Biometric Face Authentication System for Secure Smart Office Environments

by Apri Siswanto

Submission date: 09-Aug-2023 06:27AM (UTC+0700)
Submission ID: 2143263164
File name: 33890-66053-1-RV_OKE_turnitin.docx (1.84M)
Word count: 3821
Character count: 21242

Indonesian Journal of Electrical Engineering and Computer Science
Vol. 99, No. 1, Month 2099, pp. 1~1x
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v99.i1.pp1-1x

Biometric Face Authentication System for Secure Smart Office Environments

Apri Siswanto[1], Akmar Efendi[2], Evizal Abdul Kadir[3]
[1,2,3]Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau

Article Info

Article history:

Received month dd, yyyy
Revised month dd, yyyy
Accepted month dd, yyyy

Keywords:

Biometric
Face
Authentication
Smart office
Sensor

ABSTRACT (10 PT)

The use of the smart office concept in security has increased significantly recently. One of the areas of concern is the use of facial finger biometric technology for authentication systems, for example, authentication to enter a particular room in an office. This paper aims to describe a new prototype for office door automation and security that combines facial biometric technology and NodeMCU. Hopefully, this system will help increase the safety and comfort of office employees with easy installation and low cost. This system automatically controls (opens or closes) the door based on the biometrics of the user's face registered in the database on the NodeMCU microcontroller. The main system comprises a NodeMCU microcontroller, face sensors, and a door lock system.

Corresponding Author:

Apri Siswanto
Department of Informatics Engineering, Faculty of Engineering
Universitas Islam Riau
Jl. Kaharuddin Nasution No. 113 Pekanbaru, Riau, Indonesia
Email: aprisiswanto@eng.uir.ac.id

1. INTRODUCTION (10 PT)

The current development of information and communication technology offers convenience to users from various walks of life. One of the technologies currently being developed is smart office technology [1, 2]. The concept of a smart office is getting real, along with the increasing number of work activities integrated with digital technology and the internet. In simple terms, Smart Office is a collaboration of smart technology and the Internet of Things (IoT) implemented in a work environment. Smart office deployments help employees work smarter, better, and faster. In addition, the technology contained in Smart Office also helps businesses maintain spending efficiency and asset security. The technology embedded in this smart office usually includes building technology, security, front desk, meeting rooms, and other technologies [3-5].

A smart office is a combined system of technology and services specialized in office convenience with functions aimed at increasing efficiency, and security for owners and employees [6]. A smart office is an environment with information and communication technology that can support work by means of efficiency and social interaction functions [7]. According to [3] revealed, there are four advantages of a smart office that the office industry inevitably has to pay attention to, namely: "1) Smart Office educates workers; 2) Smart Office is a highly integrated ecosystem; 3) Smart Office supports remote work; 4) Smart Office keeps workers safe.

Access control and authentication, security, asset monitoring and protection, environmental management, energy-saving products, entertainment and audio distribution, home control, lighting, and appliance control are a few areas where smart office development is concentrated. Then a smart office can be

considered as a super system of subsystems that are interconnected with buildings [8]. Smart office requires connectivity between all systems and equipment in a building. This helps leaders to visualize information and make quick and correct decisions. Smart office is created using various strategies. Through building automation or building management systems, automatic centralized control of various building sub-systems, namely lighting, air temperature control, ventilation and air conditioning, and other systems [9]. The goal of a building automation system is to increase the efficient operation of the building management system, occupant comfort, and reduce energy consumption and operating costs, as well as increase the ility life cycle [10]. In the research of Siswanto, Katuk and Ruhana [11] they proposed a simple IoT-based home security system implemented using fingerprint biometric technology. This system is demonstrated using a prototype consisting of hardware and software components. The hardware includes a fingerprint sensor, microcontroller, wireless network router, application server, and smartphone. All components connect to the home network wi essly, making the system easier to implement at a lower cost. In Selvaraj and Chakrapani's research [12], they designed a light and fan control system automatically based on the intensity of sunlight. This research has successfully proposed low-cost and user-friendly energy saving in smart ices. This aligns with research by Efendi, Siswanto, and Sudarman [13], who designed an application that can help everyone control and monitor the use of home lights remotely using only a smartphone connected to the internet. This application uses the help of a microcontroller as a tool that can control electrical switches connected to mini servers connected to the network.

Furthermore, Alhajri research et al [14], proposed an IoT-based smart model for smart offices. This can help provide an effective work environment by focusing on two aspects. The first aspect is to remotely control all the devices in the office with a smartphone. The second and third aspects are increased s urity and safety. Furthermore, in Nur-A-Alam's research, et al [15] presented a smart monitoring and control automation system using remote technology (LoRa). The proposed LoRa-based system consists of a wireless communication system and various types of sensors, operated by a smartphone app d powered by a low-power battery, with an operating range of 3-12 km. The system connects the android phone and the microprocessor (ESP32) via Wi-Fi on the sending end. The ESP32 module is connected to the LoRa m dule. At the receiving end, ESP32 modules and LoRa modules without Wi-Fi were used. The study obtained correct environmental data, fire detection with 90% accuracy, and switching functionality with 2.33% accuracy at a distance of up to 12 km, demonstrating good system performance. The proposed system with a modular design has proven to be very effective in controlling and monitoring household appliances from a greater distance with relatively lower power consumption. Then in Prentice's research, et al [16, 17] developed and evaluated smart office applications.

Although many previous studies have designed security systems for smart offices based on the Internet of Things, the current system still has several gaps that need better development. Recent and previous studies by other researchers have reported many studies applied in the smart office environment. However, to our knowledge, no specific work designs a smart office using node-mcu microcontroller-based facial sensors and sends data using a Wifi network. Designing a smart office authentication system using face sensors can help reduce virus transmission impact, such as using fingerprint sensors.

This paper describes the design of a smart office prototype for the security of office doors or certain room doors with face sensors and the NodeMCU microcontroller. In our daily lives, security is a fundamental concern, and digital locks have emerged as a crucial component o his security system. Smart offices can be secured with a wide variety of security technologies. Biometric systems, digital lock systems, RFID-based security s tems, and electronic code locks are a few examples.

Currently, the biometric system is the choice for authentication systems. Biometric authentication comes from the Greek word bios which means life and metron which means measure. then it can be interpreted as the study of automatic methods to recognize hum s based on one or more parts of the human body or the behavior of the human hims f have uniqueness. In the world of information technology, biometrics are relevant to technology that is used to analyze physical and human behavior for authentication. For example in human physical recognition, namely by recognizing fingerprints, retinas, irises, facial patterns (facial patterns), signature (signature), and how to type (keystroke)[18-20].

One of the most accurate biometric technologies is facial biometrics. Everyone has different shapes, structures, and facial expressions [21]. In addition, facial biometrics is the most accurate identification technology because the face is the part of the human body that is most easily recognized. This biometric technology works by analyzing and detecting the most accurate points on the face for identifying a person's identity [22, 23]. In the process of detecting facial characteristics, three levels of facial characteristics are detected. The following are three levels of facial characteristics in facial biometric technology [24, 25]:

Level 1, the characteristics of this level are the most easily observable characteristics of the face. Generally, at this level, the system will detect the shape of the face (geometry) and the color of the facial skin.

Level 2, this characteristic detects a person's face from the facial structure. This facial structure is a component of the face, such as the nose, mouth, eyes, distance between the eyes, and others.

Level 3 is the micro level where the system will detect the most accurate point. this duck is part of the face that is not structured. For example, changes in skin color, scratches, facial skin texture, and others. This biometric technology is often used as a security system. Not only that, but even in other countries this technology has been used to tackle crime. In fact, this technology has been used in Singapore as a primary identity, such as an identity card.

2. METHOD (10 PT)

This research is experimental. The main objective of this research is to design a facial recognition and biometric system for implementation in smart office environments. Then, evaluating the performance of the designed system is an important task that must be completed, as stated in the background of the research problem. To achieve this goal, the Design Research Methodology (DRM) was used for each stage of the research [26]. The DRM stages used in this study consist of problem awareness, suggestion, development, evaluation, and conclusion.

Problem awareness and suggestions as two related steps in the general methodology of DRM were carried out in the first phase of the research. Awareness of previous research and research in smart office and biometric authentication has resulted in a good knowledge of research gaps and opportunities. It has been used as a basic research framework. The output of this step is a complete understanding of the basic design of automation and authentication systems in smart office environments and facial recognition biometric technology. Suggestions as a second step are related to investigations related to all the literature in automation and biometric authentication, especially in the smart office environment. The output of this stage is a tentative design which it describes the conceptual design of the proposed system. At the development stage, the output is a system prototype that includes technical design for monitoring, automation, and biometric authentication, especially in the IoT and smart office environments. The design of the prototype is as shown in Figure 1.

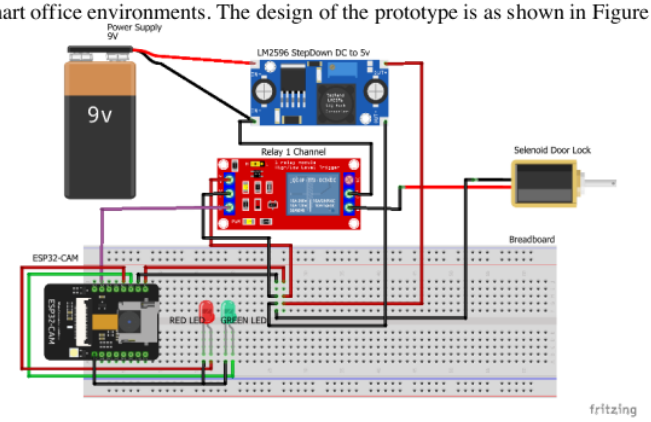

Figure 1. Hardware Prototype Design

The function of each component is described below:

(1) Face sensor (ESP32 CAM) functions as a sensor that receives facial images. The sensor generates digital data to create facial biometric templates and stores the data in a database for the first time and an input device to authenticate facial biometrics later. facial recognition works by mapping the unique geometrical face of someone who has been registered. The facial geometry in question is the distance from the chin to the forehead, the distance between the eyes, the length of the jawline, etc.

(2) The microcontroller board is the system's hub and manages all input and output activities. It takes data from facial sensors, and then processes it, stores it in memory, and communicates with the network.

(3) The power supply functions to change the current voltage so that it does not exceed the maximum limit of the device. Then it becomes backup power in the form of a battery.

(4) In this design, the relay functions as a switch (connector and circuit breaker) to operate the solenoid valve.

(5) The water flow sensor requires a voltage of 5V, therefore, a step-down module is used to reduce the power supply voltage from 12V to 5V.

(6) Solenoid door lock is an electronic device that can secure doors.

Evaluation is an important step in DRM that creates an important part of knowledge and lessons learned about the designed system and problem areas. The system is evaluated based on the proposed biometric

authentication to measure whether it will achieve the performance and security that the user requires. The evaluation will involve mathematical and statistical data which ultimately supports the results and conclusions of the research. The last step is the conclusion. This step identifies research contributions and limitations and processes research reports future research.

This research intends to implement face authentication at the main door in smart office environment. When this prototype is implemented in a smart office, an authorized employee is required to register his facial data with an application stored on the microcontroller. Employees scan their faces using the face sensor (ESP 32 cam). Scan results are stored in digital format in the microcontroller database. After that, the facial recordings are processed by generating a list of unique pattern features. The facial pattern feature is stored in the database. When employees scan their faces, the patterns generated from the faces will be matched with those stored in the database. If the two data match, then the microcontroller sends an approval signal to the switch to unlock the door and grant access to the employee. The flowchart in Figure 2 shows the process flow of the proposed system.

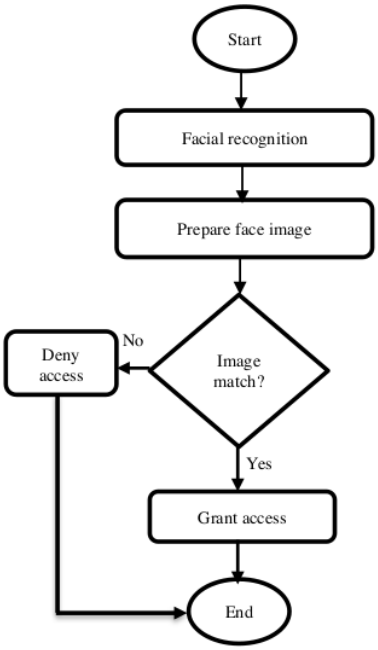

Figure 2. The process of prototype design

A client-side and server-side algorithms have been developed to show the basic authentication process. The process is divided into the enrolment and verification.

The client-side algorithm for the enrolment process.
User scans face using face sensor (ESP 32CAM);
Capture face image;
Extract face image;
Create face template;
Send face template to the microcontroller server for enrolment;

The server-side algorithm for the enrolment process.
Receive face template from sensor;
Store face template in the microcontroller database;

The client-side algorithm for the verification process.
User scans face using Sensor;

Capture face image;
Extract face image;
Create face template
Send face template to the Microcontroller Server for verification;

The server-side algorithm for the verification process.
Receive user face template from sensor;
Compare user face template with existing data in the microcontroller database;
if (user face templates match) {
open door;
else
display warning;
}

3. RESULTS AND DISCUSSION (10 PT)

This study aims to apply facial sensors for authentication at the main office door or particular doors that are implemented in an intelligent office environment. When this system is implemented in a smart office, company employees are asked to register their facial data with a simple application. The data will be stored in the NodeMCU microcontroller memory.

There are several stages in identifying facial characteristics. The first stage is the acquisition of facial biometric images. In this first stage, the system will digitally acquire a facial image. This acquisition process uses a scan tool or sensor with an infrared heat scan. The second stage is facing detection. After the system gets an image of the face, this facial biometric system will detect the face's shape, color, structure, and texture. In fact, this detection is also carried out on facial expressions and poses in its development. At this stage, the system will detect many points that are believed to be the most valid points. The third stage is the process of feature extraction and Face matching. The final stage of the facial recognition process in this biometric technology is extracting the facial features and performing the matching. The extraction and matching process is carried out using three approaches, namely appearance-based, model-based, and also texture-based. Of the three approaches, the texture-based approach is the most accurate. Figure 3 describes the configuration of biometric facial authentication using facial recognition biometrics. Hardware design is a design tool for building prototypes for smart office buildings.

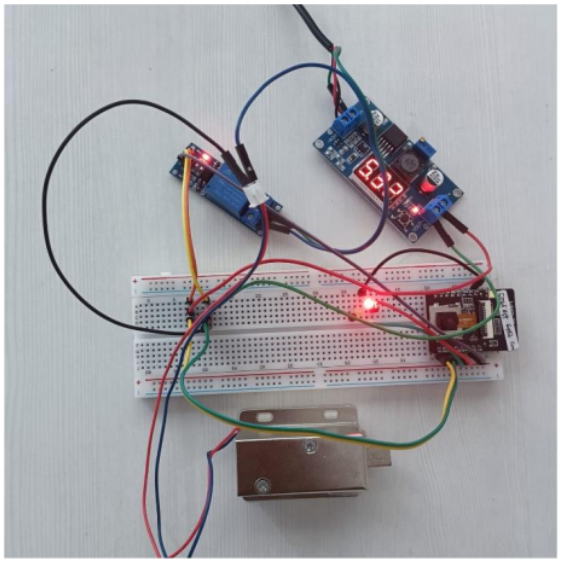

Figure 3. Hardware Prototype Design Results

In the process of registering and authenticating user face biometrics, simple coding is made here from the Arduino IDE. A user must register his face so that it can be recognized in the NodeMCU microcontroller

database. After being registered, the user will be allowed access to the prototype of the house that has been designed. Figure 4 shows the code from the face authentication and enrollment process for door locks in a smart office environment.

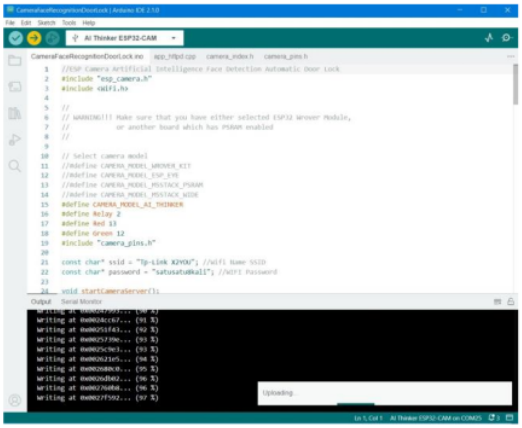

Figure 4. Face Recognition Program Code

Figure 5 describes the process of recording facial data. First, the user must register the face of the finger. The first step is recording digital data, verifying that the recording process is complete and that converting fingerprint data into a digital template is successful. After successfully recording into the database, the registered digital facial templates can access the smart office environment. Figure 6 shows the authorized authentication process.

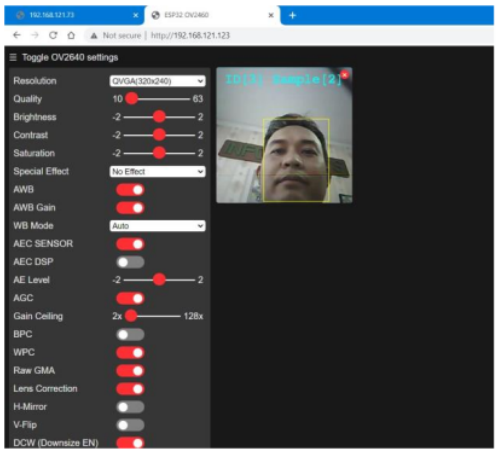

Figure 5. Authorized Authentication process

Whereas for users who are not registered in the database, the system will automatically refuse to gain access to the smart office environment. This is one of the advantages of a biometric system where there is no reason to forget passwords or keys because everything can be done with biometric technology in both the physical category of the body and human behavior. For the identification information rejected by the system, it can be seen in Figure 6.

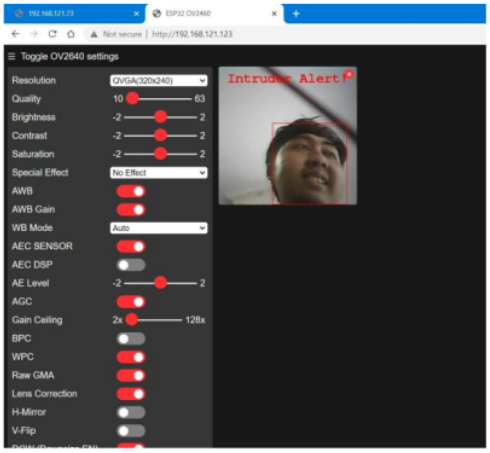

Figure 6. Denied Authentication process

Based on the tests, this prototype can work well in recording data and authenticating registered users in the database. A facial identification biometric system provides a good solution for door security in a smart office environment. A new prototype of a cost-effective biometric facial identification technology is proposed in this paper. It gives a basic idea of integrating door lock, face sensor, NodeMCU microcontroller, and door lock with a simple application. As a trend on biometric system security, this architecture will require implementation in real systems so that this system can provide better benefits. The future will be created for hardware and software design to see the capabilities of this system in secure smart offices. The author predicts this architecture is very economical.

4. CONCLUSION

The use of biometric fingerprints for door security systems in smart office environments using the NodeMCU microcontroller can be an alternative for reliable and low-cost smart office environment security. All the components used are relatively cheap and widely available in the market. It is expected that this system can provide functions similar to real systems for security in a smart office environment.

REFERENCES

[1] M. Sigala, A. Beer, L. Hodgson, and A. O'Connor, *Big Data for Measuring the Impact of Tourism Economic Development Programmes: A Process and Quality Criteria Framework for Using Big Data*. 2019.
[2] G. Nguyen *et al*., "Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey," *Artif. Intell. Rev.*, vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.
[3] C. Shorten and T. M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0197-0.
[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
[5] K. Sivaraman, R. M. V. Krishnan, B. Sundarraj, and S. Sri Gowthem, "Network failure detection and diagnosis by analyzing syslog and SNS data: Applying big data analysis to network operations," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 9 Special Issue 3, pp. 883–887, 2019, doi: 10.35940/ijitee.I3187.0789S319.
[6] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.
[7] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, "Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning," *IEEE Access*, vol. 7, pp. 115749–115759, 2019, doi: 10.1109/ACCESS.2019.2931637.
[8] S. Kumar and M. Singh, "Big data analytics for healthcare industry: Impact, applications, and tools," *Big Data Min. Anal.*, vol. 2, no. 1, pp. 48–57, 2019, doi: 10.26599/BDMA.2018.9020031.
[9] L. M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, "Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges," *IEEE Access*, vol. 7, pp. 6473–6492, 2019, doi: 10.1109/ACCESS.2018.2887076.
[10] B. P. L. Lau *et al*., "A survey of data fusion in smart city applications," *Inf. Fusion*, vol. 52, no. January, pp. 357–374, 2019, doi: 10.1016/j.inffus.2019.05.004.
[11] Y. Wu *et al*., "Large scale incremental learning," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2019-June, pp. 374–382, 2019, doi: 10.1109/CVPR.2019.00046.
[12] A. Mosavi, S. Shamshirband, E. Salwana, K. wing Chau, and J. H. M. Tah, "Prediction of multi-inputs bubble column reactor using a novel hybrid model of computational fluid dynamics and machine learning," *Eng. Appl. Comput. Fluid Mech.*, vol. 13, no. 1, pp. 482–492, 2019, doi: 10.1080/19942060.2019.1613448.
[13] V. Palanisamy and R. Thirunavukarasu, "Implications of big data analytics in developing healthcare frameworks – A review," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 31, no. 4, pp. 415–425, 2019, doi: 10.1016/j.jksuci.2017.12.007.

[14] J. Sadowski, "When data is capital: Datafication, accumulation, and extraction," *Big Data Soc.*, vol. 6, no. 1, pp. 1–12, 2019, doi: 10.1177/2053951718820549.
[15] J. R. Saura, B. R. Herraez, and A. Reyes-Menendez, "Comparing a traditional approach for financial brand communication analysis with a big data analytics technique," *IEEE Access*, vol. 7, pp. 37100–37108, 2019, doi: 10.1109/ACCESS.2019.2905301.
[16] D. Nallaperuma *et al.*, "Online Incremental Machine Learning Platform for Big Data-Driven Smart Traffic Management," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 12, pp. 4679–4690, 2019, doi: 10.1109/TITS.2019.2924883.
[17] S. Schulz, M. Becker, M. R. Groseclose, S. Schadt, and C. Hopf, "Advanced MALDI mass spectrometry imaging in pharmaceutical research and drug development," *Curr. Opin. Biotechnol.*, vol. 55, pp. 51–59, 2019, doi: 10.1016/j.copbio.2018.08.003.
[18] C. Shang and F. You, "Data Analytics and Machine Learning for Smart Process Manufacturing: Recent Advances and Perspectives in the Big Data Era," *Engineering*, vol. 5, no. 6, pp. 1010–1016, 2019, doi: 10.1016/j.eng.2019.01.019.
[19] Y. Yu, M. Li, L. Liu, Y. Li, and J. Wang, "Clinical big data and deep learning: Applications, challenges, and future outlooks," *Big Data Min. Anal.*, vol. 2, no. 4, pp. 288–305, 2019, doi: 10.26599/BDMA.2019.9020007.
[20] M. Huang, W. Liu, T. Wang, H. Song, X. Li, and A. Liu, "A queuing delay utilization scheme for on-path service aggregation in services-oriented computing networks," *IEEE Access*, vol. 7, pp. 23816–23833, 2019, doi: 10.1109/ACCESS.2019.2899402.
[21] G. Xu, Y. Shi, X. Sun, and W. Shen, "Internet of things in marine environment monitoring: A review," *Sensors (Switzerland)*, vol. 19, no. 7, pp. 1–21, 2019, doi: 10.3390/s19071711.
[22] M. Aqib, R. Mehmood, A. Alzahrani, I. Katib, A. Albeshri, and S. M. Altowaijri, *Smarter traffic prediction using big data, in-memory computing, deep learning and gpus*, vol. 19, no. 9. 2019.
[23] S. Leonelli and N. Tempini, *Data Journeys in the Sciences*. 2020.
[24] N. Stylos and J. Zwiegelaar, *Big Data as a Game Changer: How Does It Shape Business Intelligence Within a Tourism and Hospitality Industry Context?* 2019.
[25] Q. Song, H. Ge, J. Caverlee, and X. Hu, "Tensor completion algorithms in big data analytics," *arXiv*, vol. 13, no. 1, 2017.
[26] L. T. Blessing and A. Chakrabarti, *DRM: A design reseach methodology*: Springer, 2009.

BIOGRAPHIES OF AUTHORS *:*

Biometric Face Authentication System for Secure Smart Office Environments

ORIGINALITY REPORT

24%	16%	17%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Apri Siswanto, Akmar Efendi, Zalian Hasrin, Bustamil Arifin. "Chapter 18 Two-Factor Authentication for Safe Deposit Box Based on Embedded System", Springer Science and Business Media LLC, 2022 Publication	4%
2	jurnal.iainkediri.ac.id Internet Source	4%
3	e-space.mmu.ac.uk Internet Source	3%
4	Submitted to Graduate School, Mahasarakham University Student Paper	2%
5	Kholidiyah Masykuroh, Fikra Titan Syifa, Gatot Rizky Setiyanto, Afifah Dwi Ramadhani, Danny Kurnianto, Nanda Iryani. "Prototype Smart Door Lock By Using Wireless Network Based on Arduino Uno", 2021 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), 2021	2%

Publication

6	Akmar Efendi, Apri Siswanto, Adrian Sudarman. "Application Control and Monitoring of Light Usage in Smart Home Environment", 2018 Third International Conference on Informatics and Computing (ICIC), 2018 Publication	1 %
7	ijeecs.iaescore.com Internet Source	1 %
8	Sri Yuliani, Arimuliani Ahmad, Ikel Srinoviati. "Sociolinguistics perspectives on gender patterns in instagram", Journal of Education and Learning (EduLearn), 2020 Publication	1 %
9	Submitted to Hallym University Ilsong Memorial Library Student Paper	1 %
10	Submitted to Higher Education Commission Pakistan Student Paper	1 %
11	beei.org Internet Source	1 %
12	Submitted to Universiti Teknologi MARA Student Paper	1 %

13	Submitted to Raffles College of Higher Education Sdn Bhd Student Paper	<1%
14	garuda.kemdikbud.go.id Internet Source	<1%
15	paper.ijcsns.org Internet Source	<1%
16	Valeriia Afonina, Knut Hinkelmann, Devid Montecchiari. "Chapter 2 Enriching Enterprise Architecture Models withHealthcare Domain Knowledge", Springer Science and Business Media LLC, 2023 Publication	<1%
17	www.researchgate.net Internet Source	<1%
18	Rogel Ladia Quilala, Theda Flare Ginoy Quilala. "Document verification using quick response code with modified secure hash algorithm-1 and modified blowfish algorithm", Indonesian Journal of Electrical Engineering and Computer Science, 2022 Publication	<1%
19	"Smart City and Informatization", Springer Science and Business Media LLC, 2019 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		