JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

Design and Implementation of Safe Security System Using Multi-Factor Authentication: Facial Recognition, National ID Card and PIN

Syahri Muharom[1*], Sigit Adhi Sulistianto[2], Riza Agung Firmansyah[3], Wahyu Setyo Pambudi[4], Muchammad Kurniawan[5].

[1*,2,3,4] Electrical Engineering, Institut Teknologi Adhi Tama Surabaya, Indonesia.
[5]Informatics Engineering, Institut Teknologi Adhi Tama Surabaya, Indonesia.
syahrimuharom@itats.ac.id[1*], sigitadhi@gmail.com[2], rizaagungf@itats.ac.id[3], wahyusp@itats.ac.id[4], muchamad.kurniawan@itats.ac.id[5]
[*]) syahrimuharom@itats.ac.id

Abstract-Traditional storage cabinets that rely on conventional locks and provide unrestricted access are highly vulnerable to theft. To safeguard documents and other valuable items from loss, an integrated security system is required to regulate and secure access to storage compartments. This study aims to develop a security system based on facial recognition, ID cards, and a keypad interface The Haar Cascade classifier combine with LPBH utilizing the OpenCV library is employed for facial identification by storing 30 photos per person in a designated folder, and subsequently comparing facial objects captured by a webcam against pre-stored and trained facial data in the database. The analysis indicates that the optimal detection range of the system is between 100 and 300 cm. In facial orientation testing, the best recognition performance is achieved at angles between 0° and 40°. Based on 20 experimental trials, the system demonstrates an average success rate of 80%. These results suggest that a facial-recognition-based security system utilizing the Haar Cascade approach is feasible for implementation as a protective mechanism for storage cabinets.

Keywords: Security System, Face Recognition, PIN, Identity Card, Storage.

1. INTRODUCTION

Security is one of the most critical factors in daily life. An unsafe environment can significantly affect social activities, economic operations, and overall public well-being[1]. Security threats arise from various criminal acts, including theft. Consequently, both individuals and organizations employ storage cabinets or safes to reduce the risk of loss and to protect valuable assets such as jewelry, cash, letters, and important documents[2]. However, conventional storage cabinets typically rely on mechanical locks and often provide limited control over who may access the cabinet. This design makes them vulnerable to criminal attempts, particularly theft. In many cases, stealing or duplicating a physical key is a common method used by offenders to gain unauthorized access. Therefore, an effective storage cabinet should not only be physically robust but should also incorporate an access-control mechanism that ensures the cabinet can be opened only through valid and verified authentication.

To address this challenge, this study proposes a multi-factor security system for a storage cabinet that integrates facial recognition[3], RFID-based identity verification (e-KTP)[4], and a Personal Identification Number (PIN) entered through a keypad[5]. In this configuration, the cabinet can be unlocked only after completing three sequential authentication steps, facial verification, RFID card validation, and PIN entry. [6]. implemented authentication using RFID combined with a PIN/password and reported strong system reliability[7]. RFID technology is widely adopted in other practical applications such as attendance systems [8] and payment systems [9], further supporting its feasibility for access-control implementation. Additional research highlights the potential of facial recognition for security applications. [10]. Arduino is an open-source electronics platform based on easy-to-use hardware and software, in practical applications, Arduino microcontrollers are extensively employed in various embedded systems, for example used to monitoring[11], [12], [13], control [14], [15], [16].

The system used a webcam and a Raspberry Pi microcontroller; a recognized face triggered a servo mechanism to unlock the safe, while an LCD displayed the lock status. Re-locking was enabled via a manual push button. The authors reported high accuracy under frontal, upright facial positioning within a limited operational distance range[17]. Applying a Facial Recognition System Using the Eigenface Method Connected to a Smartphone, applied Eigenfaces to reduce image dimensionality and perform linear transformation using eigenvalues and eigenvectors [18]. Design of a Storage Locker System Based on Owner Password and Facial

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

Recognition, combined password verification with image processing for facial recognition using a triangular face method that measures pixel-to-pixel distances among key facial landmarks (eyes, nose, and mouth) [19].

The Haar Cascade Classifier is a machine learning-based object detection algorithm introduced by Viola and Jones, which operates by scanning input images using a sliding window across multiple scales to localize facial regions. This algorithm employs Haar-like features that represent pixel intensity differences between dark and bright regions, trained using the AdaBoost algorithm and organized into a multi-stage cascade structure to achieve efficient and real-time detection[20]. Local Binary Patterns Histograms (LBPH) algorithm to constitute a complete facial recognition pipeline. The LBPH algorithm extracts local texture features from facial images by comparing each pixel against its surrounding neighbors within a circular pattern, generating binary codes that are accumulated into a histogram representing the facial feature vector. During the recognition phase, the system computes the distance between the feature vector of the live-captured face and those of enrolled users stored in the database; an identity whose minimum distance falls below a predefined decision threshold is granted access, whereas unrecognized faces are denied[21]. Drawer Security Using an LDR Sensor and RFID, used an LDR sensor to detect drawer status. The system also employed an ESP8266 Wi-Fi module to transmit status information to a web service, while a solenoid was used for locking/unlocking and the door status was displayed online. [22].

Based on the aforementioned considerations, this study makes the following contributions is a three-stage sequential authentication system integrating facial recognition, RFID-based e-KTP verification, and a 6-digit PIN entry, which significantly reduces the risk of unauthorized access compared to single- or dual-factor authentication approaches. And an explicit two-stage facial recognition pipeline in which the Haar Cascade Classifier serves as the face detector to localize the facial region from webcam input, while the Local Binary Patterns Histograms (LBPH) algorithm performs identity classification by matching the detected face against a pre-enrolled dataset stored in the database.

2. RESEARCH METHODOLOGY

2.1 System Design

A system can operate correctly only when it is supported by a well-defined hardware architecture. The proposed device architecture is represented by a block diagram, as illustrated in Figure 1.

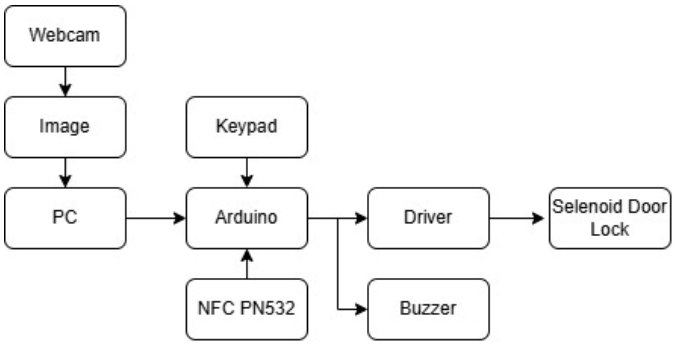


Figure 1. Block Diagram of the Proposed System

As shown in Figure 1, the system employs a webcam to capture facial images. Image processing and facial recognition are executed on a laptop using computer vision algorithms. After successful facial verification, the second authentication stage requires the user to scan an e-KTP (Indonesian National ID Card) via a PN532 NFC/RFID module. The third stage requires the user to enter a 6-digit PIN via a keypad. If all verification stages are valid, the system issues a command to release the solenoid door lock, thereby unlocking the storage cabinet.

2.2 Haar Cascade Classifier with LBPH Design

The facial recognition system in this study employs a two-stage pipeline combining the Haar Cascade Classifier for face detection and the Local Binary Patterns Histograms (LBPH) algorithm for identity recognition. The complete pipeline is divided into two stages: the training stage (enrollment) and the recognition stage, as illustrated in the block diagram below Figure 2.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

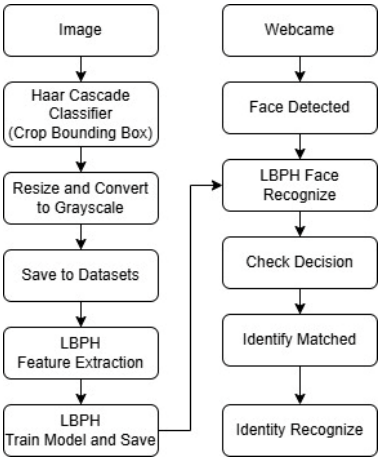


Figure 2. Block Diagram face identification system

In the training stage, facial images are captured using a webcam, with 30 images collected per authorized user. The Haar Cascade Classifier detects and crops the facial region from each image, which is then resized and converted to grayscale. The preprocessed images are stored in a structured database folder per user and used to train the LBPH recognition model via the recognizer train function. The trained model is saved as trainer containing the histogram feature vectors of all enrolled users. In the recognition stage, a live webcam frame is captured and passed through the same Haar Cascade Classifier to localize the facial region. The detected face is preprocessed and fed into the trained LBPH model via recognizer predict, which computes the Chi-square distance between the probe histogram and all enrolled gallery histograms. A decision threshold (θ) is applied: if $d < \theta$, the identity is confirmed and the system proceeds to the next authentication stage (e-KTP scanning).

2.2 System Design

A flowchart is commonly used to describe program logic and is a fundamental artifact in software design. The overall system workflow is illustrated in Figure 3.

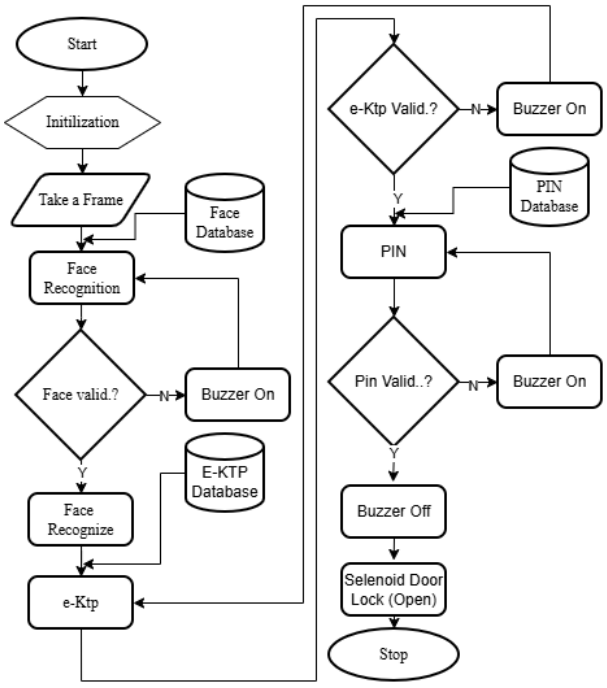


Figure 3. Overall System Flowchart

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

.

The flowchart describes the operational sequence of the storage cabinet security system based on facial recognition, e-KTP authentication, and PIN verification. First, the system initializes and verifies that all required modules are available. Next, the camera captures a facial image, which is processed using OpenCV and the Haar Cascade approach to determine whether the detected face matches the entries stored in Database Subsystem 1 (face database). After facial verification, the system proceeds to read the e-KTP using the NFC/RFID module. This stage provides up to three attempts to read and validate the e-KTP against Database Subsystem 2 (ID database). If the scanned credential does not match the database, the system triggers the buzzer alarm, the LCD displays "NOT DETECTED" (or equivalent), and the system automatically returns to the facial recognition stage. When the e-KTP is validated, the system requests a 6-digit PIN via keypad input. If the PIN is correct, the controller activates the solenoid lock to unlock the cabinet; otherwise, the system issues a failure alert and returns to the appropriate earlier stage based on the programmed logic.

2.3 Hardware Design

Hardware design specifies how all components are electrically connected within the system. The wiring/interconnection schematic of the proposed device is shown in Figure 4.

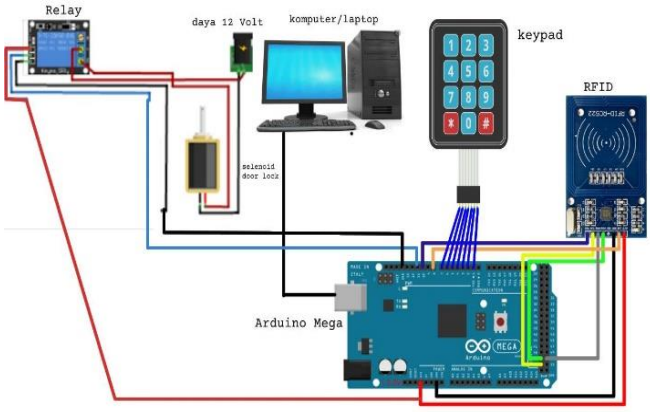


Figure 4. Hardware Wiring Diagram of the System

This diagram defines the interconnections between the Arduino Mega, PN532 module, keypad, buzzer, solenoid lock driver circuitry, and communication link to the laptop.

3. RESULT AND DISCUSSION

3.1. The Facial Recognition Process

The facial-recognition workflow is divided into two stages: (1) data acquisition (enrollment/training) and (2) recognition (identification/verification). During enrollment, the webcam captures facial images in real time. Face detection is performed using the Haar Cascade classifier in OpenCV. The detected face region is converted from RGB to grayscale for standardization and computational efficiency. The processed facial images are stored as the training dataset and serve as reference samples for recognition Figure 5.

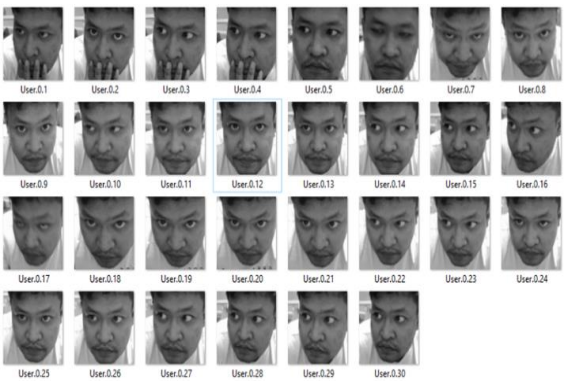


Figure 5. Face Dataset

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

In the recognition stage, the webcam captures live facial images; the system detects and preprocesses the face region and compares it against the enrolled dataset to determine whether the user is authorized. Example recognition output is shown in Figure 6.

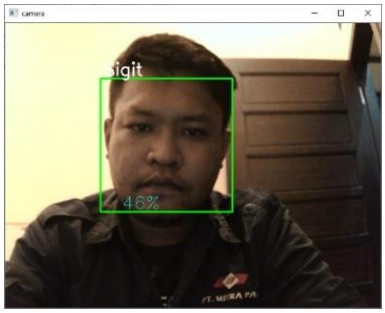
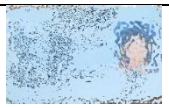
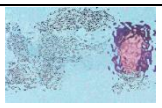
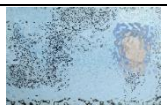
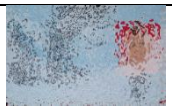


Figure 6. Face Recognize

3.2. RFID-Based Identity Card (e-KTP) Test Results

RFID/NFC module testing was conducted to evaluate the reading performance and reliability of the PN532 module when scanning e-KTP cards. The e-KTP scan serves as the second authentication factor. If the scanned credential matches the database record, the user proceeds to the next stage; otherwise, access is denied. Based on eight trials, all e-KTP data were successfully read, indicating that the RFID/NFC module provides reliable performance for this system Table I.

Table 1. e-KTP ID Detection

e-KTP	ID	Result	e-KTP	ID	Result
	1364851447365	Detected		3759678310354	Detected
	1563428142474	Detected		6742412868109	Detected
	1365133133141	Detected		7932620305489	Detected
	8979281182876	Detected		3013239914460	Detected

3.3. Face Recognition Test Results

Face recognition testing was conducted to evaluate the accuracy and operational robustness of the proposed authentication subsystem. In this study, a Haar Cascade–based approach was adopted as the primary method for facial detection and subsequent recognition against an enrolled face database. The method enables the system to determine whether a face captured by the webcam corresponds to an authorized user whose facial samples have previously been collected during the enrollment stage. Representative recognition outcomes for multiple users are presented in Figure 7, where the system successfully detects the facial region and provides an identification output for each tested subject.

Figure 7 illustrates the qualitative performance of the face recognition module and confirms that the proposed pipeline is capable of detecting facial objects and producing identity decisions under the tested conditions.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

Following this initial verification, additional experiments were performed to characterize the system's performance under varying operational parameters, Table 2 test result face recognition based on distance.

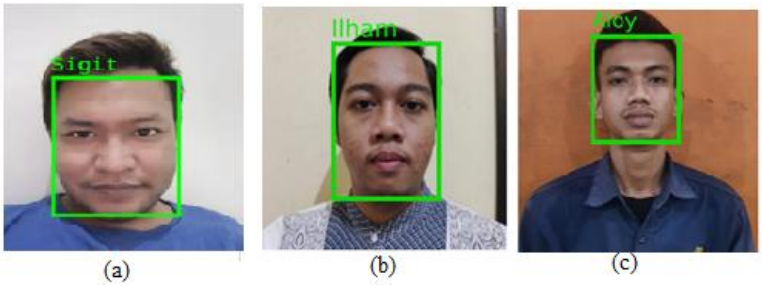
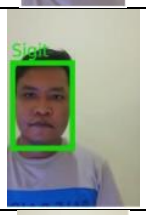


Figure 7. Face Recognize with 3 persons

Table 2. Face Detection with Distance

No	Distance	Face	Result
1	100 cm		Detected
2	150 cm		Detected
3	300 cm		Detected
4	350 cm		Not Detected

As summarized in Table 2, the proposed system demonstrates its most reliable face detection and recognition performance when the subject-to-camera distance lies within 100–300 cm. Within this range, the captured facial region maintains sufficient spatial resolution to support stable feature representation and consistent matching against the enrolled database. In contrast, at distances exceeding 300 cm, recognition becomes impractical because the face occupies a significantly smaller portion of the image frame. This reduction in effective facial pixel coverage limits the amount of discriminative information available for processing, thereby degrading both detection robustness and recognition reliability. In addition to distance evaluation, an angle-based experiment was conducted to characterize the system's tolerance to variations in facial orientation (pose) relative to the camera. This test aims to determine the maximum allowable deviation from a frontal view that still enables dependable recognition. The evaluation was performed across a pose range of 0° to 90°, representing progressively larger rotations away from the camera's optical axis. The corresponding outcomes of the angle-based assessment are reported in Table 3, which provides the measured recognition behavior under different orientation conditions.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

Table 3. Face Detection with Degree

No	Degree	Hasil	Keterangan
1	0º		Detected
2	20º		Detected
3	40º		Detected
4	60º		Not Detected

During the pose (angle)-based face recognition evaluation, the experimental results indicate that the system achieves its most reliable recognition performance when the facial orientation relative to the camera remains within 0° to 40°. Within this angular range, the captured facial region preserves adequate visibility of key facial characteristics, enabling consistent feature representation and stable matching against the enrolled database. However, when the orientation exceeds 40°, recognition performance deteriorates. This degradation is primarily attributed to partial facial visibility caused by self-occlusion and reduced frontal exposure, where only approximately 50% of the facial region is observable in the camera frame. As a result, essential discriminative features become incomplete or distorted, which can negatively affect both the robustness of face detection and the accuracy of the subsequent recognition process.

3.4. Overall System Test Results

Overall system performance testing was conducted as an end-to-end evaluation involving three users and three e-KTP cards. The aggregated results of the complete system trials are presented in Table . Based on the experimental outcomes, a total of four failures were observed across the trials. Specifically, three failures occurred during the face recognition stage, whereas one failure occurred during the e-KTP reading stage. The face recognition failures were primarily attributed to environmental and acquisition-related factors. First, unstable indoor lighting conditions were encountered during testing, where illumination levels dropped abruptly, resulting in degraded facial image quality. Under reduced illumination, the captured facial region exhibits lower contrast and reduced visibility of salient facial features, which negatively affects the face detection and recognition pipeline and can lead to missed detections or incorrect matching decisions. Second, mechanical vibration during the recognition process also contributed to performance degradation. Vibration can introduce motion blur and focus instability, thereby reducing sharpness and altering the effective facial texture representation used for recognition. Consequently, the camera may fail to maintain a consistent focus on the user's face, which can further decrease recognition reliability can see at Table 4.

Table 4. Overall Test Results

No	e-KTP	PIN	User	Status	Pin	Face	Key Status	Buzzer
1	1365133133141	142755	Sigit	Register	True	Detected	Open	Off
2	1365133133141	142755	Aloy	-	-	Not Detected	-	On
3	1365133133141	142789	Sigit	Register	True	Detected	Close	On
4	8429080251675	142755	Sigit	Register	True	Detected	Close	On
5	8429080251675	142755	Aloy	Register	True	Detected	Open	Off
6	8429080251675	142755	Sigit	-	-	Not Detected	-	On
7	8429080251675	123456	Aloy	Register	False	Detected	Close	On
8	9309708505590	142755	Ilham	Register	True	Detected	Open	Off
9	9309708505590	142755	Sigit	-	-	Not Detected	-	-

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

.

10	9309708505590	123456	Ilham	Register	True	Detected	Open	Off
11	1365133133141	143245	Sigit	Register	False	Detected	Close	On
12	9309708505590	123456	Aloy	Register	False	Detected	Close	On
13	9309708505590	133576	Iham	Register	False	Detected	Open	Off
14	8429080251675	143278	Sigit	Register	False	Detected	Open	Off
15	1365133133141	123456	Aloy	Tidak	-	Detected	-	On
16	9309708505590	123456	Aloy	Register	True	Detected	Open	Off
17	1365133133141	123456	Sigit	Register	True	Detected	Open	Off
18	1365133133141	123456	Sigit	Register	True	Detected	Open	Off
19	8429080251675	123456	Sigit	Register	True	Detected	Open	Off
20	9309708505590	123456	Ilham	Register	True	Detected	Open	Off

4. CONCLUSION

This study designed and implemented a multi-factor authentication security system for a storage cabinet integrating three sequential verification stages, face detection and recognition, RFID-based e-KTP scanning, and 6-digit PIN entry. The facial recognition pipeline employs the Haar Cascade Classifier for face detection to localize the facial region from webcam input, while the LBPH algorithm performs identity recognition by computing histogram-based feature distances against the pre-enrolled dataset. Based on experimental results, the optimal subject-to-camera distance is 100–300 cm. At distances below 100 cm, the facial region may be partially cropped, whereas at distances exceeding 300 cm, the face occupies an insufficient portion of the image frame for reliable feature extraction. In the facial orientation test, the best recognition performance was achieved at pose angles between 0° and 40°, beyond 40°, self-occlusion reduces visible facial area to approximately 50%, significantly degrading recognition accuracy. The overall system achieved a success rate of 80% across 20 end-to-end trials, with a False Rejection Rate (FRR) of 20%, primarily attributed to unstable lighting conditions and mechanical vibration. The main contribution of this study is a functional three-factor sequential authentication prototype combining biometric facial recognition, RFID-based identity verification, and PIN entry. Future work should incorporate adaptive illumination correction and deep learning-based recognition algorithms to improve system robustness and generalization.

REFERENCES

[1] V. V. Muthuswamy, “An Empirical Exploration of Human Factors, Sense of Security, and Well-Being in Contemporary Social Work Environments,” *J. Hum. Secur.*, vol. 19, no. 2, 2023, Accessed: Feb. 23, 2026. [Online]. Available: https://jhumansecurity.com/menuscript/index.php/jhe/article/view/117

[2] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, p. 1333, Jan. 2023, doi: 10.3390/electronics12061333.

[3] J. Qiang, D. Wu, H. Du, H. Zhu, S. Chen, and H. Pan, “Review on Facial-Recognition-Based Applications in Disease Diagnosis,” *Bioengineering*, vol. 9, no. 7, p. 273, Jul. 2022, doi: 10.3390/bioengineering9070273.

[4] A. A. Nair, R. Adithyan, A. Unni, and S. Nalinakshan, “RFID Door Lock Access Control Systems: Trends, Technologies and Applications,” in *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Feb. 2025, pp. 906–912. doi: 10.1109/IDCIOT64235.2025.10914928.

[5] C. Adams, “Identification,” in *Encyclopedia of Cryptography, Security and Privacy*, Springer, Cham, 2025, pp. 1165–1165. doi: 10.1007/978-3-030-71522-9_77.

[6] D. Antonio, “Rancang Bangun Aplikasi Keamanan Brankas Berbasis Sinar Laser Dengan Mikrokontroller Arduino Nano Dan Uno R3,” *J. Sisfokom Sist. Inf. Dan Komput.*, vol. 2, no. 2, Art. no. 2, Sep. 2013, doi: 10.32736/sisfokom.v2i2.90.

[7] N. W. Anggara, G. Dewantoro, and A. A. Febrianto, “Sistem Pembuka Brankas Menggunakan E-KTP atau Password Dilengkapi dengan GPS,” *J. Teknol. Elektro*, vol. 13, no. 2, Art. no. 2, May 2022, doi: 10.22441/jte.2022.v13i2.009.

[8] T. Tukadi, “Rancang Bangun Aplikasi Presensi Menggunakan SmartCard RFID Berbasis Web,” *CYCLOTRON*, vol. 4, no. 2, Art. no. 2, Aug. 2021, doi: http://dx.doi.org/10.30651/cl.v4i2.5649.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 14, No. 1, March 2026
DOI: https://doi.org/10.35447/jitekh.v14i1.1306

.

[9] M. L. B. Pamungkas, A. Rachmawan, and S. Muharom, "Rancang Bangun Vending Machine dengan RFID Sebagai Pembayaran Elektronik Berbasis Arduino," *Pros. Semin. Nas. Tek. Elektro Sist. Inf. Dan Tek. Inform. SNESTIK*, vol. 1, no. 1, Art. no. 1, Jun. 2021, doi: 10.31284/p.snestik.2021.1747.

[10] M. H. Khairuddin, S. Shahbudin, and M. Kassim, "A smart building security system with intelligent face detection and recognition," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1176, no. 1, p. 012030, Aug. 2021, doi: 10.1088/1757-899X/1176/1/012030.

[11] E. Alfianto, S. Agustini, S. Muharom, F. Rusydi, and I. Puspitasari, "Design Monitoring Electrical Power Consumtion at Computer Cluster," *J. Phys. Conf. Ser.*, vol. 1445, p. 012027, Jan. 2020, doi: 10.1088/1742-6596/1445/1/012027.

[12] O. Derek, E. K. Allo, and N. M. Tulung, "Rancang Bangun Alat Monitoring Kecepatan Angin Dengan Koneksi Wireless Menggunakan Arduino Uno," *J. Tek. Elektro Dan Komput.*, vol. 5, no. 4, Art. no. 4, Aug. 2016, doi: 10.35793/jtek.v5i4.13199.

[13] D. T. L. Praing, A. Purba, and S. Muharom, "Monitoring Suhu Dan Infus Pasien Rumah Sakit Pasca Pandemic Berbasis Android," *Pros. Semin. Nas. Sains Dan Teknol. Terap.*, no. 0, Art. no. 0, Nov. 2022, Accessed: Jan. 18, 2023. [Online]. Available: http://ejurnal.itats.ac.id/sntekpan/article/view/3445

[14] R. Firnanda *et al.*, "Sistem Pemilah Sampah Otomatis Berdasarkan Jenis Sampah Berbasis Microcontroller Arduino Uno," *Pros. Semin. Nas. Tek. Elektro Sist. Inf. Dan Tek. Inform. SNESTIK*, vol. 1, no. 1, pp. 7–15, May 2024, doi: 10.31284/p.snestik.2024.5724.

[15] M. Shofiyullah and S. Muharom, "Sistem Pengering Pakaian Otomatis Berbasis Microcontroller," *Pros. Semin. Nas. Tek. Elektro Sist. Inf. Dan Tek. Inform. SNESTIK*, vol. 1, no. 1, Art. no. 1, Apr. 2023, doi: 10.31284/p.snestik.2023.3978.

[16] A. Ramadhan, "Design and Build a Telegram – Based Infusion Droplet Control and Monitoring System | Procedia of Engineering and Life Science." Accessed: Jan. 27, 2023. [Online]. Available: https://pels.umsida.ac.id/index.php/PELS/article/view/1225

[17] T. Puasandi, "SISTEM AKSES KONTROL KUNCI ELEKTRIK MENGGUNAKAN PEMBACAAN E-KTP," p. 6, 2014.

[18] M. R. Muliawan, B. Irawan, and Y. Brianorman, "IMPLEMENTASI PENGENALAN WAJAH DENGAN METODE EIGENFACE PADA SISTEM ABSENSI," vol. 03, no. 1, p. 11, 2015.

[19] W. Sulaeman, E. Alimudin, and A. Sumardiono, "SISTEM PENGAMAN LOKER DENGAN MENGGUNAKAN DETEKSI WAJAH," *J. Energy Electr. Eng. JEEE*, vol. 3, no. 2, Art. no. 2, Apr. 2022, doi: 10.37058/jeee.v3i2.4756.

[20] "Rapid Object Detection using a Boosted Cascade of Simple Features." Accessed: Apr. 09, 2026. [Online]. Available: https://www.computer.org/csdl/proceedings-article/cvpr/2001/127210511/12OmNyXMQaN

[21] T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 2037–2041, Dec. 2006, doi: 10.1109/TPAMI.2006.244.

[22] Y. Putra, C. Prabowo, and E. Asri, "Keamanan Laci Berbasis Mikrokontroler dengan Sensor LDR dan RFID," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 3, Art. no. 3, Sep. 2020, doi: 10.30630/jitsi.1.3.15.