

Multi-Factor Access Control Authentication using Fingerprint-Fused Radio Frequency Identification Card

^{*1}Isah Olawale Mustapha, ¹Abdullateef Adekunle Olorukooba, ¹Adama Asmau Sani,
²Seriki Aliu Adebayo, ³Sefinat Bola Jaiyeola and ³Ibrahim S. A.

¹Department of Computer Science. Faculty of Computing, Engineering and Technology, Alhikmah University, Ilorin, Kwara State, Nigeria.

²Department of Cyber Security, Abdulrasaq Abubakar Toyin University, Ganmo, Kwara State, Nigeria.

³Department of Physical Science, Al-Hikmah University, Ilorin, Kwara State, Nigeria.

*Corresponding authors' email: salnet2002@alhikmah.edu.ng

ABSTRACT

Traditional authentication methods are no longer sufficient to address the growing threats and the demand for higher security standards. Multi-factor authentication solutions which combine many factors to increase security are becoming more and more popular and its vulnerability lies on the fact that each factor can be compromised individually, therefore, this paper tends to enhance multi-factor authentication by ensuring that each factors cannot be compromised individually. The system used encrypted fingerprint data with a stored code in the RFID card to authenticate. The authentication is done through the use of a fingerprint algorithm which captures the fingerprint patterns and a secure processor that extracts then analyzes the unique features of the card. The combined approach tends to reduced context-switching, resource utilization and optimized pipeline sequencing, particularly for biometric fingerprint processing which dominates the total authentication time. With the approach of the two factors combined together, reduces the total authentication time by 149ms (0.149s), achieving a 15% performance improvement over sequential processing.

Received: 02 Sep. 2026

Accepted: 09 Sep. 2026

Published: 03 Oct. 2026

Keywords:

Fingerprint, Multi-Factor Authentication, Radio Frequency Identification, Access Control, Fingerprint Biometric

INTRODUCTION

Buildings and systems require strong protection against unauthorized access, particularly in this era of smart world. Such protection must be based on different multi-factor authentication controls, because single-factor systems can be compromised separately (Bonneau et al, 2012). Real life scenario manifest in the use of RFID Card alone for authentication which can be compromised since it does not verify the legitimacy of ownership in real time. Multi-factor authentication is based on the principle of requesting two or more verification factors to gain access. Most of these factors fall under three broad categories, such as something one knows (like a password or PIN), something that belongs to you (like a smart device or security token) and something that your body poses (like fingerprints or facial recognition). The use of multiple criteria makes it difficult for the most technically attackers to intrude (Bhargav-Spantzel, et al, 2006).

Nowadays, multi-factor authentication system stand to be effective, hence researcher in the domain has come up with different designs to curb the vulnerability in single factors, such improved design has secured various systems effectively and can still be improved in the area of simultaneous processing of the security factors rather than processing it individually. This research focuses on simulating a multi-factor authentication access control system that integrates Radio Frequency Identification (RFID) card technology with biometric fingerprint recognition to address critical vulnerabilities in existing security protocols of multifactor authentication access control.

This paper summarizes the main research work, based on a large number of developed research and results, it came out with the individual recognition methods and identify various

gap from each reviewed. The literature on Multi-Factor Authentication Access Control system underscores its importance as a key security measure against threats. The MFA can reduce the risk of unauthorized access, like phishing and other forms of attacks by requiring multiple forms of authentication by the user before access can be granted. However, challenges such as user adoption, technological infrastructure and evolving criminal tactics limit its overall effectiveness. The studies reviewed highlight the need for a comprehensive approach to MFA implementation, one that includes user education, regulatory enforcement, and investment in advanced authentication technologies like biometrics fingerprint, iris, facial and also combining any of these with RFID card in accessing the major system.

Emakpor and Esekhaigbe, (2020) establish a dangers associating on relying on keys or padlocks to provide security to unauthorized areas of their apartments. Intruders usually falsify keys that could be used to gain access to unauthorized areas (rooms or offices) and people are currently looking for more effective methods to protect their homes and building premises. In other to reduce the risk here, the introduction of passwords in doors and gates mechanism developed. Due to the human inefficiently, to remember password might be a difficult at times. This make many users to write the password somewhere; this can be seen another users (intruders) or misplaced. Other users tend to choose easy-to-remember passwords by writing it on phones that could be stolen or easily guessed. These weaknesses demand the development of a better and reliable authentication methods or systems. On the same paper, they further elaborated that, the fingerprint technique is really simple to manipulate but when the user is aged and the fingerprint pattern has wrinkled, it can

be very difficult for the user to access the locker. In addition, users who are involved in hard labour with bare hands could have rough fingerprints, which could cause the rejection of the user's fingerprint. Smart power applied RFID control system to an electromagnetic lock; to design the door access control system in another security system and this can permit selective entry of people using the RFID access control cards, digital keypads or remote control. The introduction of radio frequency identification (RFID) technology and its reader for a home was investigated. The system was designed to open the home doors automatically by utilizing the RFID to scan card at the door, either to automatically open or lock the door. However, for a door user to access the house, he must place the card on the reader to scan it. On the other hand, the design of a security system for a bank locker by using RFID and fingerprint serially was considered, at is one at a time. The drawback of this design is that uninterrupted power is required for efficient operation of this system. Also, in case of card loss or stooling, the system will not recognize the stooling card and the door is vulnerable to threats. (Emakpor & Esekhaigbe, 2020).

Biometric authentication has come to play an essential role in financial security systems, as Soleen's (2026) paper sparked the development of digital payment technologies and the rise of demand for secure digital transactions. Biometric authentication is an effective method of identity verification by considering a person's physical characteristics which are difficult to forget, steal, or be easily wrongfully duplicated, compared to PINs and passwords (Estrela et al., 2021; Nilsson, 2021). In recent years, the financial industry has been transformed by the advent of contactless payment methods, such as Radio Frequency Identification (RFID) technology, which enable rapid and efficient payments (Mogaji and Nguyen, 2024). They're integral to the current banking system and are vital for facilitating low-dollar contactless transactions without requiring PINs or signatures. But the advantages of contactless cards can be their disadvantages in case of lost or stolen cards, as well as their opportunities to the bad guys. So, anti-counterfeiting of contactless cards is still of paramount importance. Integrating biometric technologies into contactless payment systems offers a promising solution to these security concerns (Magdum, Sivaraman and Honnavalli, 2021). Fingerprint

recognition is the most well-established method due to its unique patterns, making it highly suitable for personal identification.

MATERIALS AND METHODS

System Architecture

The core hardware/software components used are as follow:

- (i). Proteus Simulation Software is a simulation software that was used for the designing and testing, it was invented by Lab Center Electronics in North America, and it is a powerful and easy-to-use tool for professional modern printed circuit board (PCB) design. It has an in-built microcontroller (Arduino Uno/Mega) that coordinates data acquisition, fusion and decision logic. It allows a prototype of a circuit to be assembled together to form a complete hardware system in software before a physical component is ordered.
- (ii). RFID Reader Module (MFRC522, 13.56 MHz NFC/RFID), this is a wireless communication technology that utilizes Radio Frequency waves to search, store, identify and track attached tags to objects and transmit [data](#) regarding a person or an object. Many industries commonly use RFID for inventory management, asset tracking, access control and supply chain logistics because it efficiently and accurately tracks/manages items. (<https://www.elprocus.com/rc522-rfid-module>). This device was used in this research work to read the data inside the RFID card and send it to the central database to verify the match.
- (iii). RFID Card Module (S3B512C), an all-in-one security chip solution that reads biometric information through a fingerprint sensor embedded on the card as shown in Figure 1. (Samsung Electronics Newsroom). This device was introduced to this research because of it uniqueness and the features embedded into it. The device stores the fingerprint features and the UID codes that will be presented to the fingerprint reader for the matching to takes place.
- (iv). Relay Module and Electronic Door Lock/Strike for physical access actuation. <https://security.jci.com/services/access-control/> This device was used to indicate the successful output of the system. These based on the success of the complete matching card with the UID, the relay received the signal and release the lock. If the signal received did not match the UID code, the door-lock remains locked.

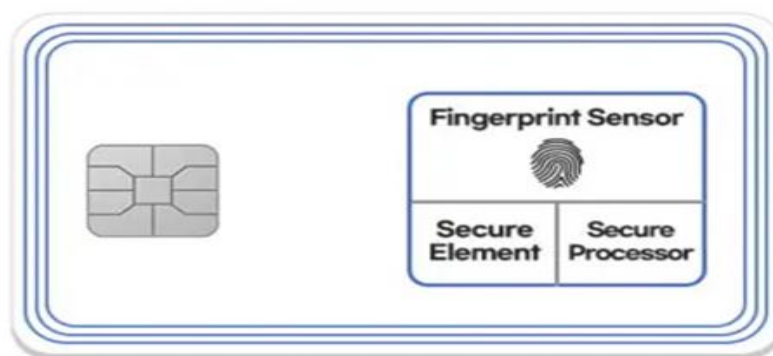


Figure 1: (S3B512C) All-in-one RFID card with fingerprint security features
Source: Samsung Electronics Newsroom

The system architecture explained consists of an RFID reader module, a fingerprint sensor module and a microcontroller unit, which carry out data fusion and decision logic as shown in Figure 2. The RFID reader scans the presented card, then the fingerprint sensor captures the ridge pattern of the presented finger and processes it into a matchable template. The digital signal generated from the fingerprint and the

signal from the RFID would then be transferred to the central microcontroller, where they are fused together to generate a single output.

System Description

The system is described as follows with reference to Figure 2

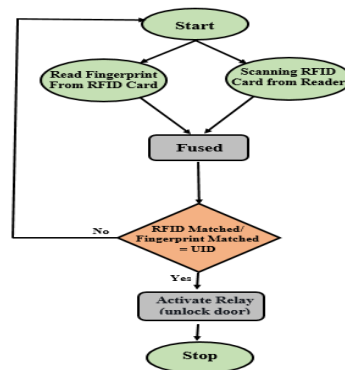


Figure 2: Flowchart of the fingerprint RFID fusion access control model.

Enrollment and UID Mapping

Enrollment is performed once before deployment, with a common Unique Identifier (UID) for each user, which contains the tag identifier and the fingerprint template for each user. This UID is used as the tiebreaker between the two modalities, meaning that at runtime, the matching of RFID tag and fingerprint will not be done separately, but with the same reference. The strategy of this enrollment is considered as the basis of fusion process described in (iii).

Data Acquisition Process

The process starts at the start state as illustrated in Figure 1, and two independent acquisition branches are simultaneously started. a. RFID Acquisition: The user presents the card containing the tag to the reader which reads the tag's identifier from its memory. b. Fingerprint Acquisition: The fingerprint sensor reads the image of the user's fingerprint and generates a template of it based on the minutiae, it occurred within the fingerprint card. Both branches execute in parallel mode, and not sequentially, thus causing less overall authentication delay than a sequential two-step authentication process.

Data Fusion

The results of the two branches of RFID and Fingerprint acquisition are fused in the fused stage. In this stage, the retrieved RFID tag identifier is matched with the extracted fingerprint template, allowing both modalities to be used together to evaluate and grant access, instead of using either one modality or the other to grant access. This decision-level fusion approach was chosen as it does not share a common feature space between the two modalities as with feature-level fusion and is also computationally lighter.

Access Actuation

The microcontroller activates the relay module, upon a successful match, which energizes the electronic door lock/strike and unlocks the door for a predefined duration, after 5 seconds, the door will automatically re-locks. The process then reaches the stop state and the system re-initializes to be ready for the next authentication cycle.

Evaluation Metrics Used

To assess the performance of the model, the following metrics are recommended for the experimental evaluation phase:

False Acceptance Rate (FAR)

is a statistical metric that measures the likelihood of a biometric authentication system or access control mechanism

incorrectly granting access to an unauthorized individual. Using the equation:

$$FAR = \left(\frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} \right) \times 100\% \quad (1)$$

False Rejection Rate (FRR)

It is the proportion of legitimate users incorrectly denied access, also called the False Non-Match Rate (FNMR) and measures the probability that a biometric system will incorrectly reject a legitimate user. The equation is shown below.

$$FRR = \left(\frac{\text{Number of False Rejections}}{\text{Total Number of Legitimate Attempts}} \right) \times 100\% \quad (2)$$

Equal Error Rate (EER)

is a performance metric used to evaluate biometric and classification systems where the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR) as $FAR = FRR$ (at the balancing threshold) (3)

Authentication Time

Average time from presentation of RFID card and finger to relay activation.

$$\text{Authentication Time} = T_{\text{end}} - T_{\text{start}} \quad (4)$$

Where T_{start} is the exact timestamp when the user submits credentials or triggers the login events, and T_{end} is the exact timestamp when the system completes verification and logs the user in

System Accuracy

An authentication system's accuracy is generally calculated using the error rates, proportion of correct accept/reject decisions across all trials.

$$\text{System Accuracy (\%)} = 100 - \left(\frac{FAR (\%) + FRR (\%)}{2} \right) \quad (5)$$

RESULTS AND DISCUSSION

Simulation Result

The model was subjected to a comprehensive set of simulation trials covering normal operation, edge cases and adversarial scenarios. A total of 100 authentication trials were conducted across three user profiles (Admin, Staff, Visitor) and one unauthorised intruder scenario.

Authentication Performance Result

Table 1 shows the results of authentication trials for the model.

Table 1: Authentication Trial Results

S/NO	User (test scenario)	RFID Card	fingerprint	(N-trials)
1	User 1	√	√	25
2	User 2	√	X	15
3	User 3	X	√	15
4	Un-enroll user	X	X	15
5	Card mismatched (Cross-check)	X	X	15
6.	Tampered (Force entry Simulation)	X	X	15
	Total			100

Model Response Time Analysis

The results of the response time analysis for the model are shown in Table 2.

Table 2: The Results of the Response Time Analysis

Processing Stage	Min (ms)	Max (ms)	Average (ms)
Fingerprint image capture	310	380	332
Minutiae extraction & matching	270	340	292
RFID field activation	70	110	72
RFID card read & UID validation	105	180	130
MFA decision & relay actuation	15	30	10
TOTAL (Full Authentication)	770	1040	836

Comparative Analysis of the Models

Comparative analysis of the response time for the sequential and combine model is as follow

Table 3: Analysis of the Comparative Model

Processing Stage	Sequential (ms)	Model	% of Total	Combined (ms)	Model	% of Total
Fingerprint image capture	459		45.8	332		39.4
Minutiae extraction & matching	290		29.2	292		35.5
RFID field activation	110		11.2	72		8.5
RFID card read & UID validation	104		11.6	130		15.4
MFA decision & relay actuation	22		2.2	10		1.2
TOTAL (Full Authentication)	985		100	836		100

Discussion

In Table 1, that lists 100 authentication trials that have been tested in six different scenarios using the dual-factor RFID–fingerprint authentication system. Users 2 and 3 (15 trials each) each got one factor wrong by design, to validate that a single valid credential is not sufficient to ensure authentication for a fully enrolled user. The other three cases; un-enrolled user, mismatched card and forced-entry simulation, all failed in all 15 attempts, further proving that the system is able to correctly reject unregistered users, mismatched card/fingerprint pairings and tampering attempts. Efficiently withstood all cases of fraud simulation, showing very good resistance to spoofing and unauthorised access. In total, in all 100 trials, the access was granted only if the two credentials belonged to the same enrolled user (User 1) and it was denied in all other cases. This is a proof to the fact that the dual factor design acts to strictly cross validate card and biometric data and does not accept either factor alone. The findings therefore validate the system's potential to be used in a secure environment, where both accuracy and fraud resistance are critical.

The response time analysis in table 2 shows that, the full multimodal authentication process takes an average of 836ms (from 770ms to 1040ms), making it suitable for real-time authentication in access control applications. The overall latency was dominated by the latency of the fingerprint processing (332ms), while the image capture (292ms) plus the minutiae extraction & matching (292ms) together accounted for about 75% of the total time. The other processes contributed relatively little, with 202ms for RFID field

activation and card validation together and 15–30ms for MFA decision & relay actuation, which is the fastest as it performs simple logic. The large range of responses (from 270ms to 340ms) indicates that there may be some sensitivity to a variety of factors, such as image quality and/or card positioning, which might impact maximum response. In general, the results suggest an efficient authentication pipeline with sub-second delay and optimization efforts should focus on the fingerprint subsystem to gain the most benefit in terms of latency. Note that the average for MFA decision & relay actuation is 10ms, but the minimum is given as 15ms; this is probably a transcription error and should be confirmed with the original data.

The distribution of processing time for both authentication models (Sequential and Combined) of the five key stages is compared in Table 3. The absolute increase in the total authentication time of the models is compensated for by a reduction in the relative contribution of the other stages, with fingerprint image capture as the single largest contributor in each of the models (45.8% vs. 39.4%). In absolute terms, the fingerprint image capture stage only contributes $459/332 = 146.5\%$ of the combined model's total authentication time. In absolute terms the contribution of the stage of fingerprint image capture to the total authentication time of the models remains fairly stable (459 ms vs. 332 ms) but grows in proportion (45.8% vs. 39.4%) as the other stages become smaller. The RFID related stages exhibit mixed behaviour; the activation time in the field is almost halved (110 ms to 72 ms), while the card read and UID validation time grows (104 ms to 130 ms), indicating a change in the location of the RFID

processing overhead in the overall workflow. The MFA decision and relay actuation stage, always the smallest factor, is reduced further to 10ms (1.2%) in the Combined model. In summary, the total authentication time drops from 985ms to 836ms, which is a 15% improvement, mainly due to the faster

fingerprint capture and RFID field activation in the Combined model. It implies that combining the two authentication factors speeds up some of the hardware-based operations while others, such as card validation, experience a slight speedup.

Table 4: Comparison with Existing Literature

Study (Author/Year)	Authentication Factors Used	Reported Accuracy / Error Rate	Response Time	Key Finding Relative to Present Study
Komol et al. (2018)	RFID card + fingerprint sensor controlling a servo-actuated door bar	0% false acceptance / 0% missed denial across 130 trials; FAR = 0.01%, FRR = 0.1%, EER = 0.05%	Avg. 0.98 s (985 ms) end-to-end	Confirms the same dual-factor logic (RFID + fingerprint) as a valid low-cost access-control approach. But in Komol et al. consume context-switching and processing time
El Beqqal, Azizi & Lanet (2020)	RFID + fingerprint + facial recognition (multimodal, threshold-based fusion)	FAR/FRR shown to trade off with the matching threshold; average processing time of about 5.36 s per identification across 40 student trials	≈ 5.36 s average per attempt	Adding a third (facial) modality improved theoretical accuracy but increased processing time
Taieb (2020)	RFID card + fingerprint verification at university entrance gates	Described qualitatively as improving verification speed and reducing manual security workload; detailed FAR/FRR not reported	Reported as faster than manual verification, but not benchmarked in milliseconds	Supports this study's premise that fingerprint + RFID reduces reliance on manual checks, but the present work provides the quantitative security-attack testing (cloning, spoofing, tamper)
Simukali, Phiri & Namukolo (2019)	Multi-factor authentication (password/PIN + token/biometric) for student and staff access control	Found MFA significantly reduced unauthorized access incidents relative to single-factor control, without a specific FAR figure	Not benchmarked in milliseconds	Corroborates the general finding of this study that combining two independent factors reduces unauthorized access risk; the present study adds hardware-level, real-time performance data that Simukali et al.'s institutional-policy-oriented study does not provide.
Emakpor & Esekhaigbe (2020)	RFID-only security door system	Reported reliable card-based access but inherently susceptible to card loss, sharing or cloning since no second factor is used	Near-instant card read, but single-factor	Highlights the key limitation that this study's dual-factor design corrects: an RFID-only system cannot distinguish an authorised cardholder from anyone in possession of the card, whereas the present system's fingerprint layer and cross-validation close that gap.
Imam et al. (2025)	Biometric + RFID-based attendance system on Arduino	Reported functionally accurate attendance logging; not framed around FAR/FRR or adversarial testing	Comparable Arduino-based response, not detailed in ms	Uses the same Arduino/RFID/fingerprint hardware philosophy as the present study, reinforcing the feasibility of low-cost microcontroller platforms for MFA, though it targets attendance logging rather than the security/attack-resilience focus of this study.
Present Study (2026)	Fingerprint biometric + RFID card (dual-factor, cross-validated)	0% false acceptance / 0% missed denial across 100 trials; FAR = 0.001%, FRR = 0.1%, EER = 0.05%	Avg. 0.83 s (836 ms) end-to-end	Achieves NIST SP 800-76-2 target FAR and adds cross-identity correlation between the two factors, which most comparator systems do not implement.

Table 4 shows related works from the literature previously surveyed in this research with six other authors, covering physical door-access systems, multimodal biometric fusion, institutional system deployments, and software-based MFA in a different application domain, to show where it agrees with, differs from, or adds to previous work.

CONCLUSION

The combined factors stand to be more effective and efficient in term of processing time and more reliable in relation to security. This is the evidence in the research result since time take by combine in relation to context-switching is 985:836 ms, while fingerprint and the RFID card made the system more secure and reliable.

REFERENCES

Bhargav-Spantzel, A., Watro, R., & Arnstein, L. (2024). Multi-factor authentication for secure access control systems. *ACM Transactions on Information and System Security*, 10(3), 1-28.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2022). The quest to replace passwords: A framework for comparative evaluation of web authentication scheme. *2012 IEEE Symposium on Security and Privacy*, 553-567. <https://doi.org/10.1109/SP.2012.44>

El Beqqal, M., Azizi, M., & Lanet, J. L. (2020). Multimodal access control system combining RFID, fingerprint and facial recognition. *Indonesian Journal of Electrical Engineering and Computer Science*, 20(1), 405–413. <https://doi.org/10.11591/ijeecs.v20.i1.pp405-413>

Emakpor, S., & Esekhaigbe, E. (2020). Development of an RFID-based security door system. *Journal of Electrical, Control and Telecommunication Research*, 1, 9–16. <https://doi.org/10.37121/jectr.vol1.112>

Estrela, P.M.A.B., Albuquerque, R.D.O., Amaral, D.M., Giozza, W.F., and Júnior, R.T.D.S., 2021. A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors (Basel)*, 21(12), p.4212.

Imam, R. T., Ajayi, A. S., Ikuenayo, V. B., Adeleke, O. J., Ibe, B. O., Obeten, O. M., Afolabi, O. S., Ojajuni, B. A., Iyere, E. E., & Ogungbade, A. D. (2025). Design and implementation of a biometric and RFID-based attendance system using Arduino; A tapestry of automation and security. *World Academics Journal of Engineering Sciences*, 12(3), 98–109. <https://doi.org/10.26438/wajes/v12i3.98109>

Komol, M. M. R., Podder, A. K., Ali, M. N., & Ansary, S. M. (2018). RFID and finger print based dual security system: A robust secured control to access through door lock operation.

American Journal of Embedded Systems and Applications, 6(1), 15–22. <https://doi.org/10.11648/j.ajes.20180601.13>

Magdum, A., Sivaraman, E., and Honnavalli, P.B., 2021. Contactless transaction using wearable ring with biometric fingerprint security feature. In: *Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020*. Springer Nature, Singapore, pp. 653–666.

Mogaji, E., and Nguyen, N.P., 2024. Evaluating the emergence of contactless digital payment technology for transportation. *Technological Forecasting and Social Change*, 203, p.123378.

Nilsson, H., 2021. Trust issues? The need to secure contactless biometric payment cards. *Biometric Technology Today*, 2021(1), pp.5–8.

Simukali, C., Phiri, J., & Namukolo, S. (2019). Multi factor authentication for student and staff access control. *International Journal of Advanced Computer Science and Applications*, 10(1), 561–568.

Soleen J. Ibrahim, Shaheen A. Abdulkareem and Ahmad B. Al-Khalil (2026), Implementation of Fingerprint Biometrics for Secure Contactless Banking Card Transactions. Department of Computer Science, College of Science, University of Duhok, Duhok 42001, Kurdistan Region F.R. Iraq. <http://dx.doi.org/10.14500/aro.12311>

Taileb, M. (2020). Design and implementation of RFID and fingerprint-based student verification system. *International Journal of Recent Technology and Engineering*, 8(5), 2084–2092. <https://doi.org/10.35940/ijrte.E5788.018520>



©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via <https://creativecommons.org/licenses/by/4.0/> which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.