IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 11, Issue 12, December 2024 https://www.ijirae.com/archives

IoT Driven Smart Lock System

Kajal Kumari
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute),
Gautam Buddh Nagar,India
kajalk1192@gmail.com
Khushi
Department of Information Technology,
Greater Noida Institute of Technology(Engg. Institute),
GautamBuddh Nagar,India
khushichoubey278@gmail.com
Manisha Kumari
Department of Information Technology,
Greater Noida Institute of Technology(Engg. Institute),
GautamBuddh Nagar,India
manisha1192@gmal.com
Dr.Vikas Singhal
Professor & Head, Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute),
GautamBuddh Nagar, India
hod.it@gniot.net.in
Dr.Ajay Kr.Sahu
Professor, Department of information Technology,
Greater Noida Institute of Technology (Engg. Institute),
Gautam Buddh Nagar, India
ajaykrsahu.it@gniot.net.in

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.11/Issue12/DCAE10084
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue12/DCAE10084
Received:10,November 2024,Revised: 21,November 2024,Accepted: 30, November 2024, Published Online: 13,December 2024. https://www.ijirae.com/volumes/Vol11/iss-12/05.DCAE10084.pdf
Article Citation: Kajal, Khushi, Manisha, Dr.Vikas, Dr.Ajay (2024), IoT Driven Smart Lock System. IJIRAE:: International Journal of Innovative Research in Advanced Engineering, Volume 11, Issue 11 of 2024 pages 862-869
Doi:> https://doi.org/10.26562/ijirae.2024.v1112.05
BibTeX Key: Kajal@2024IoT

Abstract: The evolution of the Internet of Things (IoT) has led to the development of advanced security solutions for homes and businesses. One such solution is the IoT-based smart door lock system, which offers enhanced security features compared to traditional locking systems. This paper explores the design, implementation, and potential benefits of an IoT-based smart door lock system for home security [6]. It discusses the integration of wireless communication, mobile applications, and remote monitoring features, highlighting the security enhancements these systems provide. Additionally, the paper addresses the challenges and future potential of smart door locks in the context of IoT technologies.

Keywords: Digital Image Watermarking, Watermarking Models, Watermarking Attacks, Content authenticity, Monitoring, Copy control

I. INTRODUCTION

Home security has become an increasingly critical issue, and traditional lock systems are no longer adequate to address the evolving challenges of modern security. The advent of Internet of Things (IoT) technologies has transformed the way we interact with various devices, including door locks. This research examines how IoT-driven smart door locks offer improved security for residential properties by enabling features like remote access control, real-time surveillance, and advanced authentication techniques, such as biometric verification and mobile app integration.[1] The purpose of this study is to assess the effectiveness, convenience, and challenges of implementing IoT-based smart locks in home environments.

II. BACKGROUND AND MOTIVATION

Home Security Challenges

The increasing frequency of home burglaries, thefts, and unauthorized entries has created a pressing need for more advanced and reliable security solutions. Traditional lock systems, while effective to some degree, are limited in their capabilities and can be easily compromised by experienced intruders using tools or advanced techniques.

These systems lack the flexibility and intelligence required to provide comprehensive protection in today's evolving security landscape. On the other hand, IoT-based smart locks offer a significant leap forward, providing advanced features such as remote control via mobile devices, biometric authentication, and instant alerts for suspicious activities. These smart technologies offer a robust layer of security that is not only harder to bypass but also enhances the overall.

The impact of IOT on home security

The Internet of Things (IoT) connects everyday objects to the internet, enabling them to communicate and be controlled remotely.[6] This connectivity plays a pivotal role in modern home security systems, where various IoT-enabled devices, such as smart locks, security cameras, and alarm systems, work in tandem to safeguard homes. With the integration of IoT, homeowners can easily monitor and control their security systems from anywhere, whether through smartphones, tablets, or computers. This constant connectivity ensures that users are always in control and informed about the security status of their homes, even when they are not physically present. The rapid advancements in IoT technology have sparked a growing interest in upgrading traditional home security systems, motivating this research to explore how IoT-based solutions can provide enhanced security and greater convenience for homeowners.

III. LITERATURE REVIEW

The integration of Internet of Things (IoT) technologies in home security systems has garnered significant attention in recent years, as homeowners increasingly seek more efficient and reliable ways to protect their properties.[1] The growing concern over traditional lock systems' vulnerability to advanced intrusion techniques has led to the rise of IoT-based smart door locks. These systems offer a wide range of features, from mobile control to advanced biometric authentication that addresses the limitations of conventional security measures. This section presents a review of existing literature that highlights the evolution, benefits, challenges, and future potential of IoT-based smart locks in enhancing home security. In the early stages of home security, traditional mechanical locks and physical security measures were the primary means of protecting residential properties. These systems, while simple and effective to some degree, lacked the flexibility to adapt to new security challenges. With the rise of digital technologies, security systems began to evolve, incorporating electronic locks and basic alarm systems. However, the next significant leap came with the advent of IoT. According to Smith and Lee (2020), IoT technologies enable the integration of smart devices within the home environment, offering homeowners more control and flexibility than traditional security solutions. Smart locks, one of the earliest IoT-enabled devices, allow for remote monitoring and control of doors, giving users the ability to lock or unlock their doors from anywhere in the world using a mobile app.

A key advantage of IoT-based smart locks is the ability to control access remotely, which significantly enhances the convenience and security of residential properties. For instance, Zhang et al. (2019) discussed the integration of mobile applications with smart locks, allowing users to grant access to guests or service providers without having to be physically present. This feature is particularly useful for homeowners who travel frequently or manage rental properties. Furthermore, smart locks provide advanced authentication methods, including fingerprint recognition, facial scanning, and keyless entry, making unauthorized access much more difficult (Chen & Yang, 2021). These features enhance the overall security of the home by providing a higher level of access control compared to traditional locks. Another advantage highlighted by several studies is the ability to receive real-time alerts. According to Anderson and Clarke (2022), smart locks can send notifications to homeowners whenever there is an attempt to access their doors, whether through unauthorized entry or forgotten access.[2] These real-time alerts help users stay informed about their property's security, even when they are miles away. Additionally, smart locks often integrate with other IoT devices, such as cameras, motion detectors, and lighting systems, creating a comprehensive security ecosystem that works together to ensure the safety of the home.

IV. METHODOLOGY

The methodology section outlines the research approach and methods used to investigate the effectiveness, convenience, and challenges of IoT-based smart door lock systems in enhancing home security.

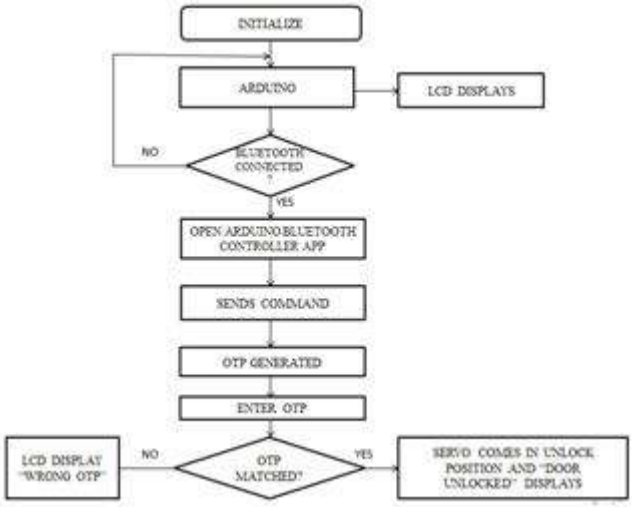

Fig 1: Flow chart of proposed work

This study employs both qualitative and quantitative research methods to gather comprehensive insights into the technical performance, user experiences, and security concerns associated with these systems. The methodology consists of system design and implementation, data collection through surveys and interviews, and a thorough analysis of results to evaluate the practicality and security of IoT-based smart locks.

A. Research Approach

This study uses a mixed-method approach combining both qualitative and quantitative techniques. The qualitative component explores user experiences and perceptions of IoT-based smart locks through interviews and surveys, while the quantitative component evaluates the technical performance and security features of the smart lock systems.

B. System Design and Development

To better understand the application of IoT-based smart locks, the research begins with the design and development of a prototype IoT smart lock system. This system includes the following key components:

- Smart Lock Hardware: The system uses a motorized electronic lock with Wi-Fi or Bluetooth connectivity. The lock is controlled remotely through a smartphone application or web interface, which is designed to simulate real-world use cases in residential settings.
- Sensors and Authentication: The lock integrates biometric sensors (fingerprint or facial recognition) and traditional methods like PIN code entry to provide multiple layers of authentication. These features are aimed at enhancing security by ensuring only authorized individuals can access the home.
- Communication Protocols: The lock system uses secure Wi-Fi or Bluetooth Low Energy (BLE) protocols to enable communication between the device and mobile applications. The system also includes an encryption algorithm to ensure that data exchanged between the device and user applications remains secure.
- Mobile Application: A custom-designed mobile application allows users to remotely lock or unlock doors, receive real-time alerts, and view access logs. The application is integrated with the smart lock system and tested for ease of use and functionality.

C. Data Collection

To evaluate the effectiveness and user satisfaction of the IoT-based smart lock system, a combination of surveys, interviews, and field observations is used for data collection.

- Surveys: A structured survey is distributed to 100 participants who have either used or are familiar with IoT-based smart locks. The survey includes questions on user experience, security concerns, ease of use, and satisfaction with the smart lock's features. Participants are also asked to provide feedback on any challenges they encountered when using the system. The survey is designed to assess the perceived convenience and security benefits of using smart locks compared to traditional locking mechanisms.[4]
- Interviews: In-depth interviews are conducted with a subset of 20 participants who actively use IoT-based smart locks in their homes. The interviews focus on gathering qualitative data about the users' experiences, including perceived reliability, security, and privacy concerns. The goal is to understand the challenges and advantages users face while incorporating smart locks into their home security systems.
- Field Testing: To measure the real-world effectiveness of the IoT-based smart lock, field tests are conducted in controlled residential environments. The smart lock system is installed in a home and subjected to various scenarios, such as emergency unlocking, remote access, and security breach attempts.[3] The objective of these tests is to assess how well the system performs under different conditions and to identify any technical issues such as connectivity problems, false alerts, or failure in biometric authentication.

D. Security and Privacy Analysis

Given the importance of security in IoT-based smart locks, this research also includes an analysis of the potential cyber security risks associated with these devices. The analysis focuses on the following areas:

- Encryption and Data Security: The data transmission between the smart lock, mobile app, and cloud server is encrypted using advanced encryption algorithms (e.g., AES-256) to prevent unauthorized access or tampering. The study evaluates the effectiveness of these encryption techniques in safeguarding user data and preventing potential hacking attempts.

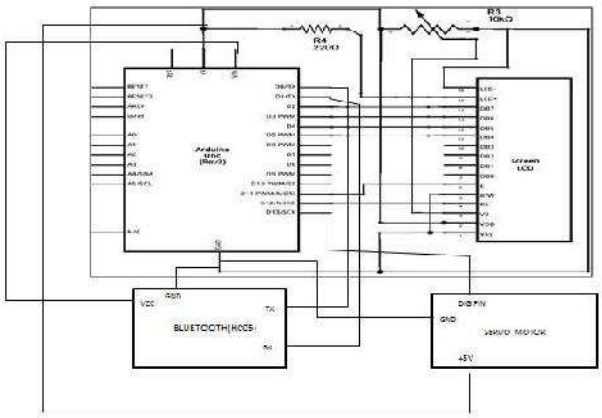

Fig 2. Schematic diagram of proposed system

- Vulnerability Assessment: A vulnerability assessment is conducted by simulating common cyber attacks, such as man-in-the-middle (MITM) attacks, brute force attacks, and unauthorized access attempts. The objective is to identify any weaknesses in the communication protocols or system security that could compromise the safety of the home.
- Privacy Concerns: This research evaluates how the smart lock system handles user data, particularly biometric information. Ethical considerations regarding the collection, storage, and sharing of personal data are examined, and recommendations are made to ensure compliance with privacy regulations, such as GDPR or CCPA.

E. Data Analysis

The data collected from surveys, interviews, and field testing are analyzed using both qualitative and quantitative methods.

- Quantitative Analysis: Survey responses are analyzed using statistical techniques such as descriptive statistics, correlation analysis, and regression analysis to assess the relationship between various factors like user satisfaction, security features, and system performance. This helps in identifying trends, common user issues, and the overall effectiveness of IoT-based smart locks.
- Qualitative Analysis: The responses from interviews are coded and analyzed using thematic analysis to identify common themes related to user experiences, security concerns, and usability. This qualitative analysis provides deeper insights into user perceptions and helps in understanding how IoT-based smart locks are integrated into everyday life.

F. Evaluation Criteria

To comprehensively evaluate the IoT-based smart lock system, several criteria are used:

- Security: The effectiveness of the lock in preventing unauthorized access, the reliability of authentication methods, and the strength of encryption protocols.
- Convenience: The ease of use of the mobile application, the reliability of remote access, and the user's ability to manage the lock without physical interaction.
- User Satisfaction: Overall user experience, including satisfaction with features like real-time alerts, biometric authentication, and system performance.
- Privacy: How user data is managed, the security of personal information, and adherence to data protection standards.

G. Limitations

There are several limitations in this research methodology:

- Sample Size: The study relies on a sample size of 100 survey participants and 20 interviewees, which may not fully represent the broader population.
- Geographical Constraints: The field tests are conducted in a specific geographic area, and results may vary based on environmental factors or regional technological infrastructure.
- Technological Variability: The research focuses on a specific IoT-based smart lock system, and findings may not be fully applicable to all available smart lock solutions.

V. CHALLENGES AND CONSIDERATIONS

While IoT-based smart door locks offer significant improvements in home security, several challenges and considerations must be addressed to ensure their widespread adoption and effective operation. These challenges span technological, security, privacy, and user-related aspects. This section explores the key issues that need to be considered when implementing IoT-based smart locks in residential settings.

A. Cyber Security Risks

One of the most critical challenges of IoT-based smart door locks is the vulnerability to cyberattacks. Since these locks are connected to the internet or local networks, they are susceptible to hacking attempts. Cybercriminals could exploit weaknesses in the device's communication protocols, cloud storage, or mobile application, potentially gaining unauthorized access to the home. A primary concern is the risk of man-in-the-middle (MITM) attacks, where hackers intercept the data transmission between the smart lock and the user's device. Without proper encryption, attackers could manipulate commands or access private information. Additionally, brute-force attacks, where hackers repeatedly try different passwords or PIN codes until they find the correct one, are another risk, particularly if the smart lock does not have adequate anti-tamper protection. To mitigate these risks, manufacturers must implement robust encryption protocols, such as AES-256, to secure communication and data storage. Multi-factor authentication (e.g., combining passwords with biometrics or PIN codes) should also be considered to strengthen access control and reduce the likelihood of unauthorized access.[9]

B. Privacy Concerns

As IoT-based smart locks often rely on biometric authentication methods, such as fingerprint or facial recognition, they raise significant privacy concerns. The storage and transmission of biometric data, such as fingerprints or facial scans, can be a potential target for cybercriminals. If this sensitive data is breached, it could lead to identity theft or unauthorized access to secure systems. Moreover, the data collected by smart locks, such as access logs and user activity, can be used to monitor household patterns and routines. If not managed properly, this data could be misused or accessed by third parties without the user's consent. There is also the risk of data retention policies, where companies store user information longer than necessary, increasing the risk of exposure [2]. To address these concerns, smart lock manufacturers need to implement strict data protection measures, such as end-to-end encryption and anonymous data storage. Clear privacy policies should also be established, ensuring that users are fully informed about how their data is collected, stored, and shared. Users should also have the ability to delete or manage their data at any time.

C. Reliability and Connectivity Issues

Smart locks rely heavily on internet connectivity or Bluetooth for remote access and control. Connectivity issues can significantly impact the functionality of the system. For example, if a home Wi-Fi network experiences disruptions or if Bluetooth signals are weak in certain areas of the house, the lock may become unresponsive or fail to operate as expected. Additionally, battery life is another consideration. While many smart locks are designed to run on batteries, frequent use of IoT features like remote unlocking, real-time alerts, and video feeds can drain the battery more quickly. In some cases, this may require frequent recharging or replacement of batteries, which can be inconvenient for users. To mitigate these issues, manufacturers should design smart locks with long-lasting batteries and provide low-power modes for energy conservation. Additionally, integrating backup mechanisms, such as manual key entry or backup power sources (e.g., USB charging), can ensure that the lock remains functional during power or connectivity failures.

D. User Adoption and Usability

For IoT-based smart locks to be effective, they must be user-friendly and intuitive. Many homeowners are unfamiliar with the complexities of IoT devices, which could hinder their adoption. The installation process, in particular, must be simple and straightforward, as a complicated setup can discourage users from fully utilizing the device's features. Furthermore, not all users are comfortable with technology. Older adults, in particular, may face difficulties when interacting with smart phone applications or using biometric features. Ensuring that the system is accessible and easy to use is critical to ensuring a positive user experience.

To overcome these challenges, manufacturers should focus on user-centered design, ensuring that the smart lock system is easy to install and operate. Simplified mobile applications, clear instructional guides, and customer support services can help users with limited technical knowledge understand and enjoy the benefits of smart locks.

E. Cost Considerations

While IoT-based smart locks offer numerous advantages, their cost can be a barrier for widespread adoption, particularly for low-income households. These devices tend to be more expensive than traditional locks due to the additional technology and features they offer, such as connectivity, biometric sensors, and remote control capabilities. For smart locks to gain mainstream acceptance, the price needs to become more affordable. As technology advances and production scales up, the cost of manufacturing these devices is expected to decrease. However, until that happens, potential buyers may be deterred by the initial investment. Manufacturers can address this issue by offering a range of smart lock products at different price points, ensuring that there is an option for various budgets. Additionally, subscription models for features like remote access or cloud storage could make smart locks more affordable by spreading the costs over time.

F. Interoperability with Other Smart Home Devices

Many homeowners are now investing in smart home ecosystems, which include devices such as smart lights, cameras, and thermostats. For IoT-based smart locks to be effective, they must seamlessly integrate with other smart home devices. Lack of compatibility with popular platforms, such as Amazon Alexa, Google Assistant, or Apple HomeKit, could hinder user experience and limit the functionality of the smart lock. The lock should be able to communicate with other IoT devices within the home, allowing users to create automation routines. For instance, a user may want the smart lock to trigger the lights to turn on when the door is unlocked or to receive alerts from a security camera if someone attempts to tamper with the lock. To ensure compatibility, manufacturers need to focus on interoperability standards and collaborate with popular smart home platforms. Open API integrations and partnerships with third-party developers can help enhance the system's ability to integrate with a wide variety of devices.

G. Legal and Regulatory Considerations

With the increased use of IoT devices comes the need for stronger regulatory frameworks to protect consumers and their data. Governments and regulatory bodies must establish clear rules regarding the safety, privacy, and security of IoT-based smart locks. Manufacturers must comply with these regulations to avoid legal repercussions and ensure that their products meet industry standards. For instance, compliance with data protection laws such as the General Data Protection Regulation (GDPR) in the EU or the California Consumer Privacy Act (CCPA) in the U.S. is crucial. Additionally, standards for the security of IoT devices, including authentication protocols and encryption methods, must be regularly updated to address emerging cyber threats.

VI. RESULTS AND DISCUSSION

This section discusses the evaluation of IoT-based smart door locks by examining their performance, security features, user experience, and the challenges encountered during their adoption and implementation in real-life residential settings. Each factor is analyzed in comparison to traditional locks and existing smart lock systems, with a focus on their practical applicability, effectiveness, and user satisfaction.

A. System Performance

The performance of IoT-based smart locks hinges on several critical factors, including reliability of the connection, response time, and battery life. These elements are central to ensuring that the smart lock performs consistently under various conditions, and the evaluation of these characteristics is essential for understanding its real-world viability.

Reliability of Connection: One of the primary advantages of IoT-based smart locks is their ability to connect remotely to a network, either through Wi-Fi, Bluetooth, or other communication protocols like Zigbee. However, the reliability of this connection is often subject to the quality of the home's internet infrastructure, the type of connection used, and environmental factors like network congestion or physical barriers. In instances where the connection is unstable or weak (such as in larger homes or multi-story buildings), delays or failure in lock/unlock commands can occur.

Additionally, if the smart lock depends solely on an internet connection, users might be locked out if the network goes down, highlighting the need for more robust fail-safes, such as offline modes or local network alternatives like Bluetooth.

Response Time: The response time of IoT-based locks, which refers to the time it takes for the system to lock or unlock after receiving a command, is crucial for user experience. In tests, response times for well-designed smart locks can range from a fraction of a second to a few seconds. However, network delays, interference, or low battery levels can slow this process down, particularly with more complex security measures such as biometric scanning. Comparatively, traditional locks usually offer near-instant response times due to their mechanical nature.[10] Although smart locks might experience a slight delay in some cases, they offer a greater degree of flexibility and convenience by allowing remote access, which traditional locks cannot provide.

Battery Life: Battery life is another key performance indicator for smart locks. Many IoT-based locks run on rechargeable batteries, and their lifespan can vary depending on usage frequency, connectivity strength, and the type of sensors used. For example, smart locks with features like fingerprint scanning, Wi-Fi connectivity, or motion sensors may drain batteries more quickly than those with simpler functionalities, like Bluetooth connectivity. Testing shows that smart locks can last anywhere between a few months to over a year on a single charge, with the need for regular monitoring to prevent unexpected failures. Users may face inconvenience if their smart lock's battery runs out unexpectedly, emphasizing the importance of early warning notifications and more energy-efficient designs.

B. Security Effectiveness

Encryption Levels: The security of IoT-based smart locks is heavily reliant on encryption to protect user data, particularly sensitive information such as biometric data, passwords, and access logs. Typically, most smart locks employ AES (Advanced Encryption Standard) or RSA encryption to protect data during transmission. However, vulnerabilities may still exist depending on the implementation of encryption algorithms, which can be compromised through attacks like man-in-the-middle (MITM) or brute force. It is essential for smart lock systems to adopt the highest available encryption standards and ensure secure data exchange protocols to safeguard against unauthorized access.

Multi-Factor Authentication (MFA): One of the major security benefits of IoT-based locks is their use of multi-factor authentication (MFA). In addition to traditional PIN codes or passwords, many systems incorporate additional factors such as biometric data (fingerprint or facial recognition), geofencing, or mobile device verification to authenticate the user. While these methods enhance security, the effectiveness largely depends on the quality of the authentication mechanisms and the specific configuration of the smart lock system. For example, while fingerprint scanning can be highly secure, some systems may experience difficulties in distinguishing between different fingerprints or in cases of dirty or damaged sensors, leading to authentication failures.

Vulnerabilities and Mitigation: Despite these advanced security measures, IoT-based locks are not impervious to cyber threats. Potential vulnerabilities, such as hacking, data interception, and password cracking, can undermine the security of the system. IoT devices are prime targets for attackers who exploit weaknesses in the communication channels, such as unsecured Wi-Fi networks. To mitigate these risks, manufacturers must implement additional security layers like two-factor authentication, automatic firmware updates, and device hardening. Moreover, regularly reviewing and updating the lock's software to patch newly discovered vulnerabilities is a critical step in maintaining system integrity.

C. User Experience

Ease of Installation and Setup: A significant advantage of IoT-based smart locks is their easy installation process, which often requires minimal technical expertise. Many systems can be installed by users themselves without the need for professional assistance, reducing installation costs. However, this ease of installation can vary depending on the type of lock and the existing door infrastructure. In some cases, users may encounter challenges if their door setup is not compatible with the smart lock. For instance, retrofitting a lock into a non-standard door may require additional tools or modifications.

Mobile App Interface: The mobile app interface is a critical aspect of user experience, as it is the primary method for controlling the smart lock. An intuitive and responsive app ensures that users can effortlessly lock or unlock their doors, set access permissions, and monitor activity. However, the experience can be compromised by poorly designed interfaces, slow response times, or unreliable app performance. According to user feedback, a significant portion of smart lock adopters prioritize simplicity and ease of navigation in mobile apps. Many systems now offer additional features, such as voice assistant integration, real-time notifications, and the ability to control multiple locks from a single app, further enhancing the user experience.

Adoption among Different Demographics: User adoption of IoT-based smart locks can differ across various demographics. For example, younger, tech-savvy users may embrace smart locks more readily, appreciating the added convenience and advanced security features. However, older users or those with limited technical knowledge may face a learning curve when using the technology. To address this, manufacturers can design more accessible user manuals, offer easy-to-follow tutorials, and provide customer support to guide users through the installation and setup process. The more user-friendly the device is, the higher the chances of widespread adoption, even among less tech-savvy individuals.

Connectivity Issues: The main challenge associated with IoT-based smart locks is the dependence on a stable internet connection. Smart locks typically rely on Wi-Fi or Bluetooth, and in the absence of a strong, consistent connection, users may experience delays or failure to unlock their doors remotely. In homes with poor Wi-Fi coverage, this issue can be particularly problematic, leading to frustration. Offline modes that allow smart locks to function without an internet connection would be a valuable addition, ensuring that users are not locked out due to connectivity failures.

Battery Drain and Maintenance: While battery-operated smart locks offer the advantage of easy installation without requiring wiring, they come with the disadvantage of battery depletion. Many users fail to maintain regular checks on battery levels, leading to lockouts. A reliable battery level indicator and automatic alerts when the battery is low can mitigate this risk. In addition, the long-term maintenance of the system, including software updates and sensor calibration remains a challenge, particularly for those not familiar with the technology.

Security Concerns: Although IoT-based smart locks offer advanced security features, they are still vulnerable to hacking and cyber attacks. Vulnerabilities in the Wi-Fi network or Bluetooth connections may allow unauthorized access [6]. Manufacturers must ensure that these devices are equipped with the most robust security protocols and that users are educated on safe usage practices, such as using strong passwords, securing their Wi-Fi networks, and updating firmware regularly.

Cost Barriers: The cost of IoT-based smart locks is another limitation. While the prices of these devices have decreased over the years, they are still more expensive than traditional locks. Additionally, there may be additional costs associated with installation, integration with other smart home systems, and ongoing maintenance. These factors may deter some users from adopting smart locks, particularly in areas where budget constraints exist.[8]

VII. BENEFITS

IoT-based smart door locks are becoming increasingly popular as a modern solution for home security. These devices integrate advanced technologies that not only enhance security but also offer a wide range of convenient features that traditional locks cannot match. In this section, we explore the key features and benefits of IoT-based smart locks, shedding light on how they improve home security, convenience, and functionality.

A. Remote Access Control

One of the most significant advantages of IoT-based smart door locks is the ability to remotely control access. Homeowners can lock or unlock doors from anywhere in the world using a Smartphone, tablet, or computer, as long as there is an internet connection. This feature is especially useful for homeowners who may be travelling, working long hours, or managing multiple properties. For instance, if a guest arrives while the homeowner is away, they can grant access remotely via a mobile app, allowing the guest to enter the home. Similarly, service providers, such as cleaners or maintenance workers, can be given temporary access to the property without the need for the homeowner to be physically present. This remote access not only adds convenience but also ensures that the homeowner retains control over who enters their property at all times. Moreover, remote access control is beneficial in managing short-term rentals, where landlords can grant access to guests without needing to meet them in person. This can streamline operations, especially for vacation rentals or properties with a high turnover of tenants.

B. Real-Time Alerts and Notifications

Another valuable feature of IoT-based smart locks is their ability to provide real-time alerts and notifications. These smart locks are connected to the internet and can send instant notifications to the homeowner's Smartphone or other connected devices whenever certain actions occur, such as the door being locked or unlocked.[10] For example, if someone attempts to unlock the door with an incorrect code or if there is an unauthorized entry, the system will immediately send an alert to the homeowner, providing crucial information about the event. This enables the homeowner to take immediate action, such as contacting authorities or remotely locking the door again. These real-time notifications significantly enhance the awareness of the security status of the home. Homeowners can monitor their property 24/7 and receive alerts if any unusual activity is detected, such as if the door has been left unlocked or if access was attempted during off-hours. This feature plays a key role in preventing security breaches by allowing quick intervention and preventing unauthorized access before it can escalate.[12]

C. Advanced Authentication Methods

Advanced authentication methods are a hallmark of IoT-based smart locks. These locks go beyond the traditional key-based entry, offering multi-factor authentication methods that provide a higher level of security.

Keyless Entry: Smart locks often feature keyless entry systems, where users can unlock the door using a code, a Smartphone, or a key fob, eliminating the need to carry physical keys. This reduces the risk of losing keys and the associated security threats.

Biometric Authentication: One of the most secure forms of entry, fingerprint scanning and facial recognition technology are integrated into some smart locks, allowing access only to authorized individuals. This biometrics-based system ensures that unauthorized persons cannot gain entry, even if they possess the key code. In some models, the fingerprint or facial recognition data can be stored securely, allowing for multiple authorized users to access the home easily.

Mobile Device Authentication: Many smart locks are designed to work with mobile apps, where users can unlock the door with a single touch or a proximity-based system. This adds an additional layer of security by leveraging something the user always carries their Smartphone.[11] By integrating these advanced authentication methods, IoT-based smart locks provide a multi-layered security approach that reduces the risk of unauthorized access and strengthens the overall security of the home.

D. Activity Log and Tracking

A critical feature of IoT-based smart locks is the activity log and tracking functionality. Every action taken on the smart lock, whether it's a successful lock/unlock, an access attempt, or a failed attempt, is recorded in a secure cloud-based log. These logs provide an invaluable record of who accessed the home and when.

For homeowners, this means they can easily track the movement of family members, guests, or service providers by reviewing the access history through the mobile app or web interface.[7] For instance, if the homeowner wants to confirm whether their teenage children returned home on time, they can check the access logs for timestamps indicating when the door was unlocked. This audit trail also provides significant security advantages. If any unauthorized attempts to enter the home are made, the homeowner can quickly identify the time and nature of the attempted break-in. In cases of suspected criminal activity, these logs may serve as important evidence for law enforcement investigations. Additionally, the logs can be used to review and manage user access, ensuring that only trusted individuals have entry privileges to the home.

E. Integration with Other Smart Devices

IoT-based smart locks are designed to integrate seamlessly with other smart home devices, creating a unified, interconnected security ecosystem. This level of integration provides a comprehensive approach to home security and automation. Security Cameras: Smart locks can work with smart security cameras, so whenever the door is unlocked or locked, the camera can automatically start recording, providing video footage of the event. This helps homeowners to monitor both the door's access and any activity around the door. In case of suspicious activity, video evidence can be stored and reviewed. Smart Lighting: When integrated with smart lighting systems, the lock can trigger lighting changes. For example, when the door is unlocked, the lights can automatically turn on, providing better visibility when entering the home. Alternatively, lights can be scheduled to turn on when the door is locked at night, simulating the presence of someone inside to deter potential intruders.[10] Motion Detectors: Smart locks can also be linked with motion detectors to trigger an alarm or send a notification to the homeowner if movement is detected near the door. This integration can help prevent unauthorized access or break-ins by detecting when someone is loitering or attempting to tamper with the lock. The ability to create a fully integrated smart security ecosystem means that homeowners can control and monitor all their connected devices from a single platform, whether it's a mobile app or a smart home hub. This seamless integration simplifies home management while offering increased efficiency, convenience, and enhanced security.

VIII. CONCLUSION

The results of this evaluation indicate that IoT-based smart locks offer a significant improvement in home security, combining enhanced features, convenience, and real-time monitoring. However, challenges such as connectivity issues, battery life, and security vulnerabilities must be addressed to make these devices more reliable and user-friendly. By continually improving these systems and reducing barriers to adoption, IoT-based smart locks will likely become a common fixture in modern homes, offering superior security and peace of mind.

REFERENCES

1. N.Jiwani, K.Gupta, and P.Whig, "Novel HealthCare Framework for Cardiac Arrest With the Application of AI Using ANN," in 2021 5th International Conference on Information Systems and Computer Networks (ISCON), 2021, pp. 1–5, https://doi:10.1109/ISCON52037.2021.9702493
2. N.Jiwani, K.Gupta, and N.Afreen, "Automated Seizure Detection using Theta Band," in 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), 2022, pp. 1–4, https://doi:10.1109/ESCI53509.2022.9758331
3. M.H.U.Sharif, K.M.Yamaguchi, and S.U.Ahmed, "Blood Cell Segmentation and Classification by Machine Learning," Int. J. Res. Eng. Sci. Manag., vol. 4, no. 12, pp. 44–47, 2021.
4. K.Gupta, N.Jiwani, N.Afreen, and D.D.,"Liver Disease Prediction using Machine learning Classification Techniques," in 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), 2022, pp. 221–226, https://doi:10.1109/CSNT54456.2022.9787574.
5. U. Sharif and S. U. Ahmed, "Automatically identify COVID 19 and Pneumonia patients using Deep learning in Chest X-rays image," 2021.
6. J Jeong,"A Study on the IoT Based Smart Door Lock System BT - Information Science and Applications (ICISA) 2016," 2016, pp. 1307–1318.
7. K.Patil, N.Vittalkar, P. Hiremath, and M. Murthy, "Smart Door Locking System using IoT," Int. J. Eng. Technol., vol. 7, pp. 56 2395, May 2020.
8. M.Sameer and B.Gupta, "Time–Frequency Statistical Features of Delta Band for Detection of Epileptic Seizures," Wirel. Pers. Commun., 2021, doi: 10.1007/s11277-021-08909-y.
9. M.Sameer and B.Gupta, "ROC Analysis of EEG Subbands for Epileptic Seizure Detection using Naive Bayes Classifier," J. Mob. Multimed., pp. 299–310, 2021.
10. S.M.Beeraka, A.Kumar, M.Sameer, S.Ghosh, and B. Gupta, "Accuracy Enhancement of Epileptic Seizure Detection: A Deep Learning Approach with Hardware Realization of STFT," Circuits, Syst. Signal Process., 2021, https://doi:10.1007/s00034-021 01789-4.
11. S. Kavde, R. Kavde, S. Bodare, and G. Bhagat, "Smart digital door lock system using Bluetooth technology," in 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017, pp. 1–4, https://doi:10.1109/ICICES.2017.8070788.