iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78495

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Smart Locking System with Digital Data Logging

S. Bhuvaneshwari[1], R. M. Gomathi[2]
[1]*UG Scholar, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai India*
[2]*Associate Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai India*

Abstract: ***Security today is a far greater issue than what we used to see in the past with just metal locks. With that in mind think of for instance in factories, office buildings, residential areas and server rooms which all require protection. What we had before does not cut it as basic locks do not have in them the ability to track or to manage everything as a whole or to report who went in and when. That leaves room for issues like break ins or misuse of the locks. Entry is via card swipe or pin which at the same time improves convenience and security. Also each time there is an access attempt the event is put into a secure spot in our MongoDB collection for later look back. A new opportunity presents itself as remote admin control which in turn gives managers the ability to adjust user rights via a web interface built on top of MongoDB, Express.js, and Node.js. As live monitoring goes on constantly alerts go off at the attempt of breach. Because of encryption which we have put in place any connection between device and server is secure from eaves and change. Control is brought to a single point even as units may be located at many sites which in turn makes rules the same throughout their application. We have logs of every event which in turn will aid in later reviews for audit or incident response. Each component is designed to work well, this is to say there is little tight coupling which in turn makes for easy updates and managed growth across different buildings. We have powered down hardware which in the past was a large draw of energy and in the software we have scaled out smartly leaving behind the old lock in issues.***

Keywords: IoT, Access Control System, Raspberry Pi Pico, Dual-Authentication, RFID, PIN Authentication, MongoDB, MEN Stack, Remote Management, Secure Communication, Audit Trail, Smart Lock

I. INTRODUCTION

The entire protection game has gradually progressed to more intelligent technology since the days of simple steel padlocks--essentially the same way that our course work will shift to not memorising stuff but rather analytical thinking to the levels of upper degree classes. In the old days, key locks had been used; they did little or nothing proactively after being locked, no signatures, no notifications, no immediate response, so when anything was lost or duplicated unauthorised there was a rapid increase in the number of problems. Part of the upgrades was in electrically, like the move to digital in our laboratories, although much of it still made the end user rely on one vendor, without the smooth integration we enjoy in our current, networked systems. It is much like when certain professors adhere to their teaching styles despite the interdisciplinary methods yielding better outcomes.

To begin with, the system is addressing the key issues of an IoT-based access solution. The box contains a Raspberry Pi Pico that does the hard work, connecting two ways to verify identity, which includes a scanner reading tags and buttons that allow typing a code. All the attempts fall into the same safe place a sheltered MongoDB collection which is run subtly by Node.js, and Express as well as the same database stack. A backdrop of a login guard provides unlimited access to a browser panel allowing users to appear or disappear, entries to be flicked on screens and automatically popping up with summaries. All the actions are recorded only once, narrowly packed together and only revealed on demand, starting at the beginning and finishing at the end.

The real change is after passive to proactive security and it does pay off well. Exact time-stamped logs imply that it is more secure and audit is effortless. With all actions being properly documented, it is easy to argue that compliance audits or sifting through historical eventualities are unproblematic. The remote control of access to anyone goes hand in hand with the instant nature of updates the no longer need to take keys back or run after locks. That flexibility is a burden of day to day operations. This instead of a toppling of old workarounds one builds something that grows to a size and remains firmly fixed. The new tools will be fitted immediately, as the base can be expanded. Physical access is secure, not due to chance, but by engineering.

II. RELATED WORK

Gurung and team demonstrated the new features of smart locks over old-school tricks by giving them memory and online check-in possibilities. They do not only lock doors, but also take note of people entering and leaving. These devices have microchips that introduce smarter protection at home, and a direction was opened to others[1].

After the work, the group of Gupta shifted to control panels - the reason why there should be such control panels in offices. Beats of a Central command is superior to solo setups in cases of the management of various people; we did not find any reason to avoid it by reflecting it internally within our own, core venue[2].

Kamelia and co. experimented with the possibility of opening doors using Bluetooth on Android phones. Although smartphones were their digital keys, the connection was not always effective at a great distance - which casts doubt on the level of reliability. This omission is an indication that there must be supporting methods of verifying access[3]. Krishnamoorthy and colleagues addressed costly sections by crafting locking systems out of cheap electronics that are safe. What they demonstrated is in line with our judgment: chips with low cost can still perform well by design[4].

Mrinal and Priyanka in 2017 discussed the topic of the role of sensing tech in automated setups. They demonstrated that the connection of door locks to other sensors enhances the overall safety in the house rather than separated functions[5]. About the same period, Nandhini and Hemavathi also tried small, yet mighty boards - particularly Raspberry Pi - as control hubs with such systems. Since this hardware is effective in working, it supports the decision made in this context to entrust delivery of strong calculation in executing linked devices and remaining connected to the internet[6].

Speaking of system safety as a viewer, the article by Prakash and Kumar in 2018 has indicated that instant warnings can actually be crucial. Included in the construction of their smart lock powered by IoT, quick breach notifications were equally relevant as much as the offline lock service[7]. A year later, Sharma and Jain concentrated on elements of weakness in the paths of online messaging. Connected locks are like doors into a network, which is why they sounded alarms that, unfortunately, these can be hacked easily[8].

Secrecy during transfer of information demanded well grounded coding techniques, which in this case was done by trusted transmission rules.

The justification of having more than a single check of the login was clear in a study provided by Singh and colleagues in 2022 - increased trust is gained in identity verification. The paper presented the effectiveness of the combination of a password you clearly remember and a physical access card in comparison with less challenging security measures based solely on one protection[9]. Verma and Tripathi five years later in their analysis incorporated previous findings, with designs being capable of development and modification with time in such a way that as fresh risks emerge, the defenses have been effective [10].

III. PROPOSED WORK

We use a stratified method which enhances security, expansion capacity and maintenance through clear segregation of tasks in domains of interaction, processing and storage as shown in Figure 1. Hardware-facing part of the access point is more similar to a minimal terminal, consisting of a Raspberry⁻ one board, which works as an MFRC522 tag reader hooked up to a 4×4 button pad in an escape hatch. Things get stored here like credentials, output actions, like unlocking, occur only on command, and status updates can be displayed in a small display.

Decision making occurs actually at the middle level, which is more like brain-to-brain control rather than an inactive relay. It is based on a Node.js server with Express.js, which carries out essential functions such as credential validation and access control, allowing policies to remain consistent whilst keeping confidential information out of cards that are not so secure. Lastly, the Data Tier maintains a distinct MongoDB store as the primary repository of user records and a complete history of access events all of which are timed to maintain isolated growth and control without losing any accuracy.

Immediately, the arrangement responds to the actions and all is held secured. Once one attempts to access a RFID tag by scanning it or typing a number, the Raspberry Pi Pico forcibly captures the data instantly shown in Figure 2 and sends it safely to a Node.js server. It has a server which verifies the incoming data with entries into the MongoDB store. Go or no-go result gives an immediate response basing on matching or not, accompanied by a record that is saved chronologically to a logger. Nothing passes without being noticed by leaving a trace because there is no attempt that does not leave a trace. Then, the server will report to the Pico: in case it is approved, the solenoid will be switched on, opening the door, and a success will be shown on the screen, as depicted in Figure 3. Upon refusal, the bolt remains locked and an error message is displayed in its place instead, as in Figure 4. All of the tries are subjected to central validation, which is also documented, thus nothing passes unnoticed. A trace is generated automatically, and it is readable.

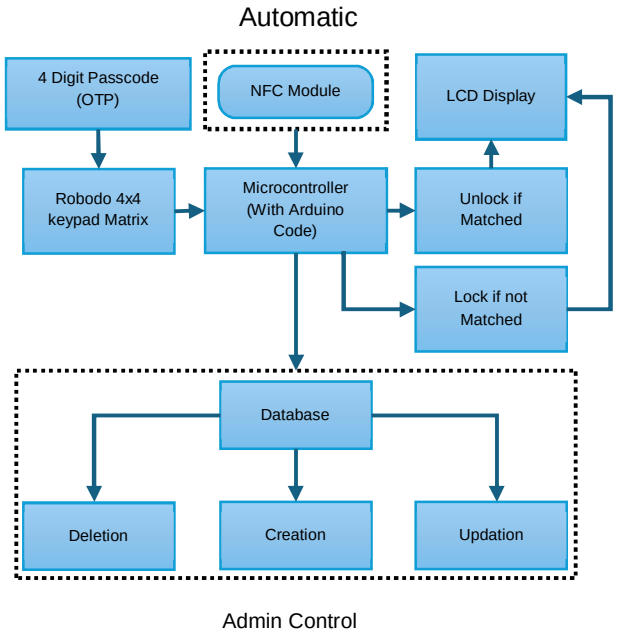


Figure 1 - Smart Locking System with Digital Data Logging

IV. RESULTS

It finished. There was a working machine, which struck every dotted spot at the beginning. The two-step login when tested was also very strong, as RFID swipes and PIN entries saw the fast and correct entry made, with the display showing simple updates each time. On the center right: live action activity. Each attempt to get in, with or without being granted, was recorded appropriately within MongoDB with a tag on who attempted it and the time. And top of that the online control panel was running fine. Another set of access credentials updated the door lock immediately and demonstrated the ease with which the online controls communicate with the real device. At the very beginning, the construction was to be reliable and cost-effective, this experiment proved that it will.

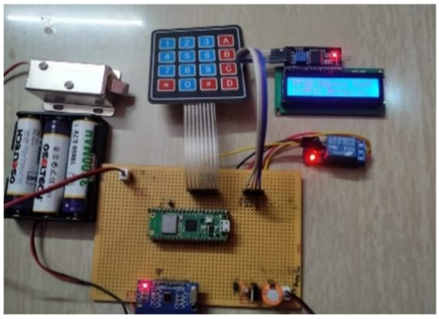


Figure 2 - Components Assembly

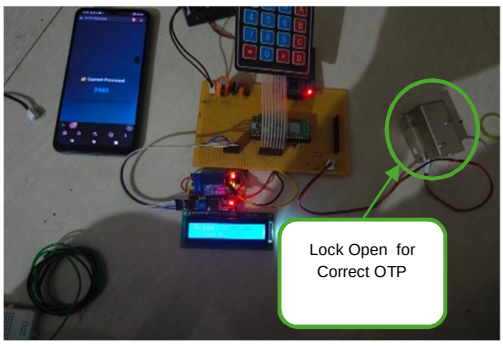


Figure 3 - Door unlock

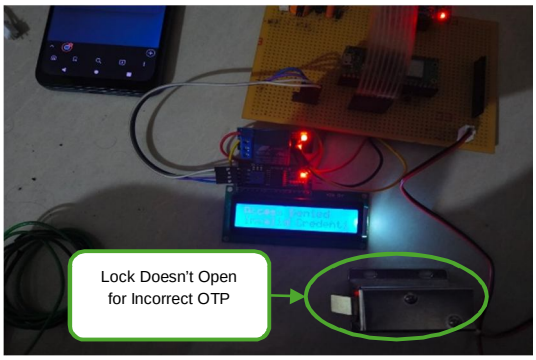


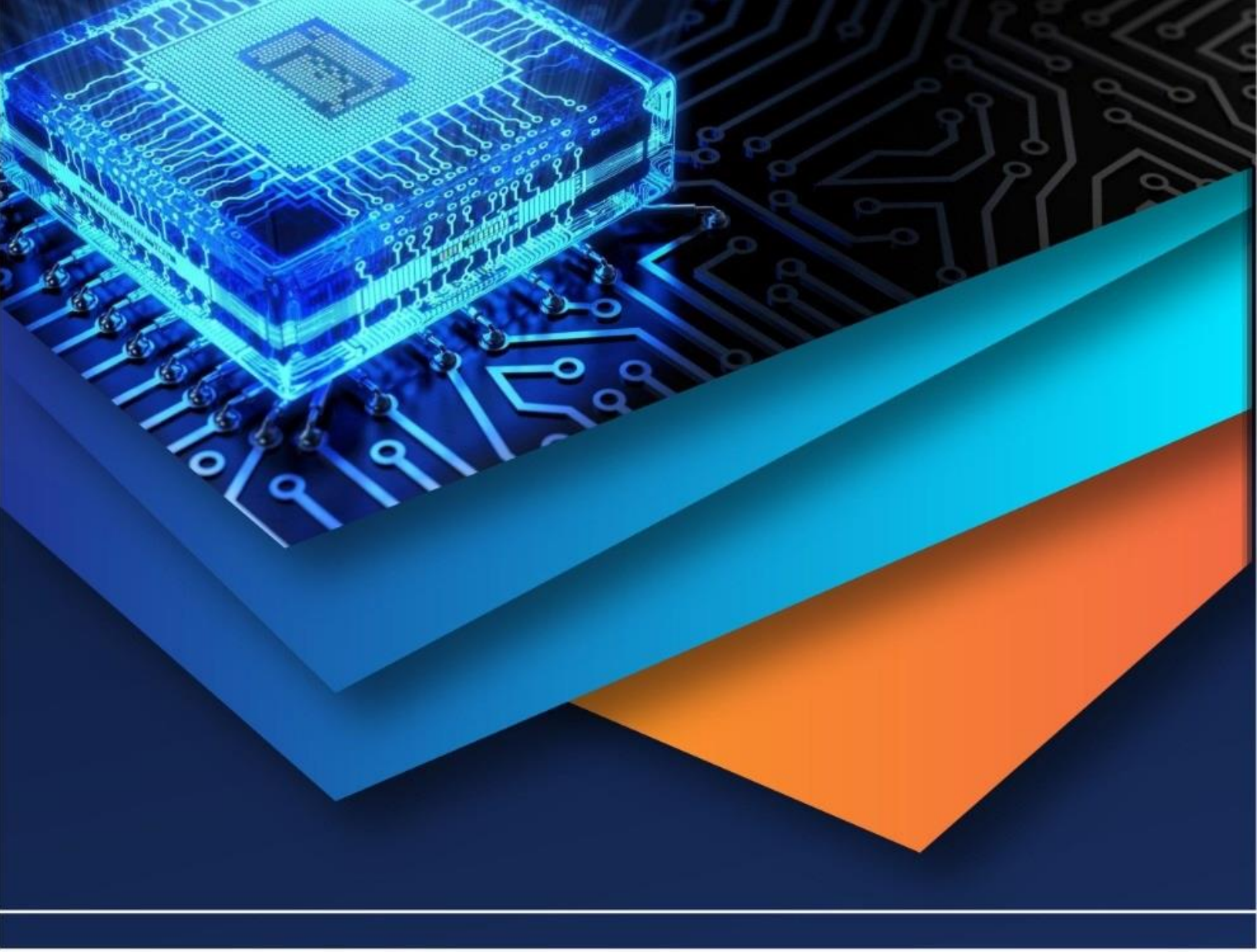
Figure 4 - Door lock

V. CONCLUSION

An IoT-powered lock system was constructed as functioning with a digital record keeping. Rather than having one step verification, it runs two layers of identity checks that are connected to a single web backend consisting of MongoDB, Express, and Node.js. It enhances a sense of security since the events of access are centralized and therefore traceable with time passage. What sets this apart? The layers are divided into hardware, server logic and user interface functional areas. Remote control is painlessly achievable, and record keeping is easily available in the future. All the parts are loosely attached to each other, permitting flexibility in the future. The developments that may take place in the future are the fingerprint sensors, phone-based controls or algorithms that may warn on odd behavior patterns. Not all things are in their places - all things are flexible. The tested ideas here provide a firm basis of solutions, which are smarter to physical access.

REFERENCES

[1] Gurung, C., Subba, D., Sharma, D., & Sharma, Y. SMART LOCK USING IOT. Department Of Computer Science And Technology.
[2] Gupta, R.K., Balamurugan, S., Aroul, K., & Marimuthu, R. (2016). IoT Based Door Entry System. Indian Journal of Science and Technology, 9(37). doi:10.17485/ijst/2016/v9i37/102136.
[3] Kamelia, L., Noorhassan, A.S.R., Sanjaya, M., & Mulyana, E. DOOR-AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE. Islamic University of Bandung, Indonesia.
[4] Krishnamoorthy, N., Kalaimagal, R., Shankar, S.G., & Asif, N.A. (2018). IoT based smart door locks. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(3), 151–154.
[5] Mrinal, M., & Priyanka, L. (2017, November 23). Smart home — Automation and security system based on sensing mechanism. 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon). IEEE.
[6] Nandhini, M., & Hemavathi, G. (2017). IoT based home automation system using Raspberry Pi. International Journal of Innovative Research in Computer and Communication Engineering, 5(3).
[7] Prakash, R., & Kumar, A. (2018). Smart lock security system using IoT. International Journal of Engineering & Technology, 7(2.8), 52–55.
[8] Sharma, A., & Jain, V. (2019). IoT enabled smart door locking system. International Journal of Computer Applications, 975–8887.
[9] Singh, A., Sachan, A., Gupta, K., Kapoor, G., Singh, H.K., & Singh, A. (2022). IOT Based Smart Lock. International Research Journal of Modern Engineering & Technology Science, 4(3), 2582–5208.
[10] Verma, P., & Tripathi, R.K. (2017). Smart home security system using IoT. International Journal of Advanced Research in Computer Science, 8(5).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY