

# Chapter 9

## Video-Based Human Authentication System for Access Control


**Chintan M. Bhatt**

*Charotar University of Science and Technology,  
India*

**Karan Mehul Kathiriya**

*Charotar University of Science and Technology,  
India*

**Kevin R. Patel**

 <https://orcid.org/0000-0002-5662-8222>  
*Charotar University of Science and Technology,  
India*

**Vidhya Piyushbhai Kothadia**

*Charotar University of Science and Technology,  
India*

**Yashvi Nileshbhai Raythatha**

*Charotar University of Science and Technology,  
India*

**Deep Kothadiya**

*Charotar University of Science and Technology,  
India*

**Poojan S. Dharaiya**

*Charotar University of Science and Technology,  
India*

**Vaishali Mewada**

*Charotar University of Science and Technology,  
India*

**Chirag Jethva**

*Charotar University of Science and Technology,  
India*

**Mayuri Jamanadas Popat**

*Charotar University of Science and Technology,  
India*

### ABSTRACT

*The issue of security is paramount in any organisation. Therefore, the authors intend to aid in the security of such organisations by bringing a video based human authentication system for access control which is a type of cyber physical system (CPS). CPS is an integration of computation and physical processes; here the computation is provided by face detection and recognition algorithm and physical process is the input human face. This system aims to provide a platform that allows any authorized person to enter*

DOI: 10.4018/978-1-7998-5101-1.ch009

*or leave the premise automatically by using face detection and recognition technology. The system also provides the administrator with the access to the logs, wherein he/she would be able to access the details of the people entering or leaving the organisation along with the live video streaming so that there is no sneaking of any unauthorized person with any other authorized person. The administrator can also do registration on behalf of a new person who requires access to the premises for a restricted amount of time only as specified by the administrator.*

## **INTRODUCTION**

There are many methods available around us that grant access after authenticating the person. For example, many of the organizations use an RFID base id-card scanning system or password-based authentication system to grant access, but in these kinds of systems, flaws are always there because as we know ID-cards can be stolen or we can miss-place it. Passwords are not secure every time. So nowadays most popular and secure methods are used for this kind of application such as biometrics identification. Many biometric identification systems are used like eye-retina, fingerprints, voice, face, etc. but while designing the system we must consider many factors as all of these methods have some pros and cons. We must take care of measures like cost, accuracy, reliability of the system, etc. In this chapter, the authors have used a face-based authentication system because nowadays spoofing is something which is a prominent threat associated with a fingerprint-based authentication system. Also, a voice-based authentication system is not that secure as face-based as we are aware that there may be a possibility that the biometric may get confused between voices or anyone can mimic anyone's voice. So, amongst all the biometrics, the face-based authentication system seems more secure. Currently, various methods available are face detection and face recognition. Like face recognition can be classified based on appearance, feature, or a hybrid mixture of both. The authors have implemented face recognition using the DLIB library which uses convolutional neural networks (CNN), a feature-based classification for face recognition. Using Face detection algorithm human faces are detected from the surrounding environment (background). At the time of face detection, various features like eyes, nose, jaw, etc. are identified and encoded. The encodings are stored in a database for further comparisons. When a person is detected, to recognize the person the features are encoded, and the encodings are compared with those stored in the database. If the encodings are nearly the same then that person is said to be authorized and the door is unlocked for him/her else an alert is passed to the security guard whenever an unknown person is detected. The objective of making this kind of system is to protect the organization from an unauthorized person right from the entrance of the premise only. If an un-authorize person tries to break into the building the security guards are alerted by sending the notification through the system and a photo of the person is captured and stored in the database so that even if he/she breaks into the building forcefully than he/she could be traced easily through this system. This system can also manage visitors as well as the interns coming to the organization and require only temporary access to the premise. They are given permission for a specific period and after that, the system will automatically deny his/her request to enter. Though this

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/video-based-human-authentication-system-for-access-control/266139](http://www.igi-global.com/chapter/video-based-human-authentication-system-for-access-control/266139)

## Related Content

---

### Information Communication Assistive Technologies for Visually Impaired People

Li-Minn Ang, Kah Phooi Sengand Tee Zhi Heng (2016). *International Journal of Ambient Computing and Intelligence* (pp. 45-68).

[www.irma-international.org/article/information-communication-assistive-technologies-for-visually-impaired-people/149274](http://www.irma-international.org/article/information-communication-assistive-technologies-for-visually-impaired-people/149274)

### Higher-Order Mobile Agents for Controlling Intelligent Robots

Yasushi Kambayashiand Munehiro Takimoto (2005). *International Journal of Intelligent Information Technologies* (pp. 28-42).

[www.irma-international.org/article/higher-order-mobile-agents-controlling/2382](http://www.irma-international.org/article/higher-order-mobile-agents-controlling/2382)

### AI and Smart Manufacturing: Building Industry 4.0

Kamaljeet Motia, Raj Kumarand Shalom Akhai (2024). *Modern Management Science Practices in the Age of AI* (pp. 1-28).

[www.irma-international.org/chapter/ai-and-smart-manufacturing/355154](http://www.irma-international.org/chapter/ai-and-smart-manufacturing/355154)

### AI in Sperm Evaluation

Panchami Sankar, Izadora Fernandes, Dwight Figueiredoand Milan Manoj (2025). *AI-Powered Systems for Healthcare Diagnostics and Treatment* (pp. 123-140).

[www.irma-international.org/chapter/ai-in-sperm-evaluation/376750](http://www.irma-international.org/chapter/ai-in-sperm-evaluation/376750)

### A Review of Generative Adversarial-Based Networks of Machine Learning/Artificial Intelligence in Healthcare

Anilkumar C. Suthar, Vedant Joshiand Ramesh Prajapati (2022). *Handbook of Research on Lifestyle Sustainability and Management Solutions Using AI, Big Data Analytics, and Visualization* (pp. 37-56).

[www.irma-international.org/chapter/a-review-of-generative-adversarial-based-networks-of-machine-learningartificial-intelligence-in-healthcare/298367](http://www.irma-international.org/chapter/a-review-of-generative-adversarial-based-networks-of-machine-learningartificial-intelligence-in-healthcare/298367)