Journal of Computer Science and Frontier Technologies
ISSN Print: 3104-4204
ISSN Online: 3104-4212
CD ISSN: 3104-4220
https://doi.org/10.63313/JCSFT.9096

Design and Prototype Validation of an STM32-Based Access-Control System with Four Alternative Authentication Methods

Junpei Zhang
School of Electronic Engineering, Tianjin University of Technology and Education, Tianjin, China

How to cite this paper: Zhang, J. (2026). Design and Prototype Validation of an STM32-Based Access-Control System with Four Alternative Authentication Methods. Journal of Computer Science and Frontier Technologies, 4(1), 97–108. ISSN Print: 3104-4204, ISSN Online: 3104-4212.
https://doi.org/10.63313/JCSFT.9096
Published: 2026-08-12

Copyright © 2026 by author(s) and Erytis Publishing Limited.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Abstract

Access-control prototypes often depend on a single credential type, so a lost, forgotten, or temporarily unreadable credential can prevent legitimate entry. This paper presents an STM32F103C8T6-based prototype that provides four alternative authentication methods: fingerprint identification, RFID-card verification, keypad-password entry, and smartphone password entry through a JDY-31 Bluetooth serial link. The firmware routes all four inputs through a common decision and actuator path while retaining separate enrollment, revocation, and password-management procedures. A relay, LCD1602, and buzzer provide lock actuation and user feedback. We validated nominal enrollment, authentication, deletion, and rejection functions under laboratory conditions and then repeated each authentication method in 20 functional trials. Each method produced 20 observed successful operations; the reported mean response times were below 1 s for RFID, approximately 0.5 s for fingerprint identification, below 1 s for the keypad, and below 2 s for Bluetooth. These measurements establish function-level feasibility and response-time performance for the tested prototype, but they do not constitute a statistical estimate of biometric accuracy, long-term reliability, or resistance to attack. The resulting architecture is intended as a low-cost and extensible platform for residential, laboratory, and small-office access-control research.

Keywords

STM32; Physical Access Control; Alternative Authentication; Fingerprint Identification; RFID; Bluetooth SPP; Matrix Keypad

1. Introduction

Physical access-control systems must authorize legitimate users while maintaining acceptable response time and operational availability. Mechanical keys remain simple, but they can be lost or duplicated and provide no electronic credential-management or event-processing capability. Risk-based guidance for

physical access control therefore emphasizes matching the authentication mechanism to the protected asset and validating credentials rather than treating any token as intrinsically trustworthy [1]. Electronic locks extend this model by combining embedded controllers with cards, biometrics, passwords, and wireless interfaces [15,16].

The design space is broader than a simple choice of sensor. Kaul and Hatzinakos combined RFID, biometric, and mobile interfaces for a banking-oriented lock, illustrating how heterogeneous credentials can be coordinated around one actuator [2]. Simatupang and Tambunan evaluated fingerprint, RFID, and keypad inputs as a multi-sensor residential prototype [3], and Tambunan et al. added remote notification to a three-level arrangement [4]. Hermawan et al. instead required an RFID token and PIN as explicit multi-factor authentication for managed rooms [5]. Together, these studies show two recurring engineering goals: increasing credential diversity and choosing whether credentials operate in parallel, in sequence, or under a context-dependent policy. They also show that counting modules is not a security metric. A four-input system may be convenient but weak if one input accepts a replayable identifier or unprotected password; conversely, a two-factor system may be stronger but less tolerant of a lost factor. The present work therefore describes both the hardware integration and the policy semantics of the prototype.

Prior prototypes have combined RFID, fingerprint sensing, keypads, mobile devices, or network services in either layered or alternative authentication arrangements [2-5,23]. Conjunctive multi-factor designs can increase assurance by requiring two or more factors, whereas alternative-method designs emphasize availability by allowing several independently authorized paths [21]. The two concepts should not be conflated. This study adopts the second architecture: four methods feed a common access-decision path, and any one valid method can actuate the lock. We describe the hardware and firmware interfaces, validate the available functions, report method-specific response times, and define the security and experimental boundaries that must be addressed before deployment.

2. System Architecture and Component Selection

2.1. Functional Requirements and System Architecture

The prototype had to accept fingerprint, RFID-card, keypad, and Bluetooth credentials through independent input paths; maintain separate enrollment, revocation, and password-update functions; retain registered credentials after power loss; and drive a relay, LCD, and buzzer after each decision. The response-time target was on the order of seconds. A further design objective was graceful functional degradation: if one input module became unavailable, another configured method could still be used. This objective is architectural; the present experiments did not inject hardware faults or quantify availability.

The STM32F103C8T6 serves as the control core (Figure 1). The input layer contains

a 4 x 4 matrix keypad, an RC522 board built around the MFRC522 reader, an optical fingerprint module, and a JDY-31 Bluetooth serial module. These devices acquire a password, card identifier, fingerprint template match, or smartphone-supplied password, respectively. The control layer performs input acquisition, record lookup, credential comparison, and the final access decision. The output layer contains the relay driver for the lock actuator, the LCD1602 for status messages, and the buzzer for audible feedback. UART, SPI, and GPIO links keep the module interfaces separable while allowing the four paths to share one decision and actuator routine.

The access policy is implemented as an OR relation across enabled methods. Each driver converts its device-specific transaction into one of three normalized states: pending, rejected, or authenticated. Only the authenticated state can request relay actuation. Credential-management operations are kept outside this shared path and require entry into the relevant enrollment, deletion, or update mode. This separation prevents a partially received Bluetooth frame, an RFID anticollision event, or a keypad scan from being treated as a completed authorization. It also provides a practical extension point: a future policy layer can require combinations such as card plus PIN without rewriting the device drivers or actuator routine.

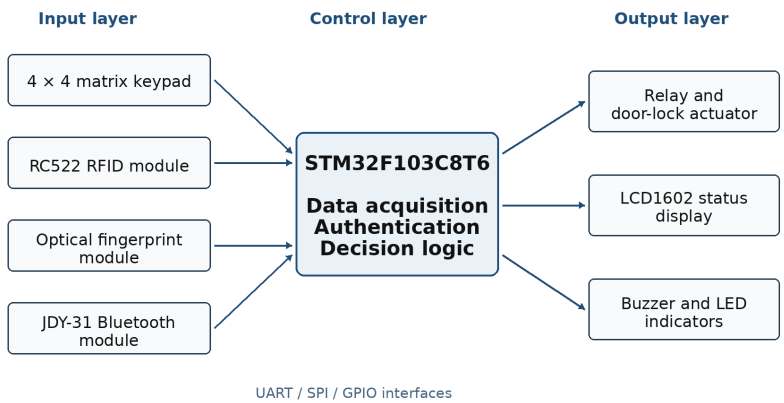


Figure 1. Layered architecture and shared decision path of the prototype.

2.2. Component Selection and Interface Rationale

The STM32F103C8T6 was selected because its 72 MHz Arm Cortex-M3 core, 64 KB Flash memory, 20 KB SRAM, 2.0-3.6 V supply range, and integrated USART, SPI, GPIO, timer, and nonvolatile-memory support are sufficient for the four input modules and three output devices [9]. The reset, clock, boot, and decoupling network follows the hardware-development guidance for STM32F10xxx devices [10]. The optical AS608/R308-series module performs template generation and 1:N search internally and exchanges commands over UART. The MFRC522 reader operates at 13.56 MHz, supports ISO/IEC 14443 Type A framing and anticollision, and communicates with the controller through SPI [11,12,24]. The JDY-31 is a Bluetooth 3.0 Serial Port Profile (SPP) slave module with a UART interface; it is not a

CC2541-based BLE 4.0 device [13,14]. Table 1 summarizes the resulting component roles.

Table 1. Principal components and interfaces.

Component	Model	Interface	Role
Microcontroller	STM32F103C8T6	-	Decision logic and peripheral control
Fingerprint module	AS608/R308 (optical)	UART	Template enrollment and 1:N local search
RFID reader	MFRC522 (RC522)	SPI	13.56 MHz card detection and identifier reading
Bluetooth module	JDY-31	UART	Bluetooth 3.0 SPP serial bridge
Display	LCD1602	8-bit parallel	Operating-state feedback

3. Hardware Implementation

3.1. Minimum Microcontroller System

The minimum system comprises the regulated supply, decoupling network, reset circuit, high-speed external clock, and boot configuration. An 8 MHz crystal and load capacitors provide the external clock source, and the phase-locked loop generates the 72 MHz system clock. NRST is held high through a pull-up network and can be pulled low manually. BOOT0 is tied low so that execution starts from main Flash memory. Supply-pin decoupling and the separation of 5 V actuator loads from the 3.3 V logic rail reduce conducted disturbances at the controller [9,10].

3.2. Matrix Keypad Interface

The 4 x 4 matrix provides 16 keys through eight GPIO lines. Rows connect to PA7, PA6, PA5, and PA4, and columns connect to PB0, PB1, PB10, and PB11 (Figure 2). The firmware drives one row low at a time while holding the remaining rows high and samples the column states. A pressed key pulls one column low, so the active row and detected column identify the key. Software debouncing and key-release detection prevent one physical press from being interpreted as multiple entries.

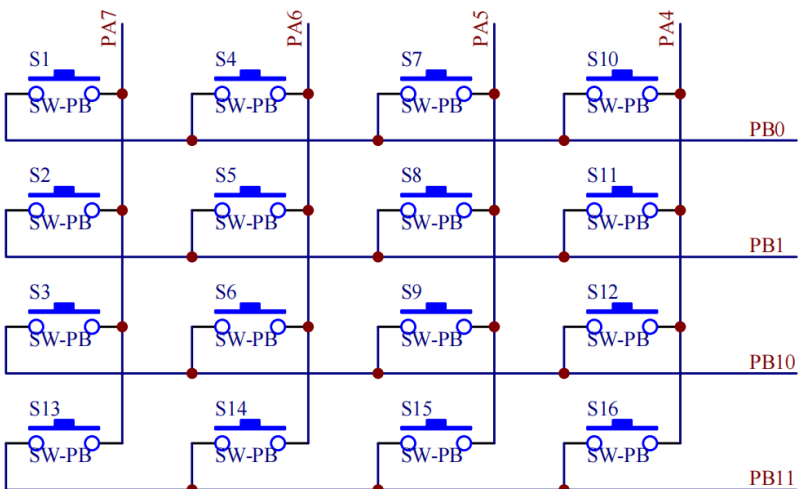


Figure 2. Simulated interface of the 4 x 4 matrix keypad.

3.3. RFID Reader Interface

The RC522 board communicates with the STM32 through SPI. In the tested wiring, SDA/SS, SCK, MOSI, and MISO connect to PA12, PA15, PB4, and PB3, while IRQ connects to PA0 (Figure 3). A regulated 3.3 V rail powers both the reader and the controller-side interface. The MFRC522 generates the 13.56 MHz field, detects a proximity card, executes initialization and anticollision, and returns the selected card data to the controller [11,12,16,24]. The prototype then compares the read identifier with locally stored records. This identifier-based implementation demonstrates access logic but does not by itself provide cryptographic card authentication [17].

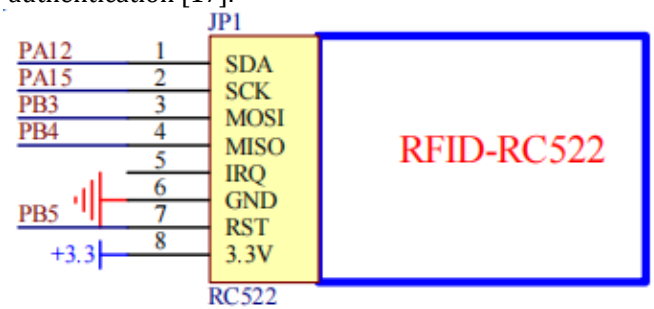


Figure 3. SPI interface of the RC522 RFID reader.

3.4. Relay Driver and Peripheral Circuits

The relay driver in Figure 4 separates the low-current microcontroller output from the lock actuator. PB6 drives PNP transistor Q1 through a current-limiting resistor. When Q1 conducts, the relay coil is energized and the normally open contact closes; when Q1 turns off, the contact releases. A flyback diode suppresses the coil's turn-off voltage, and an LED indicates the relay state. The LCD1602 uses an 8-bit parallel data bus and RS, RW, and E control lines. The firmware checks the LCD busy flag before each transfer to avoid writing while the controller is occupied.

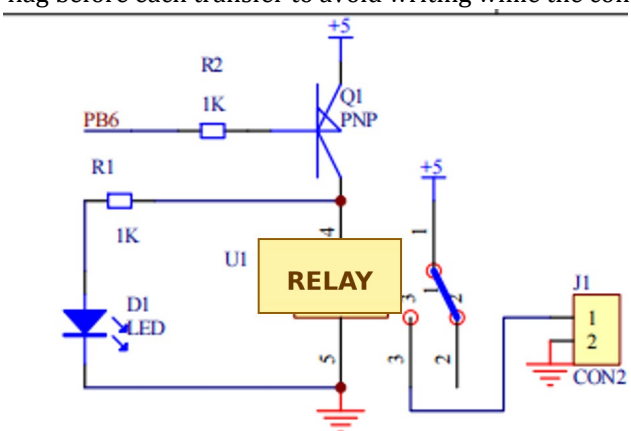


Figure 4. Simulated relay driver and flyback-protection circuit.

A center-positive DC input and latching switch feed the power tree. The 5 V branch supplies the relay and buzzer, while a low-dropout regulator generates 3.3 V for the

STM32 and communication modules. PB7 controls the buzzer and its indicator LED through an NPN low-side switch. Separating the actuator branch, limiting transistor base current, and placing local decoupling near digital devices reduce the probability that relay or buzzer transients disturb the logic supply.

4. Firmware Design

4.1. Main Program and Shared Decision Path

The firmware was developed in C using Keil MDK and organized as device drivers, authentication services, credential-management routines, and output-control functions. After reset, the program initializes the clock, GPIO, USART, SPI, timers, LCD, and stored records before entering the main loop. Timer-driven tasks scan the keypad and refresh time-dependent states; USART interrupts receive fingerprint-module and Bluetooth frames; and the main loop evaluates completed transactions. A valid result from any enabled method calls the same access-granted routine, which energizes the relay for the configured interval, updates the LCD, and sounds the buzzer. An invalid or incomplete transaction leaves the lock closed and returns a method-specific message.

The main loop can be viewed as a cooperative state machine. Device drivers acquire data asynchronously, but they publish a completed event only after their local protocol has terminated. The decision service then checks whether the event belongs to normal authentication or to an administrator-selected credential-management mode. After an unlock event, the actuator routine suppresses additional requests until the relay interval completes and the system returns to its idle prompt. Error paths clear temporary input buffers before accepting another transaction. This organization limits coupling among modules: adding or disabling one method changes event production but not the lock-control sequence. It also makes black-box testing observable because the same LCD, buzzer, and relay outputs correspond to the same decision state regardless of the input method.

4.2. Authentication and Credential-Management Routines

(1) Keypad password. The prototype uses separate configurable six-digit user and administrator codes. The administrator path opens the password-update routine, and the new value is committed only after two identical entries. The password is retained in nonvolatile memory. After a configured number of consecutive failures, the keypad is temporarily locked and the buzzer is activated. A production implementation should replace fixed initial credentials, protect stored verifiers, and define recovery and rate-limiting policies consistent with the intended assurance level [6,22].

(2) RFID card. The firmware performs card detection, anticollision, selection, and identifier reading through the MFRC522. Enrollment stores the selected identifier in

the local record table; authentication compares a newly read identifier with that table; and revocation removes a selected record. A match calls the common unlock routine, whereas an unknown or deleted identifier is rejected.

(3) Fingerprint. The controller uses the module's serial command set for image acquisition, feature extraction, template generation, storage, search, and deletion. Enrollment requires repeated placement so that the module can build a template. During authentication, the module performs a 1:N search against its internal template library and returns the result to the STM32 [15]. The controller unlocks only after a successful response; a selected template or the complete database can be removed through the administrator path.

(4) Bluetooth password. The JDY-31 provides a Bluetooth 3.0 SPP serial bridge between an Android device and the STM32 [13,14]. The controller parses a frame containing a header, payload length, password field, and check field. A valid password calls the common unlock routine; incomplete or inconsistent frames are discarded after a timeout. This transport supports convenient prototype control, but SPP pairing and a plaintext application password are not equivalent to an authenticated application protocol; Bluetooth deployments require explicit configuration, pairing, service, and application-layer security controls [7,18,19].

4.3. LCD Control Routine

The LCD1602 routine initializes the display mode, waits for the controller to become ready, checks the busy flag (BF), selects the display RAM address, and writes each character (Figure 5). If BF is nonzero, the routine repeats the readiness check rather than issuing an overlapping command. The routine continues until the complete status message has been written. This sequence makes display updates deterministic and prevents the UI from becoming a source of ambiguous test outcomes.

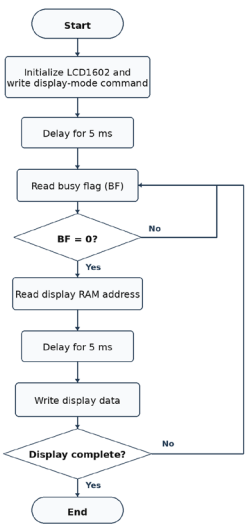


Figure 5. Control sequence used for LCD1602 status updates.

5. Prototype Validation

5.1. Test Platform and Acceptance Criteria

The laboratory platform comprised an STM32F103C8T6 development board, AS608/R308-series fingerprint module, RC522 reader, 4 x 4 keypad, JDY-31 module, LCD1602, relay driver, buzzer, lock-load indicator, and 5 V supply (Figure 6). Black-box test cases covered valid and invalid credentials, enrollment, revocation or deletion, password update, LCD feedback, and relay actuation. A trial was counted as successful only when the input was accepted by the intended method, the LCD displayed the expected state, and the relay produced the expected lock command. The source records did not include raw timing traces or repeated environmental conditions, so the analysis reports the recorded aggregate values without additional statistical inference.

The validation sequence first established the preconditions for each method: stored user code for the keypad, enrolled card identifier for RFID, enrolled template for fingerprint identification, and an established Bluetooth serial connection. Positive cases then exercised the configured credential, whereas negative cases used an unknown, deleted, or incorrect credential as applicable. Enrollment and deletion were tested before the repeated-trial phase so that the trial outcome reflected the normal authentication path rather than setup activity. Response time was defined by the original prototype records as the interval from credential presentation or completed password entry to the visible access decision. Because only the summarized values were available, this paper does not reconstruct distributions, standard deviations, or confidence intervals.

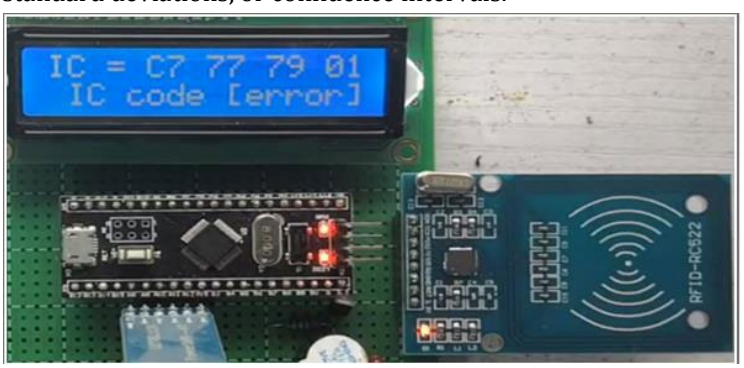


Figure 6. Physical prototype used for laboratory validation.

5.2. Functional and Response-Time Results

The RFID tests rejected an unregistered card, accepted it after enrollment, and rejected it again after revocation. The fingerprint path accepted an enrolled template and rejected the same identity after template deletion. The Bluetooth path discovered and paired with the JDY-31 and unlocked only after the smartphone sent the configured password. The keypad path accepted the configured user code, opened the password-update procedure through the administrator path, and

activated the audible feedback after verification. These cases confirmed that each input path reached the common decision and actuator logic while preserving its own credential-management operations.

Each authentication method was then exercised in 20 repeated functional trials (Table 2). The observed result was 20 successful operations in 20 trials for every method. The reported mean response times were below 1 s for RFID, approximately 0.5 s for fingerprint identification, below 1 s for the keypad, and below 2 s for Bluetooth. These values satisfy the prototype's seconds-scale response target. Because the trial count was small and only aggregate outcomes were retained, 20/20 should be interpreted as the outcome of this test set rather than as proof of a 100% population success probability or long-term reliability.

Table 2. Observed functional outcomes and reported response times.

Authentication Method	Trials	Observed Successful Operations	Observed Proportion	Reported Mean Response Time
RFID card	20	20	100%	< 1 s
Fingerprint	20	20	100%	approx. 0.5 s
Keypad password	20	20	100%	< 1 s
Bluetooth	20	20	100%	< 2 s

6. Discussion and Limitations

The main contribution is the coordination of four alternative input paths through one embedded decision and actuator layer. Related prototypes often combine two or three technologies or require sequential factors [2-5]. In contrast, the present design uses alternative authorization: any configured method can complete the transaction independently. This arrangement can preserve legitimate access when a particular credential is unavailable, but it does not increase authentication assurance in the same way as multi-factor authentication. The overall assurance is bounded by the weakest enabled path.

The security boundary is more restrictive than the functional results. The current RFID path compares card identifiers and therefore does not demonstrate cryptographic card validation; risk-based physical access guidance favors credential validation matched to the protected asset [1,17]. The Bluetooth path uses SPP and a password carried by the application frame. NIST guidance identifies configuration, pairing, service exposure, and link protection as separate concerns, so a production version should add device binding, mutual challenge-response, replay protection, encrypted application messages, and protected credential storage [6,7]. The MFRC522 remains adequate for reproducing the prototype, but NXP now marks the device as end-of-life and not recommended for new designs; a supported reader front end should be selected for a product revision [11].

The experimental boundary is equally important. Twenty repeated positive trials per method are sufficient to detect obvious logic or interface failures, but they

cannot estimate rare failure rates. The fingerprint experiment did not report false-match rate, false-non-match rate, score distributions, presentation-attack testing, or demographic and environmental coverage required for a biometric performance study [8,15,20]. The work also did not measure current consumption, electromagnetic compatibility, long-duration operation, partial-module fault recovery, relay endurance, or behavior under power interruption. Future evaluation should retain raw event timestamps, predefine positive and negative test sets, report uncertainty intervals, and include temperature, supply variation, communication interference, and fault-injection conditions.

These limitations define an appropriate use case: the present system is a research and teaching prototype for low-cost multi-method access control, not a certified high-assurance lock. Its modular interfaces make the next experiments straightforward. The firmware can expose a policy layer that switches between alternative-method mode for convenience and conjunctive multi-factor mode for higher-risk spaces [21]; the same layer can log decisions and enforce credential-specific rate limits. Such extensions would convert the current functional redundancy into a measurable security and availability study.

Credential lifecycle management also requires more than enrollment and deletion buttons. A deployable system should assign unique initial credentials, separate user and administrator roles, protect nonvolatile records against readout and rollback, log security-relevant events, and define procedures for lost cards, compromised passwords, and biometric-template replacement. NIST authentication guidance treats issuance, binding, invalidation, recovery, and reauthentication as parts of the same lifecycle [6,22]. Although that guidance targets digital services, the lifecycle principle applies directly to an embedded lock: a credential remains trustworthy only while its ownership, validity, and revocation state are controlled. The current prototype demonstrates the control hooks for this lifecycle but not the secure implementation of those controls.

7. Conclusion

This paper presented and functionally validated an STM32F103C8T6-based access-control prototype with four alternative authentication methods. Fingerprint, RFID, keypad, and Bluetooth inputs share a common access-decision and relay-control path while retaining separate enrollment and credential-management routines. In the reported laboratory tests, each method produced 20 observed successful operations in 20 trials, with reported mean response times ranging from approximately 0.5 s to below 2 s. The results support the feasibility of the architecture and its seconds-scale responsiveness; they do not establish attack resistance, biometric error rates, or field reliability. The next engineering step is therefore not to add more input methods, but to strengthen each credential path through protected storage, cryptographic card validation, authenticated Bluetooth

messaging, configurable factor policies, and a larger validation protocol with environmental, fault-injection, and security tests.

References

[1] H. Ferraiolo, K. Mehta, N. Ghadiali, J. Mohler, V. Johnson, and S. Brady, Guidelines for the Use of PIV Credentials in Facility Access, NIST Special Publication 800-116 Rev. 1, 2018. https://doi.org/10.6028/NIST.SP.800-116r1

[2] S. D. Kaul and D. Hatzinakos, "Intelligent RFID biometric enabled dual security lock in the banking environment," Journal of Banking and Financial Technology, vol. 4, no. 2, pp. 159-173, 2020. https://doi.org/10.1007/s42786-020-00022-1

[3] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," in 2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), pp. 453-457, 2022. https://doi.org/10.1109/GECOST55694.2022.10010367

[4] R. W. Tambunan, A. A. Ar-Rafif, and M. Galina, "Multi-Security System Based on RFID Fingerprint and Keypad to Access the Door," ELKHA: Jurnal Teknik Elektro, vol. 14, no. 2, 2022. https://doi.org/10.26418/elkha.v14i2.57735

[5] I. Hermawan, D. Arnaldy, P. Oktivasari, D. A. Fachrudin, R. Nuraini, and N. T. Sulthanah, "Development of Intelligent Door Lock System for Room Management Using Multi Factor Authentication," Jurnal Teknik Informatika, vol. 16, no. 1, pp. 1-14, 2023. https://doi.org/10.15408/jti.v16i1.29045

[6] D. Temoshok, J. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. Richer, Digital Identity Guidelines: Authentication and Authenticator Management, NIST Special Publication 800-63B-4, 2025. https://doi.org/10.6028/NIST.SP.800-63b-4

[7] J. Padgette, J. Bahr, M. Batra, R. Smithbey, L. Chen, and K. Scarfone, Guide to Bluetooth Security, NIST Special Publication 800-121 Rev. 2 Update 1, 2022. https://doi.org/10.6028/NIST.SP.800-121r2-upd1

[8] ISO/IEC 19795-1:2021, Information technology - Biometric performance testing and reporting - Part 1: Principles and framework, 2nd ed., 2021. https://www.iso.org/standard/73515.html

[9] STMicroelectronics, STM32F103x8/STM32F103xB: Medium-density performance line Arm-based 32-bit MCU, DS5319 Rev. 20, 2025. https://www.st.com/resource/en/datasheet/stm32f103rb.pdf

[10] STMicroelectronics, Getting started with STM32F10xxx hardware development, Application Note AN2586 Rev. 8, 2022. https://www.st.com/resource/en/application_note/an2586-getting-started-with-stm32f10xxx-hardware-development-stmicroelectronics.pdf

[11] NXP Semiconductors, MFRC522: Standard performance MIFARE and NTAG frontend, Product Data Sheet Rev. 3.9, 2016. https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

[12] ISO/IEC 14443-3:2018, Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision, 4th ed., 2018. https://www.iso.org/standard/73598.html

[13] Bluetooth SIG, Serial Port Profile, Version 1.2, adopted July 24, 2012. https://www.bluetooth.com/specifications/specs/serial-port-profile-1-2/

[14] JDY-31 Bluetooth Module User Manual, firmware series JDY-31-V1.2, 2019. https://myosuploads3.banggood.com/products/20190129/20190129043725SKUA87502.pdf

[15] JAIN A K, ROSS A, PRABHAKAR S. An introduction to biometric recognition [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 4-20. DOI: 10.1109/TCSVT.2003.818349.

[16] WANT R. An introduction to RFID technology [J]. IEEE Pervasive Computing, 2006, 5(1):

25-33. DOI: 10.1109/MPRV.2006.2.

[17] JUELS A. RFID security and privacy: A research survey [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 381-394. DOI: 10.1109/JSAC.2005.861395.

[18] PADGETTE J, BAHR J, BATRA M, et al. Guide to Bluetooth Security [R]. Gaithersburg, MD: National Institute of Standards and Technology, 2017. NIST Special Publication 800-121 Revision 2. DOI: 10.6028/NIST.SP.800-121r2.

[19] RYAN M. Bluetooth: With Low Energy Comes Low Security [C]//7th USENIX Workshop on Offensive Technologies (WOOT 13). Washington, D.C.: USENIX Association, 2013.

[20] RATHA N K, CONNELL J H, BOLLE R M. Enhancing security and privacy in biometrics-based authentication systems [J]. IBM Systems Journal, 2001, 40(3): 614-634. DOI: 10.1147/sj.403.0614.

[21] ROSS A, JAIN A K. Information fusion in biometrics [J]. Pattern Recognition Letters, 2003, 24(13): 2115-2125. DOI: 10.1016/S0167-8655(03)00079-5.

[22] TEMOSHOK D, FENTON J, CHOONG Y Y, et al. Digital Identity Guidelines: Authentication and Authenticator Management [R]. Gaithersburg, MD: National Institute of Standards and Technology, 2025. NIST Special Publication 800-63B-4. DOI: 10.6028/NIST.SP.800-63b-4.

[23] AL-FUQAHA A, GUIZANI M, MOHAMMADI M, et al. Internet of Things: A survey on enabling technologies, protocols, and applications [J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2347-2376. DOI: 10.1109/COMST.2015.2444095.

[24] NXP SEMICONDUCTORS. MFRC522: Standard performance MIFARE and NTAG frontend [R]. Rev. 3.9, 2016.