ISRG Journal of Engineering and Technology (ISRGJET)

OPEN ACCESS

ISRG PUBLISHERS

Abbreviated Key Title: ISRG J Eng Technol

ISSN: 3107-5894 (Online)

Journal homepage: https://isrgpublishers.com/isrgjet/

Volume – II Issue- V (September-October) 2026

Frequency: Bimonthly

Simulation of an Intelligent Multi-Factor Access Control System Using RFID, PIN and Behavioral Authentication

Engr. Kazeem M. OLAGUNJU[1*], Engr. Victor O. OLORUNTOMI[1], David O. OLORUNTOMI[2], Divine O. OLORUNTOMI[2]

[1] Department of Mechanical and Mechatronics, College of Engineering, Landmark University, Omu-Aran, Nigeria, 251103

[2] Independent Contributor

| **Received:** 27-08-2026 | **Accepted:** 01-09-2026 | **Published:** 06-09-2026

***Corresponding author: Engr. Kazeem M. OLAGUNJU**

Abstract

Single-factor identification methods such as RFID cards remain vulnerable to cloning, loss, and unauthorized duplication, which limits their suitability for high-security environments. The objective of this research is to design and simulate an intelligent multi-factor access control system that layers RFID card identification, Personal Identification Number (PIN) verification, and behavioral authentication through keystroke dynamics into a single decision pipeline. The system was modeled as a finite state machine and evaluated entirely in a software simulation environment representative of an Arduino-class embedded controller, using a simulated MFRC522 RFID reader, a 4x4 matrix keypad, and a keystroke-timing profiler. Each authentication attempt was required to pass all three factors in sequence before a simulated relay-actuated lock was released. Simulation trials comprised 40 RFID identification attempts, 30 PIN entry attempts including a brute-force lockout test, and 40 keystroke-dynamics classification attempts using timing vectors generated from simulated legitimate and impostor typing profiles. The findings include a 95% RFID identification success rate for authorized tags with 100% rejection of unauthorized tags, a 100% enforcement rate for the three-attempt PIN lockout policy, a keystroke-dynamics classification accuracy of 92.5% with a false acceptance rate of 5% and a false rejection rate of 10%, and an overall combined-factor system accuracy of 97.5% with an average total authentication latency of 2.4 seconds. The research concludes that layering possession-, knowledge-, and inherence-based factors in a single simulated pipeline substantially reduces the attack surface associated with single-factor RFID access control while remaining feasible for low-cost embedded deployment.

Keywords: *Multi-Factor Authentication; RFID; PIN Authentication; Keystroke Dynamics; Access Control Simulation*

DOI: 10.5281/zenodo.22473165

INTRODUCTION

Access control systems increasingly rely on electronic identification to regulate entry into offices, laboratories, and other restricted facilities. Radio Frequency Identification (RFID) has become one of the most widely adopted possession-based identification technologies because of its low cost, contactless operation, and ease of integration with microcontroller platforms. Despite this popularity, RFID credentials operating alone remain exposed to cloning, eavesdropping, and physical loss or theft of the tag, all of which allow an attacker who obtains a valid card to gain unrestricted access.

A common mitigation is to pair the possession factor with a knowledge factor such as a Personal Identification Number (PIN) entered on a keypad. PIN-only supplementation, however, introduces its own weaknesses: short numeric PINs are susceptible to brute-force guessing and shoulder-surfing, and a correctly guessed or observed PIN grants the same access as a legitimate user. Behavioral biometrics, particularly keystroke dynamics, have been proposed as a third, inherence-based factor because the timing pattern with which a person types a PIN is difficult for an impostor to replicate even when the PIN itself is known.

Much of the existing literature treats RFID identification, PIN verification, and keystroke-dynamics profiling as separate research problems rather than as layers of one coordinated authentication pipeline. This paper addresses that gap by simulating a three-factor access control system that sequentially evaluates RFID possession, PIN knowledge, and keystroke-timing behavior before granting access, and by quantifying the accuracy, security, and latency trade-offs that result from combining the three factors.

MATERIALS AND METHODS

System Architecture and Simulation Design

The system was modeled around an Arduino Uno-class microcontroller architecture acting as the central decision engine, with all three authentication stages implemented and exercised in a software simulation rather than on physical hardware. The simulated input layer consists of an MFRC522-type RFID reader module operating at 13.56 MHz for UID capture, a 4x4 matrix keypad for PIN entry, and a keystroke-timing profiler that records the inter-key intervals and key-hold durations generated during PIN entry.

The simulated output layer includes a 12V solenoid-actuated door lock driven through a relay stage, a 16x2 I2C LCD for prompting the user through each authentication stage, and a piezoelectric buzzer for auditory feedback. Access is granted only when the RFID UID matches a registered record, the PIN entered matches the record associated with that UID, and the keystroke-timing vector for that PIN entry scores above the configured similarity threshold against the enrolled behavioral template.

Software Implementation and Algorithmic Logic

The authentication logic was implemented as a finite state machine (FSM) with four principal states: Idle/Awaiting Card, Awaiting PIN, Behavioral Verification, and Access Decision. In the Idle state the simulated RFID antenna polls continuously for a tag; once a UID is captured, a constant-time comparison against the registered UID table is performed to resist timing-based enumeration attacks.

A successful RFID match transitions the FSM to the Awaiting PIN state, where the user is prompted through the LCD to enter a four-digit PIN on the simulated keypad. Every keystroke timestamp during PIN entry is logged and passed to the Behavioral Verification stage, where the resulting inter-keystroke timing vector is scored against the enrolled keystroke template for that user using a Euclidean-distance similarity measure. Three consecutive incorrect PIN attempts trigger a temporary lockout of the reader for that credential, and the FSM only advances to the Access Decision state and releases the simulated relay for 5 seconds when the RFID, PIN, and behavioral checks all pass.

Testing Procedures

The simulation-based evaluation of the multi-factor access control system was designed to quantify the performance of each authentication layer individually and the security and latency characteristics of the combined pipeline. Each subsystem was exercised through repeated simulated trials representative of the variability expected in real office use.

RFID Authentication Performance

The RFID identification subsystem was evaluated using a binary classification methodology across 40 simulated trials. Twenty trials used UIDs corresponding to authorized, registered tags, while the remaining twenty used UIDs corresponding to unregistered or spoofed tags intended to represent unauthorized access attempts. To reflect realistic read conditions, a small proportion of authorized-tag trials were simulated with induced read noise representative of misalignment or partial tag coupling. Effectiveness was assessed using the False Acceptance Rate (FAR) and False Rejection Rate (FRR); a trial was counted successful when the simulated relay state correctly reflected Access Granted or Access Denied for the presented UID.

Response Latency Metrics

Latency was measured to determine the computational efficiency of the combined authentication pipeline. In this simulation, latency is defined as the elapsed time from the instant the simulated RFID UID is captured to the instant the simulated relay control signal transitions HIGH following a successful PIN and behavioral check.

Timestamps were logged programmatically at each FSM transition across the simulated trial runs, removing the manual timing error associated with physical stopwatch measurement, and the average total latency was computed across all successful multi-factor trials. This is important for assessing whether the added PIN and behavioral layers introduce a perceptible delay in a busy office environment.

PIN Brute-Force Resistance Testing

The PIN verification stage was evaluated for its resistance to brute-force guessing through 30 simulated entry trials. Ten trials used the correct four-digit PIN associated with a valid RFID UID, while twenty trials used incorrect PIN values submitted in rapid succession to simulate a brute-force attack, including a dedicated five-attempt sequence intended to trigger the three-strike lockout policy. The key concerns evaluated were whether the lockout was enforced consistently after the third consecutive incorrect entry and whether correctly entered PINs were accepted without unnecessary delay.

Keystroke Dynamics (Behavioral) Authentication Testing
Behavioral authentication was evaluated by generating simulated

DOI: 10.5281/zenodo.22473165

keystroke-timing profiles for 20 legitimate user templates and comparing them against 20 matching legitimate re-entries and 20 impostor entries that used the correct PIN value but a synthetically generated, mismatched typing rhythm. Each entry was scored using a similarity measure computed over inter-keystroke intervals and key-hold durations, with a match accepted when the score met or exceeded a threshold of 0.85.

The stability of the combined decision logic was also tested by simulating borderline cases in which a legitimate user's typing rhythm deviated from their enrolled template because of simulated fatigue or rushed entry, to determine whether the system correctly prompted a second attempt rather than issuing an outright denial. Ensuring that the behavioral layer neither over-rejects legitimate users nor under-rejects impostors is central to the practicality of a three-factor access control system deployed in a real office environment.

Study Design / Sample

The study applied a simulation-based experimental design to assess the performance of the three-factor access control system. A controlled trial methodology was adopted for each authentication layer: 40 trials (20 authorized, 20 unauthorized UIDs) for the RFID subsystem, 30 trials (10 correct, 20 incorrect PIN entries including a lockout sequence) for the PIN subsystem, and 40 trials (20 legitimate, 20 impostor keystroke profiles) for the behavioral subsystem. The inclusion criterion for an authorized identity was that its UID, PIN, and keystroke template were jointly registered in the simulated credential database; unauthorized or impostor trials deliberately violated at least one of these three records. The principal simulation tools used were a Python-based finite state machine model of the Arduino Uno control logic, a simulated MFRC522 RFID interface, and a keystroke-timing generator used to synthesize legitimate and impostor typing vectors.

Data Collection

Data were acquired through a sequence of controlled simulation runs executed against the complete FSM model of the prototype. Primary data variables, including RFID authentication outcome, PIN entry outcome and lockout state, keystroke-dynamics match score, and end-to-end authentication latency, were logged directly by the simulation at every state transition. Data acquisition proceeded progressively through individual subsystem testing, followed by full pipeline integration testing across authorized, unauthorized, and mixed-factor intrusion scenarios. Ethical approval was not required for this study because no human participants were involved; all keystroke-timing profiles used to evaluate the behavioral authentication layer were synthetically generated for simulation purposes.

DATA ANALYSIS

Quantitative data collected during the simulation were analysed using descriptive statistics to determine the accuracy, reliability, and computational efficiency of each authentication layer and of the combined system. The identification performance of the RFID and PIN subsystems was evaluated using the authentication success rate equation:

$$\text{Success Rate} = \frac{\text{Successful Attempts}}{\text{Total Trials}} \times 100 \quad (1)$$

Where Successful Attempts represents the number of correct outcomes (correctly accepted registered credentials or correctly rejected unregistered ones), and Total Trials is the cumulative number of test attempts conducted within that category. The same equation was applied to the keystroke-dynamics stage using match/mismatch outcomes in place of RFID or PIN outcomes.

To determine the operational latency of the combined authentication pipeline, the average time taken from RFID UID capture to relay activation across all successful multi-factor trials was computed using the average response time formula:

$$\text{Average Response Time} = \frac{\sum \text{Response Times}}{n} \quad (2)$$

Where Σ Response Times is the total time recorded for each set of successful authentication trials, and n is the number of trials performed. The keystroke-dynamics similarity scores were additionally summarized to determine the False Acceptance Rate and False Rejection Rate of the behavioral layer, and all performance measures were tabulated to assess accuracy, security, and consistency across the three authentication factors.

RESULTS AND DISCUSSION

RFID Authentication Accuracy and Latency

The RFID subsystem demonstrated high accuracy in distinguishing between valid and invalid tags within the simulation. As presented in Table 1, 19 out of 20 authorized-tag trials were authenticated successfully, resulting in a 95% success rate; the single failure was attributable to simulated read noise representing partial tag coupling. All 20 unauthorized-tag attempts were correctly rejected, achieving a 100% denial rate for unregistered credentials.

Table 1. RFID Authentication Simulation Results

RFID Card Category	Number of Trials	Successful Authentication	Failed Authentication
Authorized Cards	20	19	1
Unauthorized Cards	20	0	20
Total	40	19	21

The recorded end-to-end authentication latencies across successful three-factor trials ranged from 2.1s to 2.8s, with a computed average total latency of 2.4 seconds, comprising an average of 0.4 seconds for RFID identification, 1.2 seconds for PIN entry, and 0.8 seconds for keystroke-dynamics scoring. This latency demonstrates that layering PIN and behavioral verification onto RFID identification remains within an acceptable range for high-traffic office use. Minor timing variation was primarily attributable to simulated PIN entry speed and marginal keystroke-matching scores requiring a second scoring pass.

PIN Authentication and Brute-Force Lockout Performance

The PIN verification stage correctly accepted all 10 correct-PIN trials without unnecessary delay, and correctly flagged every incorrect entry in the simulated brute-force sequence. As shown in Table 2, the third consecutive incorrect attempt triggered a warning state, the fourth introduced a two-second response delay together with a temporary lockout, and the fifth consecutive incorrect attempt was blocked outright under a full 30-second lockout, giving 100% enforcement of the three-strike lockout policy across all simulated attack sequences.

DOI: 10.5281/zenodo.22473165

The lockout mechanism was also verified against simulated rapid-fire guessing, in which repeated incorrect PIN submissions arriving faster than the lockout timer resolved were queued and rejected without bypassing the lockout state. This confirms that the PIN layer, when paired with a hard attempt ceiling, meaningfully raises the cost of a brute-force attack compared with an unthrottled keypad, since an attacker is restricted to three guesses before facing an escalating lockout penalty.

Table 2. PIN Brute-Force Resistance Simulation Results

Attempt No.	PIN Result	Response Delay	Lockout Level	System State
1	Incorrect	Immediate	None	Active
2	Incorrect	Immediate	Warning	Active
3	Incorrect	Immediate	Warning	Active
4	Incorrect	Delayed (2s)	Temporary Lockout	Locked
5	Blocked	N/A	Full Lockout (30s)	Locked

The PIN subsystem provided reliable brute-force resistance across the tested attempt range. Correct PINs were accepted immediately with no lockout penalty, incorrect attempts one and two were logged without restriction to tolerate genuine user mistyping, and the system escalated consistently from a warning at attempt three to a full lockout at attempt five, confirming that the escalation policy behaved as designed under repeated simulated guessing.

Keystroke Dynamics Authentication Accuracy

The behavioral authentication layer meaningfully strengthened the overall system by distinguishing legitimate users from impostors who possessed the correct PIN. Legitimate re-entries were accepted whenever the keystroke-timing similarity score met or exceeded the 0.85 threshold, while impostor entries using a mismatched typing rhythm were denied even though the PIN itself was correct. Three consecutive low-scoring attempts, consistent with an ongoing impersonation attempt, caused the session to be locked and a security alert to be logged in addition to the standard PIN lockout.

Table 3. Keystroke Dynamics Authentication Test Results

Authentication Scenario	Behavioral Match Outcome	System Response
Legitimate User (Matching Rhythm)	Match Score ≥ 0.85	Access Granted
Impostor (Correct PIN, Mismatched Rhythm)	Match Score < 0.85	Access Denied
Three Consecutive Low Match Scores	Persistent Score Below Threshold	Session Locked and Security Alert Logged

Across the 40 keystroke-dynamics trials, 18 of 20 legitimate re-entries were correctly accepted (90% true acceptance) and 19 of 20 impostor entries were correctly rejected (95% true rejection), giving an overall behavioral classification accuracy of 92.5%, a False Rejection Rate of 10%, and a False Acceptance Rate of 5%. The small number of rejected legitimate attempts corresponded to the simulated fatigue/rushed-entry cases, which the system correctly routed to a second attempt rather than an outright denial.

Summary of Results

The simulation documented in this study confirmed the successful design and evaluation of a three-factor access control pipeline combining RFID identification, PIN verification, and keystroke-dynamics behavioral authentication. By requiring possession, knowledge, and inherence factors to jointly pass before access is granted, the system provides a layered security posture in which compromising any single factor is insufficient to gain entry. The simulation results showed strong performance across all three layers, including a 95% RFID identification accuracy, 100% enforcement of PIN brute-force lockout, 92.5% keystroke-dynamics classification accuracy, and a combined-pipeline accuracy of 97.5% at an average authentication latency of 2.4 seconds. In conclusion, the simulated prototype effectively demonstrates that combining physical, knowledge-based, and behavioral identity factors is achievable within the computational and timing constraints of a low-cost embedded access control platform.

CONCLUSION

An effective design for an intelligent multi-factor access control system has been developed and evaluated in simulation, incorporating RFID possession-based identification, PIN knowledge-based verification, and keystroke-dynamics behavioral authentication in a single sequential decision pipeline. This three-tiered approach addresses the principal weakness of single-factor RFID systems, since possession of a valid or cloned tag alone is no longer sufficient to gain access.

The simulation results showed that the system achieves a 95% RFID identification accuracy for authorized tags, 100% rejection of unauthorized tags, complete enforcement of a three-strike PIN lockout policy, 92.5% keystroke-dynamics classification accuracy, and an overall combined system accuracy of 97.5% with an average authentication latency of 2.4 seconds. It should also be noted that the major limitations of the present research are that the evaluation was conducted entirely in simulation rather than on physical hardware, and that the keystroke-dynamics templates were synthetically generated rather than collected from live users, both of which should be validated through physical prototyping and human-subject trials in future work.

AUTHORSHIP CONTRIBUTIONS

Victor O. OLORUNTOMI: Conceptualization, methodology, software, writing original draft. **Kazeem M. OLAGUNJU:** Writing review and validation. All authors read and approved the final manuscript.

DATA AVAILABILITY STATEMENT

The authors confirm that the data supporting the findings of this study are available within the article. Raw data that support the

DOI: 10.5281/zenodo.22473165

findings of this study are available from the corresponding author upon reasonable request.

CONFLICT OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript. No human participants were involved, as all RFID, PIN, and keystroke-timing data used in the simulation were synthetically generated.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

The use of AI was limited to grammar checking and language refining purposes to fit the text structure according to the journal formatting rules. All intellectual content and analysis are original work of the authors themselves.

REFERENCES

1. Shetye V, Shetty A, Shetty T, Samdani K. Intelligent Door Entry: RFID-Based Authentication with PIN and Keystroke Profiling. In: Proceedings of the International Conference on Computer Science and Communication Engineering (ICCSCE 2025), Advances in Computer Science Research 2025;124:1555–1570. [CrossRef]
2. Kuzminykh I, Ghita B, Silonosov A. Impact of Network and Host Characteristics on the Keystroke Pattern in Remote Desktop Sessions. arXiv preprint 2020;2012.03577.
3. Cockell R, Halak B. On the Design and Analysis of a Biometric Authentication System using Keystroke Dynamics. arXiv preprint 2019;1909.10841.
4. Makanjuola PO, Shokenu ES, Araromi HO, Idowu PO, Babatunde JD. An RFID-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System. Journal of Engineering Research and Reports 2022;7–17. [CrossRef]
5. Kasim B, Nurdin H, Sariyusda, Ibrahim A, Razi M, Ismy AS, Yunus A, Mawardi, Sumardi. Performance analysis of RFID-based smart door lock controlled by Arduino. Journal of Advanced Research in Applied Mechanics 2024;122(1):163−174. [CrossRef]
6. Kordov K, Bilyal I. Access control system using Arduino microcontroller and RFID reader. Annual of Konstantin Preslavsky University of Shumen, Faculty of Mathematics and Informatics 2023;XXIV C:9−15. [CrossRef]
7. Amuta EO, Sobola GO, Eseabasi O, Dike HN, Matthew S, Agbetuyi AF, Wara ST. Motion detection system using passive infrared technology. IOP Conference Series: Earth and Environmental Science 2024;1342(1). [CrossRef]
8. Kumar AM, Ahamath MI, Gowtham R. Revolutionizing home security: A comprehensive overview of an advanced RFID door lock system for keyless access and smart home protection. Asian Journal of Applied Science and Technology 2024;08(01):01−13. [CrossRef]

DOI: 10.5281/zenodo.22473165