing between human skeletal joint trajectories in order to identify the identity of a given skeleton sequence.

5. EXPERIMENTAL RESULTS

Traditional security system requires the user a key, a security password, an RFID card, or ID card to possess access to the system. However, these security systems have deficiencies; for instance, they will be forgotten or stolen from unauthorized people. As a result, there is a need to develop a better system for higher security. For many years, people are using non-living thing (Like smart cards, plastic cards, PINS, tokens, keys) for authentication and to urge grant access in restricted areas. So, there are chances that one might forget the pins, keys, cards, etc. but in case face recognition is used for the door operating system then there is a hope of providing higher security. Face has many features (like eyes, nose, etc.) which are unique and it can reflect many emotions of a person. There are two sorts of biometric as physiological characteristics (face, fingerprint, finger geometry, hand geometry, palm, iris, ear and voice) and behavioural characteristics (gait, signature and keystroke dynamics

In this chapter used real time datasets. This framework used the face detection and recognition techniques. Then can evaluate the performance using accuracy metrics. The accuracy metric is evaluated as

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} *100$$

The proposed algorithm provide improved accuracy rate than the machine learning algorithms.
Accuracy table shown in table 1.

Algorithm	Accuracy (%)
Adaboost classifier	50
Viola jones classifier	70
Grassmann algorithm	90

Table (1) Accuracy table

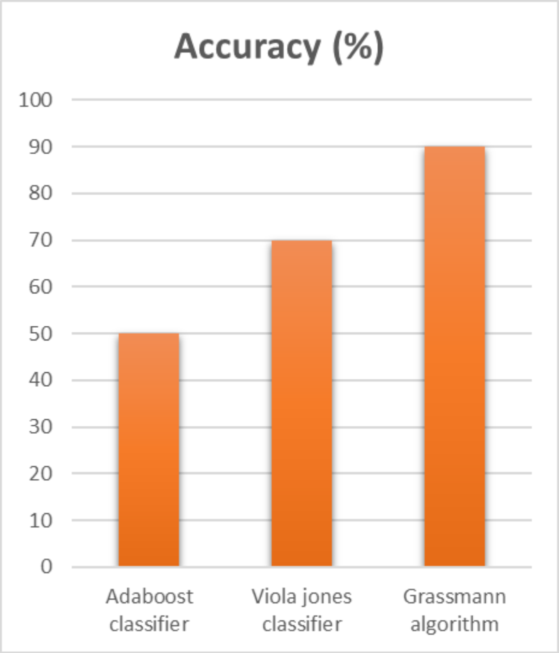

Fig 2: Performance report

From the performance chart in fig 4, Grassmann algorithm provide high level accuracy than the existing machine learning algorithms. The proposed system provides reduce number false positive rate.

6. CONCLUSION

In conclusion, smart door security using face recognition is a powerful and convenient technology that enhances the security and convenience of modern homes and buildings. Smart door security using face recognition offers several benefits compared to traditional key-based systems. One major advantage is that face recognition systems are more secure and difficult to bypass. Unlike keys, which can be lost or stolen, a person's face cannot be easily replicated or duplicated, making it a reliable form of identification. Additionally, face recognition systems offer greater convenience since there is no need to carry or keep track of keys. This can be especially useful for busy individuals who have their hands full or are prone to misplacing items. Another advantage of smart door security using face recognition is that it allows for greater control and customization of access. The system can be programmed to recognize specific faces and grant access only to those individuals, allowing for greater control over who is allowed into the building. The system can also be configured to restrict access during certain times of the day or to specific areas of the building, making it easier to manage access and increase security.

REFERENCES

[1] Mun, Hyung-Jin, and Min-Hye Lee. "Design for visitor authentication based on face recognition technology using CCTV." IEEE Access 10 (2022): 124604-124618.

[2] Aldahmani, Aaesha, et al. "Cyber-security of embedded IoTs in smart homes: Challenges, requirements, countermeasures, and trends." IEEE Open Journal of Vehicular Technology 4 (2023): 281-292.

[3] Mehmood, Muhammad Qasim, et al. "Invisible touch sensors-based smart and disposable door locking system for security applications." Heliyon 9.2 (2023).

[4] Ashraf, Zeeshan, et al. "Robust and lightweight remote user authentication mechanism for next-generation IoT-based smart home." IEEE Access (2023).

[5] Arshad, Iram, et al. "A novel framework for smart cyber defence: a deep-dive into deep learning attacks and defences." IEEE Access (2023).

[6] Nayak, Manjushree, and Ashish Kumar Dass. "GSM and Arduino based Smart Home Safety and Security System." Recent Trends in Information Technology and Its Application 6.1 (2023): 1-6.

[7] Guntur, Jalalu, et al. "IoT-Enhanced Smart Door Locking System with Security." SN Computer Science 4.2 (2023): 209.

[8] Mustafa, Bilal, et al. "IOT based low-cost smart home automation system." 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2021.

[9] Khan, M. Adil, et al. "Prototype model of an IoT-based digital and smart door locking system with enhanced security." 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). IEEE, 2022.

[10] Siswanto, Apri, Akmar Efendi, and Evizal Abdul Kadir. "Biometric face authentication system for secure smart office environments." Indonesian Journal of Electrical Engineering and Computer Science 32.2 (2023): 1134-1141.

[11] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[12] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[13] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[14] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[15] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[16] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[17] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[18] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[19] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[20] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[21] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019