Kurra Naga Sai
M. Tech Student, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Dr. TD Sunil
Associate Professor, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

Dr. MN Eshwarappa
Professor & Head of Department, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

A comprehensive review of door lock security systems

Kurra Naga Sai, Dr. TD Sunil and Dr. MN Eshwarappa

DOI: https://doi.org/10.33545/27075923.2024.v5.i1a.61

Abstract
Door lock security systems serve an important role in property protection, privacy, and general security. This comprehensive review examines several types of door lock security systems, including standard mechanical locks, electronic locks, and smart locks. It investigates their mechanisms, strengths and limitations, as well as technological developments. Furthermore, the study examines potential vulnerabilities and security concerns for each type of lock mechanism. It also investigates emerging trends in door lock security, such as biometric authentication and connection with smart home devices. This study seeks to provide insights for bettering the design and implementation of reliable security solutions for residential, commercial, and institutional contexts by analysing the effectiveness and limitations of various door lock security systems.

Keywords: Door lock security, mechanical locks, electronic locks, smart locks, biometric authentication, security vulnerabilities, smart home integration.

1. Introduction
Importance of Door Lock Security
Door lock systems are the primary security measure against unauthorised access, burglary, and intrusion. Door lock security integrity is critical in protecting lives, assets, and sensitive information in a variety of settings, including private houses, business establishments, institutional facilities, and government buildings. The significance of strong door lock security goes far beyond physical barriers; it includes psychological reassurance, privacy protection, and the maintenance of society order. The reasons why door locks security is essential are stated below:

1. Protection of Property and Assets: Door lock security is basically concerned with safeguarding property and valuables from unauthorised access and theft. Whether it's a family home, a retail business, or a corporate office, expensive possessions, secret documents, and merchandise require reliable safety.

2. Ensuring Personal Safety and Privacy: Beyond material goods, privacy and personal safety can only be guaranteed by having secure door locks. A safe door lock gives residents of residential buildings a sense of security and tranquility, enabling them to work, relax, and go about their everyday lives without worrying about being harmed or having their privacy violated. Comparably, door lock security shields personnel, guests, and private data from intrusions and dangers in business and institutional settings**.**

Evolution of door locks technology
Door lock technology has evolved over thousands of years, from simple mechanical mechanisms to complex electrical and smart lock systems, as illustrated below.

1. Early Mechanical Locks
Ancient civilizations, including the Egyptians, Greeks, and Romans, used fundamental mechanical locking devices as early as 2000 BCE. These early locks were primarily made of wooden or metal bolt mechanisms that were activated by keys made of wood, metal, or bone. The pin tumbler lock, believed to have originated in ancient Mesopotamia and Egypt, used pins of varied lengths to prevent unauthorised entry without the proper key.

Corresponding Author:
Kurra Naga Sai
M. Tech Student, Department of Electronics and Communication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

2. Medieval and Renaissance Innovations

The introduction of lever tumbler locks in the 18th century by English inventor Robert Barron marked a significant advancement in lock technology, paving the way for more secure and reliable locking mechanisms.

3. Industrial Revolution and Mass Production

The Industrial Revolution introduced mass production processes, which enabled the widespread availability of low-cost mechanical locks for household and commercial use. Innovations such as interchangeable cores, patented by Linus Yale Sr. in the mid-19th century, revolutionized lock manufacturing by allowing for standardized keying systems and easier rekeying of locks.

Introduction of Electronic Locks

The latter half of the 20th century saw the emergence of electronic lock technology, which replaced traditional mechanical components with electronic circuits and actuators. Electronic locks provided benefits such as keyless entry, programmable access control, and audit trails to track entry and exit activity. Magnetic stripe card locks, launched in the 1970s, were among the early versions of electronic locks, utilizing encoded cards with magnetic stripes to enable access.

Advancements in Smart Lock Technology

In recent decades, smart lock technology has transformed door security by combining electronic components, communication features, and enhanced authentication techniques. Smart locks provide remote access via smartphones, allowing users to lock and open doors from anywhere with an internet connection. Biometric identification methods, such as fingerprint scanning and facial recognition, are becoming more common in smart lock systems, providing more security and convenience.

Integration with IoT and Home Automation

The Internet of Things (IoT) revolution has eased the integration of smart locks into home automation ecosystems, allowing for seamless communication with other smart devices and systems. Smart locks can now be linked to voice assistants, security cameras, and smart home hubs, allowing users to manage access and security remotely using voice commands or mobile apps

2. Literature Review

Shrajna Shetty et al. [1] A review of important papers on door lock systems, including features, technologies, and operation, can help in selecting the optimum system for a specific project area of implementation and making necessary changes to current systems.

Annmary Vadakkan et al. [2] Password-based door lock system is controlled by an Arduino. The password is entered via a keypad. Arduino compares the entered password with the default password. A correct password unlocks the door with the help of a servo motor and shows the status on the LCD. If the password is incorrect, the door remains closed and displays "WRONG PASSWORD" on the LCD. The buzzer will also sound when the password is entered incorrectly for an indefinite number of times.

Mr. Suryasevak Singh et al. [3] An OTP-based door lock system comprises a microcontroller, GSM module, LCD display, keypad, and solenoid lock. The authentication technique used here could be an OTP (four-digit numeric) code generated in an Arduino microcontroller and sent to the registered mobile range through the GSM module (Global System for Mobile Communications), Mobile no will be initiated in the code then as the OTP will be received with help of Keypad Matrix type the OTP then the solenoid lock will open this all procedure will be displayed on I2C LCD.

Prof. Mohammad Nasiruddin et al. [4] OTP and Fingerprint Based Door Locking Systems include two methods for opening a door: utilizing a mobile phone and a fingerprint sensor. The fingerprint module is linked to Arduino. Arduino is used to rotate a motor that is linked to the door latch, and the status is displayed on the LCD. When the user places his or her finger on the fingerprint sensor, if the fingerprints match the saved fingerprints, the Arduino runs the program, which delivers output to the motor driver, and the door opens, When an SMS is sent by the GSM Module to a mobile phone with the inserted SIM, the OTP is entered via the matrix keypad, and the message is verified in the Arduino, which runs the programme and outputs to the motor driver circuit, which is responsible for the motor's rotation and the door opening. The mobile phone wirelessly talks with the GSM module, and Arduino is used to rotate a motor attached to the door latch, displaying the status on an LCD. If we lost our phone like we disused above in OTP based system we can open the door by fingerprint sensor this will increase the stranded level of door lock security system compare to OTP based door lock system.

Sadia Akter Prity et al. [5] The project uses RFID & Keypad Module for door access control, with added security and control provided by the SIM900 module. The 16x2 LCD module is connected to the board for display purposes. After scanning the RFID tag, the user must enter a keycode on the keypad. The SIM900 module allows the user to send messages to control the door lock, with notifications sent via SMS. If the tag matches, the user is notified on the LCD display, and if it doesn't match, they are notified via SMS. The user will also be informed via SMS of any unauthorized attempts to access the door. The use of the SIM900 module enhances the authentication process. It is some more advance mode of password, OTP, OTP & Fingerprint based door lock system but in this if we lost mobile or RFID card then we can't open the door.

Etinosa Noma- Osaghae et al. [6] The iris is a highly reliable physical trait for individual identification, being stable, unique, and different for each eye of the same person. In 1992, Daugman created an effective algorithm for iris recognition using the integro-differential method to detect iris boundaries and 2D Gabor filter for feature extraction.

The door access control system focused on using iris recognition for verification to enhance security and prevent impersonation. The system utilized the ATmega128 chip and an iris scanner to control access to a door, allowing entry only to verified individuals. The embedded chip was programmed in C language using the GNU Compiler and Eclipse as the development platform. The system consisted of an enrollment and verification phase, where users were enrolled by providing their iris pattern for identification. Access was granted only if the provided iris pattern matched the stored information in the database.

The iris will not change for life time if we compare with fingerprints it is difficult to capture our fingerprints as we age because of skin loses elasticity with age. Compare to

fingerprint based door lock system it standees are more in door lock security system.

Sharvani Yedulapuram et al. [7] In face recognition based door lock system uses a Pi camera to capture images of approaching intruders. The Haar cascade algorithm is then used to detect faces in the captured images. The algorithm needs to be trained with positive and negative images to recognize faces. Haar cascades are similar to convolution kernels and are used for real-time face detection. Adaboost machine learning algorithm is used to simplify calculations. If a matching face is detected, the system sends signals to unlock the door. If no match is found, the system keeps the door locked and turns on LEDs. Haar cascade classifier is used to detect single faces in preprocessed images by analyzing features like edges, lines, and center surround. The classifier works in stages, testing windows with different Haar-like features. If a window fails a stage, it is discarded and not tested further. Haar cascade classifiers are known for their fast detection speed.

M. Tseng et al. [8] The proposal suggests a monitoring system for door-opening activities using a single wrist-worn sensor. This system can track upper limb movements during daily tasks, particularly focusing on three key gestures involved in door opening: grasping, rotating, and opening. Data is collected using a 3-axis accelerometer and gyroscope, with four participants performing door opening motions with their right hand, recorded 14 times each. Manual labeling via camera assists in gesture identification, and collected data is wirelessly transferred to a laptop for processing. Raw sensor data undergoes preprocessing with a moving average, followed by event detection and identification of rotation gestures using valley-peak points. The system's performance yields an accuracy of 0.933 and a precision of 0.896.

Koselendra L et al. [9] A smart Wi-Fi door lock system is created using ESP32 CAM and the Blynk App. When someone rings the doorbell, the owner receives a phone notification with a photo of the visitor. Additionally, the owner can remotely unlock the door via the mobile app after confirming the visitor's face recognition. The system utilizes a modified standard shelf with face verification technology. A Windows Forms Application, developed in C#, manages storing, verifying, and unlocking trusted faces. It employs a proprietary API for face verification and an IoT Cloud API to communicate with the Wi-Fi Module and Arduino. The Wi-Fi Module connects to an Arduino Uno, which controls a servo motor for locking and unlocking the door.

Eshwarappa M.N et al. [10] Speaker recognition involves identifying speakers based on their speech signal by extracting features from the speech signal and creating reference models for each speaker. The system uses Mel Frequency Cepstral Coefficients (MFCCs) for feature extraction and explores modeling the excitation source and supra-segmental features for improved recognition. The system can be used for identification or verification, with text-dependent approaches. Two different feature extraction techniques, MFCC and Wavelet Octave Coefficients of Residues (WOCOR), are used, along with modeling techniques like Vector Quantization (VQ) and Gaussian Mixture Modeling (GMM).

Eshwarappa M.N et al. [10] Recent approaches in handwriting recognition focus on textural features and character shape elements, using techniques such as Hidden Markov Models and Support.

Vector Machine features extracted from handwriting images, specifically the VPP vector and HPP vector. The VPP vector represents the sum of gray levels in each column of a handwriting image, indicating variations in gray level distribution. This feature is unique to each user and can vary even within the same user. The HPP vector, which provides information on handwriting variations across the lateral extent, is also considered important. A writer recognition system is created by segmenting individual words from sentences for better performance The DTW distances between users by averaging method are calculated and fused to identify the user. A similar process is used for HPP vectors.

Eshwarappa M.N et al. [10] Multimodal or Multi-biometric systems improve upon the limitations of unimodal systems by integrating multiple sources of information, such as physiological or behavioral characteristics, for enrollment and identification. Integration can occur at the feature, measurement, or score levels, with varying degrees of complexity and effectiveness. The integration process involves combining scores obtained from individual matchers using techniques like Sum rule or Product rule, preceded by score normalization to ensure compatibility. The resulting multimodal biometric system utilizes the strengths of each individual system for improved performance and robustness

Fatih Titrek et al. [11] Biometric Recognition Systems use unique characteristics to automatically verify individuals, with finger vein technology being a popular choice due to its user-friendly and cost-effective nature. The impact of the HVTP (Horizontal and Vertical

Total Proportion) feature extraction algorithm on success rates when combined with fusion techniques is explored in this study. Various techniques like HF(Homomorphic Filter) and PMAD (Perona-Malik Anisotropic Diffusion) are used to improve the quality of finger vein databases, while methods like GLRLM (Gray Level Run Length Matrices and), GLCM (Gray Level Co-occurrence Matrices), SFTA (Segmentation-based Fractal Texture Analysis), HTP (Horizontal Total Proportion), and VTP (Vertical Total Proportion)are used to describe texture features. Combining multiple features can improve the accuracy of finger vein recognition systems. The study identifies two types of finger vein recognition procedures, one focusing on image quality improvement and the other on increasing success rates through new feature vectors or fusion techniques. The study found that using the HVTP feature extraction approach with GLRLM, GLCM, and SFTA features, along with Ensemble and KNN classifiers, resulted in accuracy rates above 95%, making finger vein recognition systems the best among all biometric recognition systems

3. Overview of Mechanical, Electronic and Smart Locks
1. Overview of Mechanical Lock Mechanisms

Mechanical locks are operates based on physical mechanisms that engage or disengage a bolt to secure or release a door. The most popular type of mechanical lock is the pin tumbler lock, which is made up of a set of pins of varied lengths that prevent the lock from rotating without the proper key. When the key is inserted and spun in the lock cylinder, the pins align at the shear line, allowing the lock to open. The varieties of Pin Tumbler Locks and Lever Tumbler Locks are prominent under this category

Strengths
Mechanical locks are inherently resistant to electronic hacking and cyber-attacks, making them suitable for locations where cyber security is a priority. Traditional mechanical locks are generally inexpensive, making them available to a wide range of customers and companies. Mechanical locks provide a reliable and long-lasting level of security.

Weaknesses
Traditional mechanical locks are vulnerable to physical manipulation and unauthorized key copying, lacking advanced features like remote access and audit trails. Despite their durability, they can still be compromised by burglars using techniques like lock picking. While they offer reliability and affordability, users should be aware of their vulnerabilities and take steps to enhance security.

2. Electronic Locks
Electronic locks represent a significant development in door security technology, providing keyless entry, programmed access control, and increased convenience over traditional mechanical locks. These locks use electronic components like keypads, RFID readers, and biometric scanners to permit or deny access to a door. Electronic locks are popular in residential, commercial, and institutional contexts due to their versatility, security features, and ability to integrate with access control systems.

Overview of Electronic Lock Systems
Electronic locks use electronic circuits and actuators to control access to doors, replacing traditional mechanical components. They often include keypads, card readers, or biometric scanners for authentication, eliminating the need for physical keys. These locks can run on battery power or be connected to a building's electrical system. Keycard and keypad-based systems are common, with keycards or key fobs being used to authenticate users, and keypad entry requiring a PIN code. RFID and NFC technologies are frequently used for contactless authentication, allowing for quick and convenient access control.

Advantages
Electronic locks provide keyless entry, which eliminates the need for physical keys and reduces the possibility of unauthorised key duplication. Administrators can use programmable access control to dynamically manage access privileges, granting or revoking access remotely as needed. Electronic locks are compatible with access control systems, allowing for centralised management of many doors and user credentials.

Limitations
Electronic locks may rely on batteries for power, necessitating routine maintenance to assure continuous performance. Hacking and electronic manipulation weaknesses, such as faking RFID signals or exploiting software flaws, constitute a security issue. Electronic locks may be more expensive upfront than traditional mechanical locks, but they provide long-term cost benefits through better security and convenience.

3. Smart Locks
Smart locks are the cutting-edge of door security technology, combining electronic access control, internet connectivity, and enhanced authentication mechanisms. These locks provide exceptional ease, flexibility, and control over access to their homes, workplaces, or other secure areas. Smart locks have grown in popularity in residential, commercial, and institutional contexts due to their ability to interact with smart home ecosystems, give remote access, and boost security.

Connectivity Options
Smart locks can connect to the internet via Wi-Fi, Bluetooth, Zigbee, Z-Wave, or other wireless protocols, depending on the model and manufacturer. Wi-Fi-enabled smart locks offer direct internet connectivity, allowing users to control the lock remotely from anywhere with an internet connection. Bluetooth-enabled smart locks communicate with nearby devices, such as smartphones or smart home hubs, for local control and automation.

Mobile App Integration and Remote Access
Smart locks are usually supported by smartphone apps that enable users to operate and monitor them remotely. These apps allow users to lock and unlock doors, offer temporary access to guests or service providers, and receive real-time notifications about entrance and exit activities. Remote access capabilities give consumers more convenience and flexibility by allowing them to manage access to their property from anywhere with an internet connection.

Table 1: Comparison of different Door lock system of its features and limitations

Sl. No.	Type of Door Lock System	Features	Limitations
1.	Traditional Keypad Locks	Gets information using a number keypad? Basic security feature with code-based authentication.	Restricted functionality and susceptible to shoulder surfing and code guessing. Inflexibility in the way code is managed. Restricted ability to track user access.
2.	RFID (Radio Frequency Identification) Locks:	Key fobs or RFID cards are used to allow access. Quick and easy access without the need for physical keys.	Prone to card theft or cloning. Costly to replace cards that are lost or stolen. Card detection has a limited range and requires close proximity
3.	Biometric Locks	Use voice, handwriting, iris, fingerprint, and finger vein matching identification to grant access. Superior security with distinct biometric information	Possible problems with precision and dependability, particularly during severe weather. Greater initial cost in comparison to other lock types. Restricted ability to hold biometric information for numerous users.
4.	Bluetooth-Enabled Locks	Operated via a Bluetooth link and a smartphone app.	Susceptible to signal interception and Bluetooth hacking.

#			
		Easy remote access and management.	Depends on Bluetooth range and smartphone battery life. Problems with specific smartphone models' or operating systems' compatibility
5.	Wi-Fi-Enabled Locks	Allows for Wi-Fi networking to enable remote access and control. Integration for increased usefulness with smart home systems.	Reliance on Wi-Fi connectivity, which is prone to interference or network failures. Possible security hazards associated with Weaknesses in Wi-Fi networks. Greater power usage in comparison to other kinds of locks
6.	Smart Locks with Voice Control	Control by voice using virtual assistants such as Google Assistant or Alexa. Operates without using hands, adding ease.	Worries about potential illegal voice command access and privacy. Problems with voice recognition accuracy, particularly in noisy settings. Voice commands needs internet access to function.
7.	Multi-factor Authentication Locks	Combines two or more biometric, RFID, or PIN-based authentication techniques. increased security by using several authentication layers	Complexity and potential usability issues in the event that many authentication steps are involved. Using several authentication techniques results in higher integration expenses. An increased risk of user lockout due to misplaced or forgotten login credentials.
8.	Cloud-Connected Locks	Synchronizes with cloud services to enable monitoring and remote access. Enables the centralized administration of several locks. dependence on the internet	Reliance on internet access to provide Monitoring and remote access. Issues with data privacy pertaining to cloud storage. Concerns around downtime and cyberattacks arise from cloud services' vulnerability to cyberattacks.
9.	Integrated Smart Home Security Systems	Integrates complete home security systems with digital door locks. Gives all security devices centralized control and monitoring.	For certain users, the expense and complexity may be prohibitive. Reliance on a single, central system to handle all security requirements. Possible problems with various smart home gadgets not working together

Overall review emphasizes that the emerging trends and technologies in door lock security systems are revolutionizing the way we control access to our homes, businesses, and institutions.

Conclusion
Door lock security systems play a critical role in safeguarding lives, property, and sensitive information in residential, commercial, and institutional environments. Throughout this Comprehensive review, we have explored the evolution of door lock technology, from traditional mechanical locks to advanced electronic and smart lock systems. Have examined the strengths, weaknesses, and vulnerabilities associated with each type of lock system, as well as emerging trends and technologies shaping the future of door lock security which may aid in further research in this area of technology.

References
1. Shetty S, Shetty S, Vishwakarma V, Patil S. Review Paper on Door Lock Security Systems. IEEE International Conference on Convergence to Digital World Quo Vadis (ICCDW); c2020.
2. Vadakkan A, Babu VK, Pappachan C, Sunny A. Door locking using keypad and Arduino. International Research Journal of Modernization in Engineering Technology and Science, 2021 Nov, 03(11).
3. Singh S, Deshmukh SS, Tabhane SS. OTP Based Door Lock System. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).
4. Mohammad, Nasirruddin, Kachhwaha P, Gawande M. IoT and Fingerprint Based Door Looking System. International Journal on Recent and Innovation Trends in Computing and Communication. 2018;6(6):233-235.
5. Prity SA, Afrose J, Hasan MM. RFID Based Smart Door Lock Security System. American Journal of Sciences and Engineering Research, 2021, 4(3).
6. Noma E, Okereke C, Okesola OJ. An Iris Biometric Door Access Control System. 2017 International Conference on Computational Science and Computational Intelligence Design and Implementation.
7. Yedulapuram S, Arabelli R, Mahender K, Sidhardha C, Reddy S. Automatic Door Lock System by Face Recognition. IOP Conference Series: Materials Science and Engineering. 2020;981:032036.
8. Tseng M, Liu K, Hsieh C, Hsu SJ, Chan C. Gesture spotting algorithm for door opening using single wearable sensor. 2018 IEEE International Conference on Applied System Invention (ICASI).
9. Prathapagiri D, Eethamakul K. Wi-Fi Door Lock System Using ESP32 CAM Based on IoT. The International Journal of Analytical and Experimental Modal Analysis, 2021 Jul, 13(7).
10. Eshwarappa MN, Latte MV. Multimodal Biometric Person Authentication using Speech, Signature and Handwriting Features. International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence.
11. Titrek F, Baykan ÖK. Finger Vein Recognition Based on Multi-Features Fusion. Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Konya Technical University, Turkey. Corresponding Author Email: ftitrek@ktun.edu.tr
12. Kiran BL, Jeevan BS, Chandan J, Mohananka C, Vallabh Mahale. Using IoT for door lock security

systems. Undergraduate Student, Dept. Of Computer Science & Engineering, Jyothy Institute of Technology, Visvesvaraya Technological University, Thataguni Post, Bengaluru, India. Undergraduate Student, Visvesvaraya Technological University, Thataguni Post, Bengaluru, India.

13. Nehete PR, Chaudhari JP, Mahajan JT, Rane KP. Literature survey on door lock security systems. Int J Comput Appl. 2016 Nov;153(2):13. Dept. of ETC, Godavari College of Engineering, Jalgaon, India – 425001.

14. https://www.slideshare.net/AmreenShaikh60/evolution-of-smart-home-lockspdf