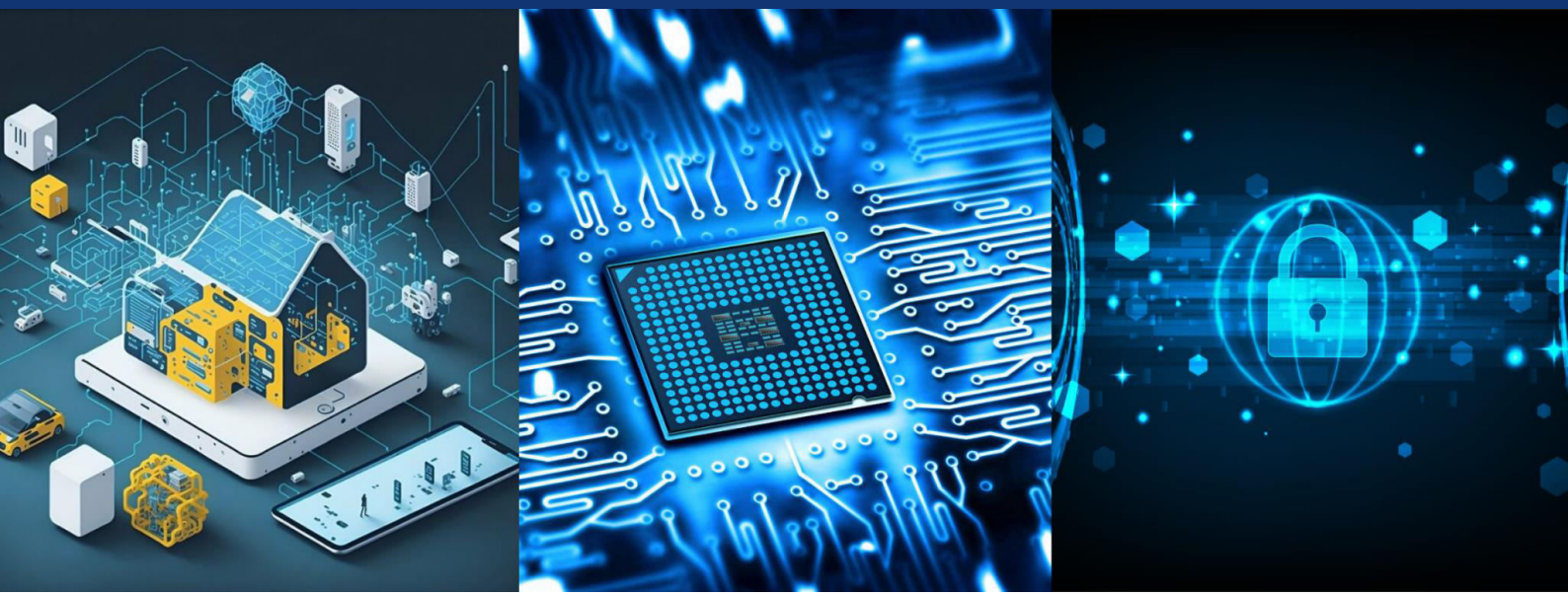
IJIRCCE

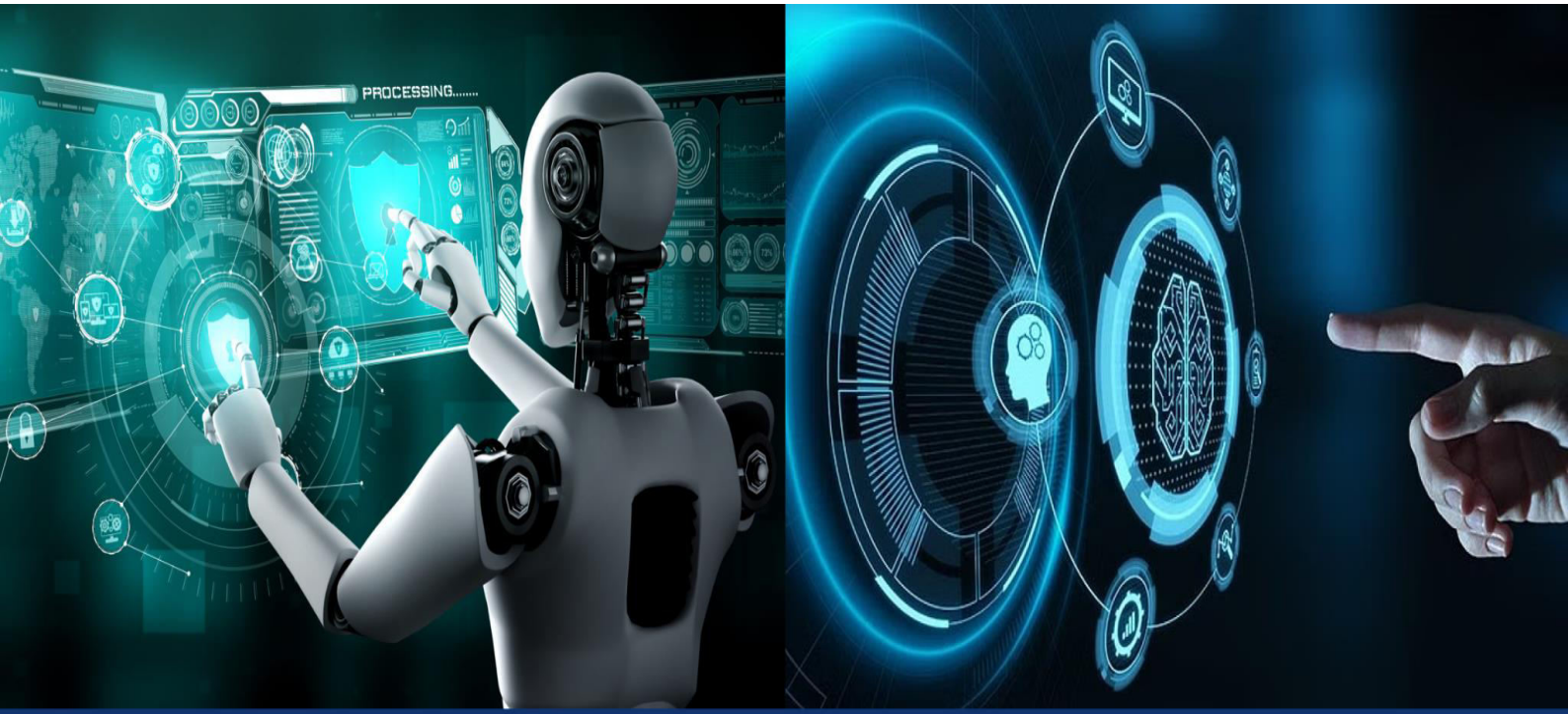
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 10, October 2026

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Design & Implementation A Low-Cost Arduino-Based Smart Door Security System with Brute-Force Attack Prevention for IoT Smart Homes

Nahed A. Al Nahash

Cybersecurity Consulting Specialist & Trainer, Computer & Information Technology, Department of Cyber Security.

Ednex Academy, Najran, Saudi Arabia

ABSTRACT: The rapid integration of IoT technology into residential settings has increased smart homes' vulnerability to security breaches, especially because many smart door locks use easily cracked passwords. Most affordable smart locks lack practical protection against such attacks. This paper addresses this issue by implementing and analysing a cost-effective smart door security system based on the Arduino Uno R3, using keyless authentication and auto-locking after three consecutive unsuccessful attempts.

The purpose of the experiment is to design a brute-force-resistant mechanism for use in resource-constrained smart homes. The design and simulation were done using Tinkercad and incorporated an Arduino Uno R3, a 4 x 4 keypad, a 16 x 2 LCD, and a micro servo motor for the locking/unlocking mechanism. We conducted five experiments to evaluate password acceptance/rejection, the lockout mechanism, brute-force resistance, and system resets, among others. The analysis shows 100% accuracy in distinguishing valid from invalid passwords, effective lockout after three invalid attempts, and timely unlocking after 30 minutes elapse, with an average of 12 milliseconds for password validation. In sum, the research shows that adding a time-based lockout mechanism to affordable embedded door-lock firmware significantly increases resistance to brute-force attacks.

KEYWORDS: Internet of Things (IoT), Smart Home Security, Arduino Uno R3, Smart Door Lock, Brute-Force Attack Mitigation, Password Authentication, Embedded Systems Cybersecurity

I. INTRODUCTION

From an innovative concept, smart homes have become part of residents' daily lives, using sensors, actuators, and controllers to automate lighting, climate, entertainment systems, and, in many cases, physical security [1]. The main driver of these changes is the development of the Internet of Things (IoT), a paradigm in which ordinary objects are equipped with sensing, computing, and communication technologies to exchange information and interact with the environment without direct human involvement [2]. In such an environment, smart door locks become especially important because, unlike smart bulbs and thermostats, door locks represent a physical boundary between a family and the outside world, and vulnerabilities in their authentication mechanisms become concrete security threats.

Evidence shows that attacks on these devices have grown at the same pace as the proliferation of connected devices. According to industry telemetry, the number of connected IoT devices will reach about 21.1 billion by the end of 2025, reflecting double-digit annual growth [3,4]. In addition, on average, about 820,000 automated attacks targeted IoT devices daily throughout 2025, a 46% increase from the previous year, when the main targets were routers and gateway-adjacent devices [5,6].

In [7,8], authors report on the period up to mid-2026 and highlight unprecedented botnet attacks using devices commonly found in households, such as routers, cameras, and digital video recorders, showing how vulnerable endpoint devices in residential areas are unwittingly leveraged in large-scale infrastructure attacks. Although most of these attacks target routers and cameras rather than door locks directly, they indicate a broader trend: automated attackers often target devices with no security measures against unauthorized access.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Although the use of smart lock technologies that incorporate biometric authentication, mobile apps, and even cloud connectivity [9,10] is gaining commercial popularity, a considerable part of self-made and budget-oriented smart lock designs discussed on maker websites and academic examples are based on the use of basic numeric passwords entered via a keyboard and lack any protection mechanisms from brute-force attempts [11]. This approach is problematic because password-based authentication alone can be easily exploited by brute-force or password-list attacks without a mechanism to limit attempts [12]. However, despite plenty of information on established prevention methods, including account lockouts, IP rate limiting, and multi-factor authentication, these techniques have not been applied to affordable embedded systems that any average homeowner can manufacture or buy [13,14]. Two-factor and biometric locks have addressed this problem but at a much higher cost [15], which prevents widespread use by cost-conscious individuals and families.

Concurrently, most academic research on securing the smart home focuses on network-level protection, such as machine learning-based intrusion detection mechanisms that operate within the gateway or the cloud [16,17]. This creates a research gap in surveys of architectural attacks against smart home security systems that describe attacks at threat a conceptual level [18,19], as well as in network-based IDS, which rely on the assumption of a secure physical access mechanism. Few papers address the problem of building a cheap, self-contained, experimental solution for defending against brute-force attacks on door locks.

To help bridge this knowledge gap, this research focuses on developing and implementing a low-cost smart door security system based on the Arduino Uno R3 microcontroller to address brute-force and repeated-guessing attacks using a time-out strategy. After three consecutive failed password attempts, the system locks out all attempts to access the door for the next 30 minutes. This gives the homeowner time to detect a potential threat and prevents the attacker from guessing indefinitely.

The main contributions of the study include:

- The development of a smart lock that uses Arduino to integrate keypad authentication, an LCD screen for status, and a servomechanism for opening.
- A method to mitigate brute-force attacks by monitoring the number of failed authentication attempts.
- A timeout measure that denies future authentication attempts for a predetermined period after failure.
- A cost-effective way to design and implement the system using commonly available hardware parts.
- Testing the effectiveness of authentication, lock-out, and action timing in various correct and attack scenarios.

II. RELATED WORK

This section reviews previous research related to the proposed system, grouped under smart home security, authentication techniques, intrusion detection, and Arduino-based smart locks, followed by the limitations that led to this study.

A. Smart Home Security

Overall, studies of smart home security threats invariably reveal unauthorized access, data theft, and denial of service as the key threats affecting connected home devices [1]. In this regard, authors in [18] examined the security status of various categories of smart home devices, such as voice assistants, smart TVs, lockers, and sensors. They noted that the main technical measures to mitigate security threats are encryption, authentication, and intrusion detection [18]. Another bibliometric study of smart home literature from 2013 to 2025 found that the most researched domains are Internet of Things applications and home automation systems, while the top contributing disciplines are computer science and engineering [1].

In addition to the architectural analysis, a study done under the sponsorship of NIST on the perceptions of end-users discovered that the level of security and privacy worries for smart homes differed significantly from one category of smart devices to another, with entry control devices, including doors and cameras, having far greater worries among homeowners compared to the convenience devices such as smart speakers [20]. Smart home security has many layers but still lacks a clear solution.

B. Authentication Systems

Smart locks can be secured with simple numeric codes, RFID cards, fingerprint recognition, and two-factor authentication through apps [15]. Two-factor authentication combines a knowledge factor, such as a PIN code, with possession factor or biometrics. It is often touted as more secure than single-factor password access because an attacker must bypass two separate factors at once [14]. Biometric locks used by various firms claim near-zero false-acceptance rates and extremely

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

fast recognition [9]; however, this level of sophistication generally requires specialized hardware and cloud computing services that increase costs and introduce security issues related to the latter. -Password- and keypad-based systems remain favoured in cheaper, more hands-on projects because they avoid this added cost and use components like a 4x4 matrix keypad with a system like Arduino [11]. But the very fact that makes these systems cheap also makes them susceptible to guessing attacks without a limit on attempts.

C. Intrusion Detection

Intrusion detection-based smart home security solutions have been developed independently of access-control solutions. Authors in [16] suggested a two-level intrusion detection mechanism based on machine learning, where a small classifier runs on a microcontroller-based smart thermostat, and a more complex classifier operates in the cloud. The authors claimed an intruder detection rate of more than 99% for multiclass classification from the cloud side [16]. Another work on adaptive intrusion detection architecture for smart homes was suggested by [17]. Authors in [21] tested various machine learning techniques, including meta-heuristic-optimized classifiers, on a smart home attack dataset. Their analysis revealed high classification efficiency across several attacks [21]. Various reviews of intrusion detection in IoT have also shown that machine learning, specifically ensemble learning and deep learning models, has become a primary tool for detecting anomalies in IoT networks [22]. These solutions are highly efficient at detecting malicious activity but do not prevent an attacker from guessing a door keypad password.

D. Arduino Smart Locks

Many maker- and hobby-oriented sources describe smart lock designs that integrate RFID readers, keypads, servo motors, and LCDs on an Arduino board [11]. Most of these projects compare the entered code or number with a predefined one and unlock a servo-controlled door latch when they match; any other attempt denies access, with an optional buzzer notification. Although these smart locks are relatively affordable, most lack protection against brute-force attacks.

E. Existing Limitations

From the previous subsections, three main drawbacks occur throughout literature. First, architectural and survey-based research [1,18,19] mentions the risk of brute force and unauthorized access theoretically but offers no solution or implementation. Second, intrusion detection studies in [16,17,21] focus on network-level threats rather than specifically addressing repeated password guesses for a physical keypad lock. Finally, current low-budget Arduino-based smart locks [11] have a functional user-authentication feature. Still, the lack of lockout or rate-limiting features leaves them vulnerable to brute-force attacks, as many other researchers have warned [12,13]. Table 1 summarizes representative studies against these criteria.

Study	Hardware	Authentication	Attack Prevention	Limitation
Vardakis et al. (2024)	No	General discussion	Conceptual only	Review only, no implementation
Alshamsi et al. (2024)	No	IDS-based	Yes (ML detection)	No hardware implementation
Javed et al. (2024)	Microcontroller (ESP32)	Not addressed	Yes (2-layer ML IDS)	Targets network traffic, not door entry
Sallay (2024)	No	Not addressed	Yes (ensemble ML)	Dataset/simulation based, no physical lock
Oyelakin et al. (2025)	No	Not addressed	Yes (ML classification)	Dataset-only evaluation
Proposed System	Arduino Uno R3	Keypad password	Time-based lockout	Experimentally evaluated prototype

TABLE I: COMPARISON OF REPRESENTATIVE RELATED STUDIES WITH THE PROPOSED SYSTEM

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

F. Research Gap

Although many studies address IoT and smart-home security and networking, and many machine-learning works focus on smart-home intrusion detection, few papers offer practical, cost-effective implementations of password protection with a lockout feature at the door entry. Arduino developers' work shows how easily one can implement a password- and servo-based door-opening system. However, very few projects include lockout features, which are widely discussed in the authentication and security literature [12,13]. This gap matters because a smart lock without an attempt-limiting algorithm provides an illusion of security; an unauthorized individual with access to the keypad hardware, either physically or remotely, can guess passwords indefinitely without repercussions. Current research addresses this gap by combining affordable embedded hardware with a lockout algorithm proven experimentally, not just theoretically.

III. PROPOSED ALGORITHM

The proposed model comprises an intelligent smart door lock system that relies on an Arduino Uno R3 microcontroller as the primary control and authentication point for the lock system. The homeowner uses a 4x4 matrix keypad to enter the required numeric code. At the same time, a 16x2 LCD screen displays information and status messages. After authentication, the Arduino activates a micro servo that physically operates the door latch. Authentication and locking run entirely on the microcontroller, so the system can operate as a standalone security portal without a constant network connection, while still working with a home network or IoT gateway for additional features like remote alerts.

The heart of the system is a failed-attempt counter that tracks how many times a password fails to match the saved password. As soon as the failed-attempt counter reaches three, the system enters lockout mode for 30 minutes, after which it accepts no more keypad entries until it resets. When the correct password is entered, however, the counter resets to zero, and the servo motor unlocks the door.

This approach takes advantage of the program's deterministic flow and low memory requirements, ensuring the system can run effectively on the microcontroller and meet the effectiveness requirements set out in the research study. Figure 1 below shows the system architecture.

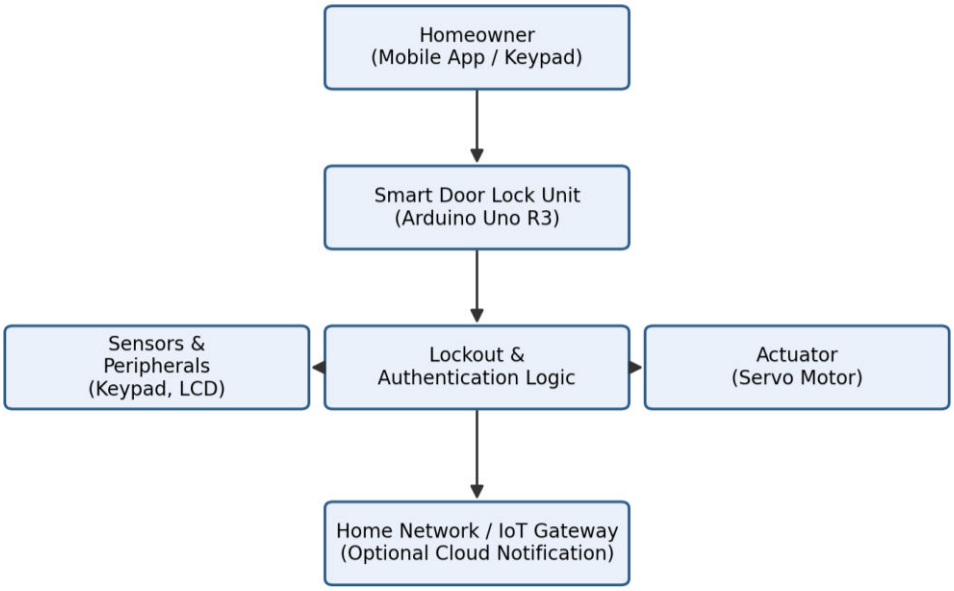


Figure I: Smart Home Security Architecture

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

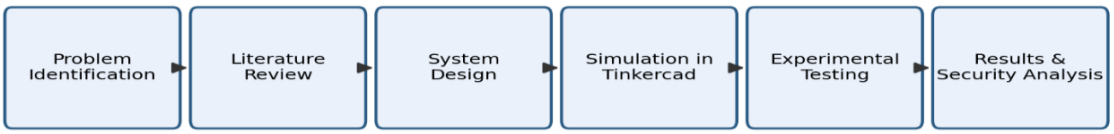


Figure II: Research Workflow

IV. MATERIALS AND METHODS

A. Hardware

The above-mentioned prototype was assembled from the following components: an Arduino Uno R3 board, which acts as the microcontroller that is responsible for interpreting keypad data, controlling the LCD [23], and operating the servo motor; a 4x4 matrix keypad, which is employed for entering the numeric code; a 16x2 LCD screen, which is responsible for displaying requests, messages, and warnings to the user; a micro servo motor, which simulates a mechanical lock of the door and turns to an opened state after successful authentication and back to a closed one afterwards; and an ordinary power source supplying the necessary voltage to the Arduino board and all the connected devices [24]. These components were chosen for their affordability and availability, and because they fit the research's low-cost requirement.

B. Software

The system firmware was programmed and compiled in the Arduino IDE for the Arduino Uno R3 microcontroller board. The circuit design, wiring, and testing were done in Tinkercad, an online electronic simulation application from Autodesk. This was used to test the keypad, LCD, servo, and Arduino connections before physical assembly. The firmware controls keypad scanning, comparison, LCD, servo movement, and the failed-attempt counter/lock timer, as explained later (Appendix I).

C. Algorithm

The authentication process employs a simple password verification technique as shown in Figure III below. The system receives password input from the keypad and verifies whether it matches the stored password. On success, the servo opens the door and resets the counter to zero. On failure, the system increments the counter and issues a denial notification. If the count exceeds three attempts, the system locks itself for 30 minutes, then reverts to its normal state after resetting the counter.

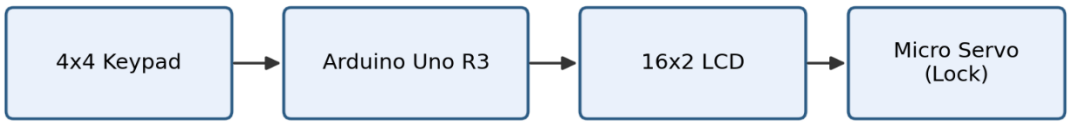


Figure III: System Block Diagram (Arduino to LCD, Keypad, and Servo)

The brute-force lockout logic that governs the transition into and out of the locked state can be summarized in pseudocode as follows:

```
attempts = 0 LOOP:  read password from keypad  IF password == stored password THEN  unlock servo()
attempts = 0  ELSE  attempts = attempts + 1  display ("Access Denied")IF attempts >= 3 THEN  display
("System Locked - 30 min")  lock_system_for(1800) // seconds  attempts = 0  END IF  END IF END LOOP
```

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

D. Methodological Approach

This research used an engineering methodology involving description, literature comparison, theoretical cybersecurity model development, and simulation to design a cost-effective smart door security system in the Internet of Things (IoT) environment. The methodology ensured that the theoretical and practical aspects of the proposed smart security system were informed by existing cybersecurity knowledge. This engineering methodology is used extensively in IoT cybersecurity studies, where theoretical security analysis is coupled with prototype design and experimentation [18,19].

A descriptive-analytical method was first used to understand the current state of smart home security and identify the main weaknesses related to password authentication. The literature on smart home security, Internet of Things architecture, authentication methods, and cyberattacks was critically analyzed to trace how existing protection methods evolved and what challenges remained for affordable embedded security systems [1,2]. This provided a theoretical basis for determining security needs for the proposed smart lock design.

For further analysis, we used scientific content analysis of recent journal publications, conference presentations, and industry reports on IoT attacks, smart lock authentication, intrusion detection, brute force prevention, and embedded security. We placed special emphasis on publications from 2021 to 2026 to ensure the suggested solution reflects the latest advances in IoT security.

Additional sources for conducting this research involved desktop studies using online scientific databases and peer-reviewed articles. The database sources included IEEE Xplore, SpringerLink, ScienceDirect, MDPI, and others, which provided credible information on smart home cybersecurity, authentication techniques, and Arduino-based embedded systems. This approach ensured the adopted devices met engineering standards and provided cybersecurity recommendations; the system design was based on security theories used in practice. Such theories include threat modelling and attack surface analysis. Threat modelling was used to identify the most likely ways to attack the system using passwords, such as brute force attacks, dictionary attacks, and password guessing. Next, an attack surface analysis was applied to identify potential vulnerabilities in the authentication process and assess how a timeout lockout policy may affect the likelihood of attacks [13].

Further, a comparative study assessed various smart home security systems discussed in previous studies. It compared authentication methods, attack protection, implementation difficulties, hardware needs, and cost. This comparative analysis helped show that no practical, low-cost solution combines password authentication with brute-force attack protection.

The final step of the design process involved validating the conceptual framework through simulation-based experimentation. Instead of testing the prototype in an actual physical setting, the design concept was tested using the Tinkercad simulation environment and the Arduino programming environment. Through simulation, the authentication process, password validation, lockout, servo action, and system response were validated in both normal and malicious settings. This simulation-based approach allowed testing the proposed security design's practical performance before physical implementation.

V. SIMULATION RESULTS

Table II presents the results for correct and incorrect passwords. The results show that the system successfully authenticated all correct passwords and denied all incorrect passwords.

Test	Success Rate
Correct password (10 trials)	100%
Wrong password (10 trials)	0% (access correctly denied)

TABLE II: INAUTHENTICITY ACCURACY

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

As shown in Table III, warnings are generated after failures in the first and second stages, whereas a lockout occurs after the third failure.

Failed Attempts	System Response
1	Warning message on LCD
2	Warning message + buzzer alert
3	System locked for 30 minutes

TABLE III: LOCKOUT MECHANISM RESPONSE

Table IV provides the average execution times for the system's main functions. The password check took about 12 ms, the servo motor operation (a physical action) took about 380 ms, and the LCD update took about 20 ms. These values show that authentication and lockout procedures add minimal lag to the response time, and motor actuation adds the most.

Operation	Average Time (ms)
Password check	12
Servo activation	380
LCD update	20

TABLE IV: EXECUTION TIME OF CORE OPERATIONS.

The entire system was consistent in terms of meeting the design specifications through all five experiments: the correct passwords always opened the door, the wrong passwords were always denied, the lockout feature was activated after the third denial regardless of the rate of submission, and after the 30-minute delay, the system returned to normal operation.

VI. DISCUSSION

A. ADVANTAGES

The system shows that an effective mitigation control for brute-force attacks can be incorporated into an inexpensive Arduino-based smart lock without costly biometric devices or cloud connectivity. Experimental data indicate that the lockout system activates effectively and consistently after the third unsuccessful attempt at any attack rate, and that the additional authentication code has little impact on processing time compared with the servo motor's mechanical delay.

B. Limitations

The prototype was tested in the Tinkercad simulation environment rather than on fully assembled hardware; therefore, real-world factors such as electrical noise, keypad debounce time, and servo wear and tear were not included in the current experiments. The system also lacks protection against shoulder surfing, physical interference with the lock box, and firmware password theft, which would require additional security measures outside the scope of this project. A user may be inconvenienced if they enter the wrong password after a set number of tries and a defined cooldown period.

C. Implications

As far as cost-conscious families and student dormitories are concerned, the design provides a practical example of an application of a well-known security concept, the account lockout policy, to the context of affordable embedded hardware. It is reasonable to assume that other cost-effective smart home entry projects may also incorporate the lockout policy.

VII. CONCLUSION AND FUTURE WORK

This work discusses the design and testing of a low-cost smart door security system using an Arduino Uno R3 microcontroller to prevent brute-force attacks in a residential Environment. The developed system uses a 4x4 keypad, a 16x2 LCD, and a servo-controlled latch, along with a failed-attempt counter and a 30-minute lockout, to address a gap identified in the literature review. This is because the reviewed literature describes brute-force vulnerability only conceptually, and intrusion detection systems detect anomalous traffic.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Five experiments verified that the system is capable of accepting correct passwords, rejecting invalid ones, imposing lockout immediately after three wrong attempts irrespective of the speed of attack, and resuming normal function automatically once the waiting period expires, with password checking having practically no impact on performance compared to the mechanical action of the servo. The security analysis has shed more light on which types of attacks, such as brute force and dictionary guess attacks, the lockout mechanism handles. In contrast, others such as shoulder surfing, tampering, and even leaking passwords from the firmware remain difficult challenges in the hardening process and warrant future research. Overall, the research shows that a basic, deterministic lockout strategy can significantly improve the security of low-cost smart locks, providing an easy-to-implement countermeasure that can be adopted both commercially and academically.

Future possibilities in this line of research might include implementation of network connectivity to alert lockout events to a homeowner's phone, use of a second authentication method like an RFID card to reduce shoulder surfing threat, investigation of hashing or encryption of passwords to solve the problem of firmware-based password leaks, and testing of the design in the fully built physical system instead of simulation alone. Comparing the rule-based lockout used in this work with machine learning anomaly-detection techniques used in works like [16,21] could highlight the trade-off between simplicity and sophistication in the door-entry system scenario [16,21].

REFERENCES

1. Zia, M. F., Siddiqua, M., Ouameur, M. A., Bagaa, M., & Turjman, F. (2025). Securing the future: A survey on smart home security in IoT-integrated smart cities. Advances in Networks, 12(1), 1-18
2. Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet of Things 1–2: 81–98.
3. Mclntosh, H. (2026). IoT Security Statistics for 2026: Devices, Botnets, and the New Regulatory Floor.
4. AI, V. (2026). What is IoT security? Risks, best practices & enterprise guide.
5. DeepStrike. (2025). IoT Hacking Statistics 2025: The Definitive Report on Threats, Risks & Regulations.
6. Dexpose. (2026). IoT hacking statistics 2026: Latest trends, attacks & data.
7. Asimly. (2026). The Top Internet of Things (IoT) Cybersecurity Breaches in 2026.
8. SecureIoT.house. (2026). The state of IoT security in mid-2026: Record botnets, a returning malware empire, and a regulatory clock about to start.
9. Swiftlane. (2026). Best fingerprint door locks to buy in 2025.
10. WebProNews. (2026). Smart locks revolutionize home security: AI, biometrics, and $16B market boom by 2033.
11. Digest., C. (2025). How to make an RFID door lock system using Arduino?
12. IB, G. I.-G. (2025). What Is a Brute Force Attack? Types, Tools & Prevention.
13. Ruambo, F. A., Masanga, E. E., Lufyagila, B., Ateya, A. A., Abd El-Latif, A. A., Almousa, M., & Abd-El-Atty, B. (2025). Brute-force attack mitigation on remote access services via software-defined perimeter. Scientific reports, 15(1), 18599.
14. Anderson. (2025). Understanding the benefits of two-factor authentication in smart locks.
15. CoramAI. (2025). Guide to biometric access control systems for secure door locks in 2025.
16. Javed, A., Ehtsham, A., Jawad, M., Awais, M. N., Qureshi, A.-u.-H., & Larijani, H. (2024). Implementation of lightweight machine learning-based intrusion detection system on IoT devices of smart homes. Future Internet, 16(6), 200.
17. Sallay, H. (2024). Designing an Adaptive Effective Intrusion Detection System for Smart Home IoT: A Device-Specific Approach with SDN Deployment. International Journal of Advanced Computer Science & Applications, 15(1).
18. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the internet of things. Electronics, 13(16), 3343.
19. Alshamsi, O., Shaalan, K., & Butt, U. (2024). Towards securing smart homes: A systematic literature review of malware detection techniques and recommended prevention approach. Information, 15(10), 631.
20. Haney, J., Acar, Y., Li, A., & Haney, F. (2025). Survey on Smart Home Users' Security and Privacy Perceptions and Actions: A Device Category Perspective.
21. Oyelakin, A., Sanni, S., Adegbola, I., Salau-Ibrahim, T., Bakare-Busari, Z., & Saka, B. (2025). Novel Machine Learning Approaches for Identifying Attacks in IoT-based Smart Home Environment.
22. Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. Cyber Security and Applications, 3, 100082.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

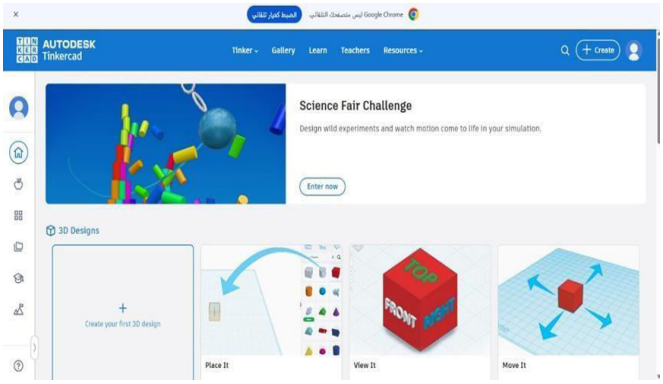
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

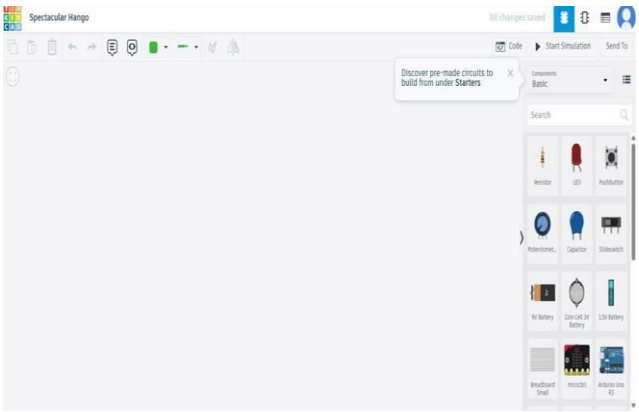
23. Bereziuk, V., Lemeshev, M. S., Bogachuk, V. V., & Duk, M. (2018). Means for measuring relative humidity of municipal solid wastes based on the microcontroller Arduino UNO R3. Paper presented at the Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018.
24. Rajarajeswari, S., & Hema, N. (2022). Smart Door Locking System AI Enabled IoT for Electrification and Connected Transportation (pp. 101-126): Springer.

Appendix-I

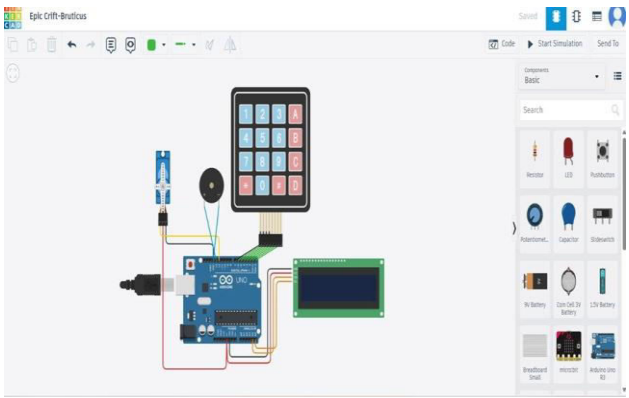
a. Complete Arduino Uno R3 circuit implemented in the Tinkercad simulation environment.



b. Arduino program password authentication and servo control.



c. Program segment illustrating the failed-attempt counter and brute-force lockout mechanism.



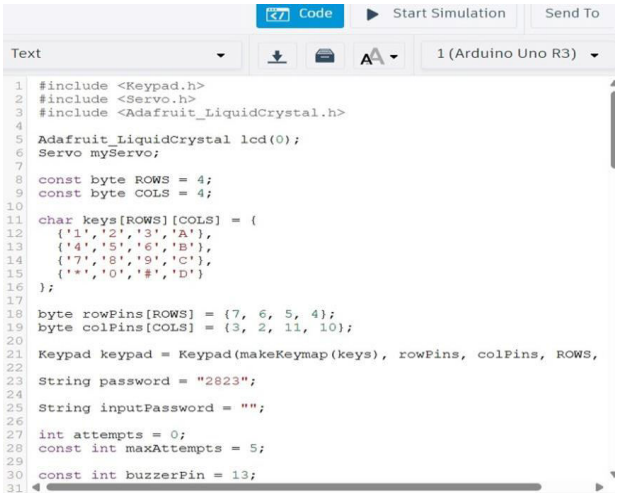
© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

d. The simulation output shows successful authentication and door unlocking.





INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details