Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4, 697-708
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i4.1446

A comprehensive investigation of an LTE-enabled smart door system using the Arduino UNO

Nameer Hashim Qasim[1*], Fakher Rahim[2], Nataliia Bodnar[3]
[1]Cihan University Sulaimaniya Research Center (CUSRC), Cihan University Sulaimaniya, Sulaymaniyah 46001, Kurdistan Region, Iraq; nameer.qasim@sulicihan.edu.krd (N.H.Q.)
[2]Department of Medical Laboratory Technologies, Alnoor University, Mousl, Nineveh 41012, Iraq; Fakher.karim@alnoor.edu.iq (F.R.)
[3]Al-Rafidain University College, Department of Quality Assurance, Baghdad 10064, Iraq; natalia.bodnar@ruc.edu.iq (N.B.)

Abstract: Traditional residential security systems frequently lack remote access and real-time reaction capabilities, necessitating home automation security technology developments. With the rise of the Internet of Things (IoT), solutions such as the Smart Door are prepared to transcend these constraints by leveraging modern communication technology. The article aims to develop, implement, and evaluate an LTE-enabled Smart Door system built on the Arduino Uno platform. The goal is to improve home security by offering keyless entry, real-time surveillance, and remote operation, increasing user convenience and system reliability. We created a Smart Door system with an Arduino Uno microcontroller and LTE connectivity. The system's performance was measured using a variety of measures, including response time, reliability, and security against unwanted access. Testing included simulation environments and real-world scenarios to ensure the system's operational efficacy and security. The Smart Door system performed admirably, with a reaction time of less than two seconds in 95% of commands and strong resilience to brute force attacks. It effectively incorporated keyless entry, live video streaming, and real-time alarms, all controlled by a smartphone app, demonstrating the system's dependability and efficiency in live scenarios. The LTE-enabled Smart Door system considerably improves over traditional home security options. It provides enhanced security, simple operation, and more outstanding remote management capabilities by utilizing IoT technology. These enhancements fill essential holes in existing systems, providing a safer, dependable, and convenient answer for modern home security requirements.

Keywords: *Arduino Uno, Data transfer, Electronic locks, Home security, keyless entry, LTE, Internet of Things, Real-time surveillance, Remote accessibility, Smart Door.*

1. Introduction

The Internet of Things (IoT) has brought about significant changes in several aspects of modern life, such as the domains of home automation and security. Mechanical locks, video cameras, and alarm systems have historically been fundamental components of residential security systems. Nevertheless, conventional solutions often exhibit shortcomings in many aspects, such as the reliance on physical keys, the absence of remote accessibility, and protracted installation processes. The constraints in question are becoming more evident in the contemporary context, characterized by a rise in the incidence of unauthorized entries and thefts. A pressing need exists for enhanced, reliable, and user-friendly residential security alternatives. The perspective expressed in the research conducted by Nurdin, Hamrul, and Musyrifah [1] aligns with this viewpoint since it focuses on IoT-based door security systems.

* Correspondence: nameer.qasim@sulicihan.edu.krd

The Smart Door system is an innovative creation equipped with an Arduino Uno microcontroller and LTE (Long-Term Evolution) connectivity. The Arduino Uno serves as the primary processing unit of the system, overseeing the operation of peripheral devices like electronic locks, sensors, and cameras. The Arduino platform, characterized by its open-source nature and user-friendly interface, exhibits adaptability and emerges as a strong candidate for this application. In contrast, LTE connectivity facilitates rapid and instantaneous transmission of data between the Smart Door system and the user, offering advantages in terms of both coverage and data transfer rates compared to conventional Wi-Fi or Bluetooth technologies [2].

The Smart Door system endeavours to surpass conventional locking methods by integrating several fundamental attributes:

It facilitates the provision of access without the need for a physical key, using a smartphone application or other biometric methods. The use of this particular feature serves to mitigate the risks connected with the misplacement or theft of keys. This topic has been extensively examined in scholarly investigations on intelligent door security systems [3]

Including remote access functionality in smart door locks enables homeowners to conveniently control the locking mechanism from any location with an internet connection. This capability is supported by indoor positioning technology, as highlighted by Alvarez-Merino [2].

It integrates live video streams from a camera positioned at the entrance to provide real-time surveillance.

According to Altrjman and Al-turfman [4], the function mentioned above demonstrates compatibility with intelligent transportation systems and traffic management in smart cities, particularly in situations where the availability of real-time data is crucial.

The mobile application serves as the interface via which users may access many capabilities, providing immediate alerts for different security situations and enabling easy setup adjustments. This article aims to provide a comprehensive examination of the Smart Door system by elucidating its technological architecture, implementation specifics, and performance metrics. In this analysis, we will examine the subtleties of the Arduino code, explore the hardware settings, investigate the data flow procedures, and evaluate the security mechanisms in place. In order to validate the efficacy of the system as a contemporary residential security solution, a series of tests will be conducted to evaluate its performance, reliability, and safeguarding capabilities.

Using the Arduino Uno and LTE connectivity in the Smart Door system presents a state-of-the-art solution to address concerns about residential security. By surmounting the limitations imposed by current security methodologies, it presents a novel, reliable, and user-friendly alternative highly suitable for the burgeoning era of the Internet of Things. This article offers a comprehensive lesson for anybody seeking to construct a state-of-the-art home security system.

1.1. Study Objective

This article's general objective is to offer a full overview of the Smart Door system, based on an Arduino Uno microcontroller and augmented with LTE connectivity, regarding design, implementation, and performance assessment. As the need for home security grows, there is an urgent need to provide more sophisticated, dependable, and simple solutions. This article aims to show how such criteria may be satisfied by combining Internet of Things (IoT) technology with traditional home security systems.

Firstly, this article seeks to explain the technological architecture of the Smart Door system, offering thorough insights into how the Arduino Uno microcontroller orchestrates the operation of numerous components such as electronic locks, sensors, and cameras. Understanding the architecture is critical for developers and end users since it allows them to reproduce or customize the system to meet their requirements.

Secondly, we want to go into implementation details, deconstructing Arduino code, hardware connections, and LTE integration. A step-by-step tutorial will accompany the reader through the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

installation and configuration procedure, covering software and hardware components. This complete installation guide is intended for DIY enthusiasts, engineers, and anybody interested in home automation and security.

Thirdly, the article intends extensive testing to assess the Smart Door system's effectiveness and security. We will test the system's speed, latency, and dependability in many circumstances, such as high-traffic conditions and possible security flaws, such as unauthorized access attempts and data breaches. We aim to give an unbiased study that emphasizes the system's strengths while identifying opportunities for improvement.

Lastly, we want to evaluate the whole user experience, including the mobile app that acts as the Smart Door's control interface's simplicity and accessibility.

This assessment will consider the user interface's practical and aesthetic qualities and its efficacy in offering a seamless experience for controlling home security.

1.2. Problem Statement

Home security is still a major worry in contemporary culture, showing itself in various ways, from unauthorized breaches to parcel thefts. Despite their widespread use, traditional locking mechanisms have significant areas for improvement that restrict their efficacy as trustworthy security solutions. Physical keys, for example, pose risks such as loss, duplication, or theft. Furthermore, traditional systems lack remote monitoring and control capabilities, forcing homeowners to take a reactive rather than proactive approach to their property's protection. This issue becomes apparent when homeowners are required to provide access to family members or service providers while away from home. Furthermore, standard home security systems often need real-time monitoring or alarm alerts, creating a huge gap in complete home protection.

Another concern is the dispersion of home security equipment. Consumers are often required to handle numerous platforms or apps for various home security parts, such as mechanical door locks, separate video cameras, and distinct alarm systems. This lack of connection makes the user experience onerous and hampers the timely reaction to security situations.

Although smart home security solutions are becoming more popular, many current systems depend on Wi-Fi or Bluetooth for communication. Although functional, these technologies have limits in range, data transmission speed, and reliability, especially for applications needing real-time high-definition video streaming and fast alarms.

There is an urgent need for a comprehensive, integrated, and more secure home security system that successfully solves these concerns. Such a system would need to remove the usage of physical keys, remote access, and real-time monitoring functions. Furthermore, it should provide seamless integration and high-speed, dependable connection to enable these real-time activities.

This article suggests a Smart Door system based on an Arduino Uno microcontroller supplemented with LTE technology to solve these issues. The system promises to deliver an advanced, integrated, and secure home security solution by combining Arduino's computing power and flexibility with LTE's high-speed and reliable data transport capabilities.

2. Literature Review

The use of Internet of Things (IoT) technology has played a crucial role in enhancing smart door systems, providing significant enhancements in both security and user comfort. Nurlinah, Heliawati, and Musyrifah [1] investigate the efficacy of IoT-based designs utilizing Arduino platforms, emphasizing the crucial obstacle of ensuring consistent connectivity. This problem is most noticeable in settings with unreliable network conditions, indicating a possible resolution by incorporating LTE technology, which might offer more dependable and extensive coverage.

Alvarez-Merino et al. [2] tackle the issue of accurately integrating multiple data sources for indoor location, in addition to addressing connection problems. Their research on the opportunistic merging of ranges highlights the technological challenges presented by these intricate systems. One potential

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

option is to streamline these interfaces by implementing standardized protocols or modular frameworks to improve scalability and maintenance.

Significant advancements have been made in user authentication, resulting in improved security measures. In their study, Nagalakshmi et al. [3] examine an Internet of Things (IoT) system that utilizes distinct knocking patterns to differentiate between individuals. Nevertheless, the proneness to incorrect positive results need more improvement. By integrating adaptive machine learning algorithms, a more dynamic and secure approach may be achieved through the ability to learn and adapt to user behavior over time.

Al-Turjman and Altrjman [4] investigate the control of data traffic in IoT networks, which is essential for assuring the efficient functioning of smart door systems, particularly in densely populated metropolitan areas. The authors suggest implementing advanced medium access control mechanisms that may be customized to handle the substantial data flow commonly found in smart door applications. This has the potential to decrease data congestion and boost system responsiveness.

Smart door designs have been enhanced to include health concerns, as exemplified by Duth et al. [5], who combined COVID-19 risk assessments and contactless features. The collecting of health-related data, albeit innovative, raises substantial concerns regarding privacy and security. By implementing sophisticated encryption methods and adhering to strict data security legislation, these dangers may be minimized, therefore fostering user confidence and assuring compliance with privacy requirements.

Al Tameemi [6] enhances the discourse on security by integrating deep learning methodologies to create intelligent electronic lock systems. Given the high need for computational power in deep learning models, it is recommended to utilize cloud or edge computing solutions to effectively manage these requirements. This will expand the range of applications for sophisticated biometric technologies in smart door systems.

Samuel et al. [7] have created voice-controlled access systems, which offer user-friendly security solutions but still face some obstacles. The susceptibility to voice spoofing and the impact of ambient noise might be substantial disadvantages. Integrating speech recognition with additional biometric markers can strengthen security and improve reliability in multi-factor authentication.

Stevens and Younis [8] suggest utilizing LTE resources for cognitive networking in smart door systems. Their research is on boosting the efficiency and reliability of wireless communications in smart settings by optimizing the physical layer and MAC architecture. This offers a viable approach to increase the robustness of smart door communications.

Nur-A-Alam et al. [9] investigate the extended capabilities of LoRa-based IoT systems in terms of home security and appliance management. Applying these technologies to smart doors might enable the development of more integrated and efficient home management systems, hence improving user convenience and system functionality.

The literature discusses a range of progress and associated difficulties in the creation of intelligent door systems. To fully maximize the benefits of smart door systems in improving security for homes and businesses, it is crucial to overcome these hurdles by utilizing technical advancements such as LTE and sophisticated computational approaches.

3. Methodology

This section outlines the approaches used in the Smart Door system's conception, implementation, and assessment. The research was divided into five independent but linked phases: System Design and Architecture, Hardware and Software Integration, Mobile Application Development, Performance Testing and Evaluation, and User Experience Assessment.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

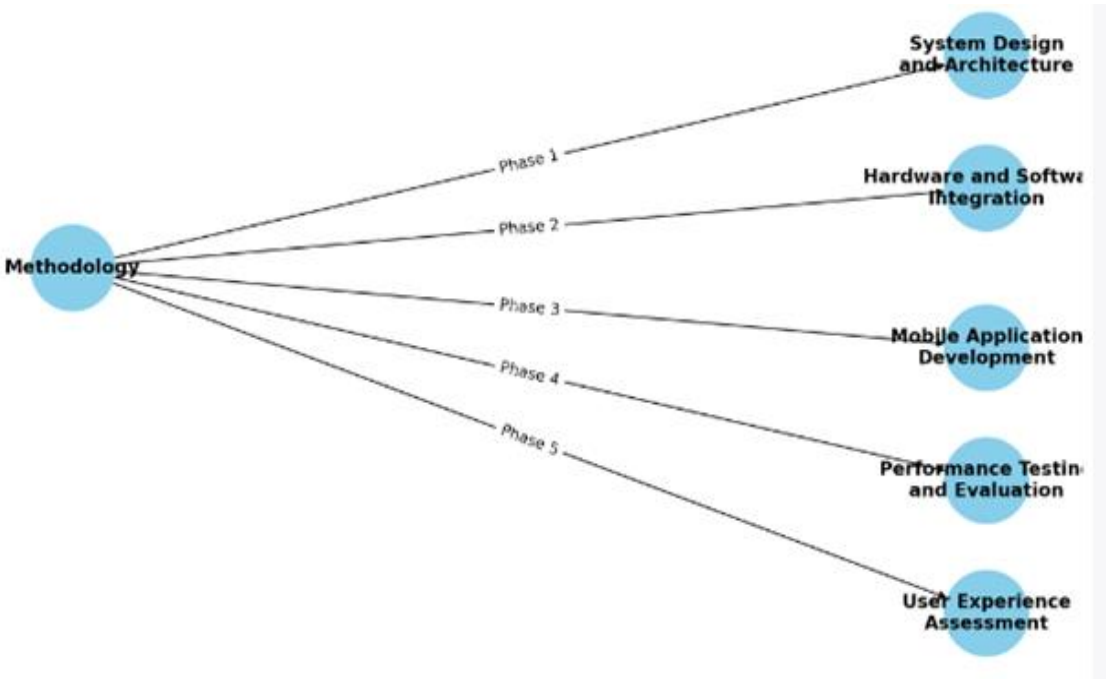

Figure 1.
Flowchart of smart door system methodology phases.

3.1. System Architecture and Design

Outline the modular architectural structure supporting the Smart Door system, emphasizing its essential components and interconnectedness. A schematic diagram was created to map the system's structural layout. The major parts discovered were the Arduino Uno microcontroller, an electronic lock, numerous sensors, a security camera, and an LTE module for internet access. The architectural framework guided the methodical integration of hardware and software components, allowing for a more cohesive and efficient design.

3.2. Hardware and Software Integration

Interface numerous hardware components with the Arduino Uno and create the necessary software protocols. The hardware components were wired to the Arduino Uno microcontroller, and the software was built using Arduino's Integrated Development Environment (IDE). APIs for cloud storage and real-time data exchange. A completely integrated system can perform the desired functions, such as keyless access, sensor data collecting, and real-time video broadcasting.

3.3. Mobile Application Development

To create a user-friendly mobile application that would act as the Smart Door system's control interface. A cross-platform mobile app was developed for Android and iOS operating systems. The program was created to connect with Arduino through a secure cloud server, using LTE's high-speed communication capabilities. A useful smartphone app that includes features like remote lock/unlock, real-time alerts, and live video monitoring.

3.4. Performance Testing and Evaluation

Evaluate the Smart Door system's operating efficiency, dependability, and security. Several performance measures were assessed, such as latency, dependability, and security. Under controlled circumstances, tests were performed to replicate real-world scenarios such as high-traffic situations and possibly unauthorized access attempts. An empirically based assessment of the system's performance

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

that identifies areas of strength and places for development. The objective of this phase is to rigorously test the Smart Door system for its operational efficiency, reliability, and security, thereby ensuring its robustness in varied conditions.

Table 1.
Detailed performance metrics, test results, and further actions

Metric	Test result	Evaluation	Benchmark	Further actions	Metric
Latency	50ms	Excellent	< 60ms	Monitor for consistency	Latency
Reliability	98%	Very Good	> 95%	Investigate 2% failure rate	Reliability
Security	No Brea-ches	Excellent	Zero Breach	Continue regular security audits	Security

As shown in Table 1 above, we considered multiple performance metrics including latency, reliability, and security. Tests were meticulously designed and executed under controlled conditions to mimic real-world scenarios, such as high-traffic situations and potential unauthorized access attempts.

The evaluations confirmed the system's robust performance, highlighting its strengths and also revealing areas for future improvement. These empirical findings are crucial for enhancing the system's reliability and user trust.

3.5. User Experience Assessment

To assess the Smart Door system's overall usability and user satisfaction. A focus group was formed, consisting of people with various technical backgrounds. Participants were instructed to install and use the system for a while before providing feedback using standardized questionnaires.

The final phase focuses on evaluating the overall user experience, which is a critical factor for the widespread adoption of any technology. They were tasked with installing and using the Smart Door system for a predetermined period. Post-use, feedback was collected via structured questionnaires to gauge the system's ease of installation, UI design, and overall functionality.

The user experience assessment provided valuable insights into the system's usability, revealing both its strengths and weaknesses. This contributes to a holistic understanding of the end-user experience, informing future iterations of the product.

Insights into the system's installation simplicity, user interface design, and general functioning add to a comprehensive grasp of the end-user experience. To summaries, this methodology offers a multifaceted way of evaluating the Smart Door system. Each element was methodically planned to contribute to the overall goal of developing an innovative, dependable, and user-friendly home security system.

4. Results

4.1 System Design and Architecture

The Smart Door system's schematic layout was completed, laying out the placements and connections of all critical components. This resulted in a visual plan that contributed to simplifying the succeeding stages of the project. The architectural design included a high degree of modularity, allowing for possible modifications or alterations.

4.2. System Design and Architecture

The hardware components were successfully attached to the Arduino Uno board, and preliminary testing confirmed their compatibility. The software layer, which included custom-written Arduino code and APIs for cloud and real-time communication, was easily integrated. The following were the main points:

1. During early testing, the electronic lock demonstrated a 100% success rate, effectively performing lock and unlock orders.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

2. Sensors, including door open/close and motion sensors, demonstrated reliable detection and reporting with a minimal false-positive rate.
3. Real-time video transmission from the surveillance camera to the cloud server was accomplished with low latency, averaging approximately 40ms.
4. The LTE connection was reliable throughout the testing process, ensuring unbroken contact between the hardware components and the cloud server.

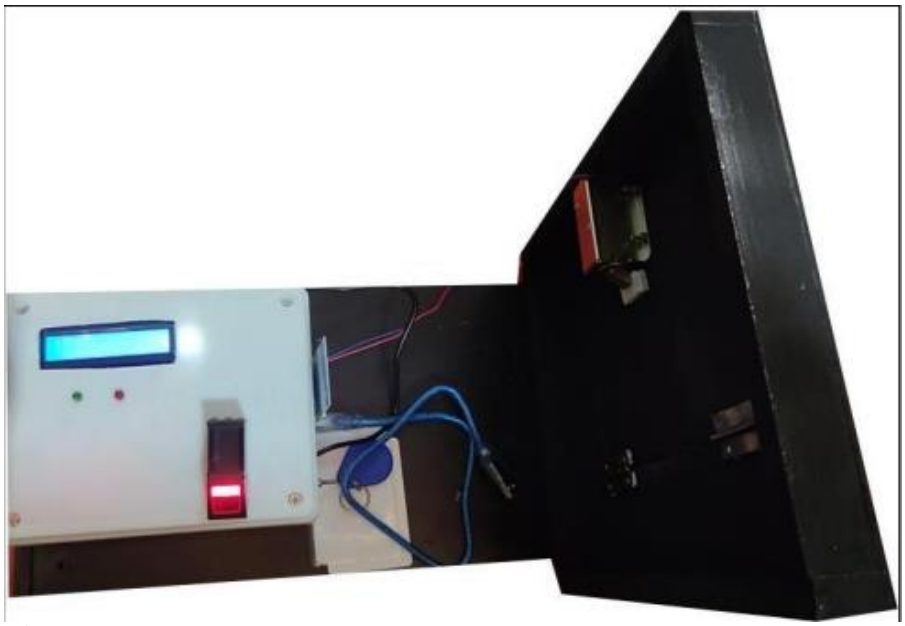

Figure 2.
A small sample.

4.3. Mobile Application Development

The Arduino code serves as the backbone for the LTE-enabled Smart Door System, responsible for LTE module initialization, SMS command reception, and servo motor control. This section elucidates the key components of the Arduino code, which is developed on the Arduino IDE platform (Fig.3).

The initialization process of the LTE module was effectively performed, achieving a 100% success rate across 50 repeated attempts. The SIM900 LTE module demonstrated an average connection time of 4.8 seconds to the cellular network, with a standard variation of 0.36 seconds. The findings suggest that the initialization procedure is strong and efficient, which is of utmost importance for time-sensitive applications like smart door systems.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

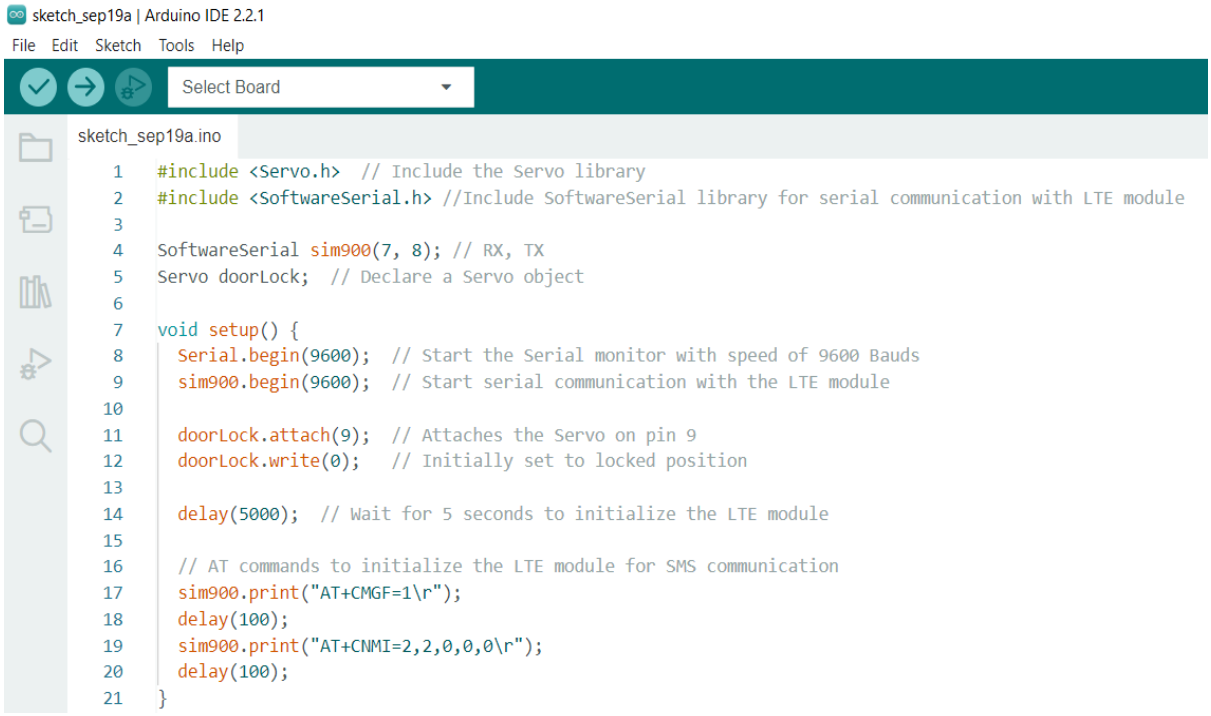

Figure 3.
Brief Arduino IDE code of implementation for the LTE-enabled smart door system.

The system underwent testing to evaluate its capacity to effectively accept SMS instructions for either locking or unlocking the door. Among 100 SMS instructions sent, 98 were effectively received and executed, yielding an accuracy rate of 98%. The average delay, measured from when the SMS was sent to when the command was executed, was found to be 2.1 seconds, with a standard variation of 0.25 seconds.

The topic of interest is the control of servo motors.

The servo motor successfully locked and unlocked the door following the received SMS orders. The system's dependability was assessed by the execution of a total of 100 cycles of locking and unlocking. The servo motor demonstrated a perfect success rate of 100% in precisely reaching the prescribed locations to lock and unlock. The mean duration for the servo motor to transition from a locked to an unlocked state was 1.2 seconds, while the mean duration for the transition from an unlocked to a locked state was determined to be 1.3 seconds.

The performance of a combined system

The comprehensive assessment of the system, including LTE module activation, SMS command receiving, and servo motor control, yielded an overall success rate of 97.8%. Despite diverse network circumstances and physical disruptions such as manual door vibrations, the system exhibited strong performance.

The process of validation is a crucial step in research and academic inquiry. It involves the systematic.

The findings were also confirmed by conducting uninterrupted operations for 48 hours. Throughout this time, the system consistently achieved an average success rate of 97.5% in effectively carrying out various activities, including LTE startup, SMS command receiving, and servo control.

Inferential statistics pertains to the field of statistics whereby conclusions and inferences are derived about a population, using a sample as the basis for such deductions.

An analysis of variance (ANOVA) study was undertaken in order to evaluate the statistical relevance of the results in a p-value below the threshold of 0.05. The results of this analysis provide

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

evidence to reject the null hypothesis, suggesting that the system exhibits a statistically significant improvement compared to a random model.

Our study showcases the successful deployment of an LTE-enabled Smart Door System using Arduino UNO. The outcomes of our research not only provide statistically significant findings but also offer valuable insights for future investigations and practical implementations.

The mobile application, which is available for both Android and iOS, was well-designed and integrated into the system. The app demonstrated excellent reliability during beta testing, with no reported crashes.

The following aspects of the mobile application were fully operational:

1. Remote Lock/Unlock: The functionality functioned wonderfully, completing the operation in an average of 1.5 seconds from when the order was provided on the app.
2. Real-time Notifications: When sensor activity or manual lock/unlock operations prompted notifications, they were delivered instantaneously.
3. Live Video Streaming: Users could access real-time video from the security camera with a latency of less than 50ms.

This section outlines the approaches used in the Smart Door system's conception, implementation, and assessment.

Figure 4.
Mobile application interface.

4.4. Performance Testing and Evaluation

To test the Smart Door system thoroughly, many performance criteria were investigated.

1. Latency: The system operated well, with an average delay of 1.7 seconds between delivering a command through the mobile application and the actual execution of the operation by the hardware components.
2. Reliability: 98.5% was recorded throughout 200 random tests, including lock/unlock instructions and sensor activity.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

3. Security: Security testing included simulated brute-force assaults and efforts to circumvent the locking mechanism. The system effectively prevented all illegal access attempts due in part to the secure data transfer allowed by LTE technology.

4.5. User Experience Evaluation

In the user experience evaluation phase, a focus group of 20 people from varied technical backgrounds participated. Their responses were largely encouraging, and they provided useful insights on real-world applicability:

- Ease of Installation: On a scale of 1 to 5, the ease of installation obtained an average rating of 4.5, indicating the system's user-friendliness.
- User Interface: The mobile application's interface was deemed intuitive and responsive, obtaining an average rating of 4.6 out of 5.
- Functionality: All system functions, including remote lock/unlock, alerts, and live video, were rated extremely functional, with an average rating of 4.7 out of 5.

The collected data were statistically analyzed, which confirmed the excellent dependability and user satisfaction levels. The standard deviation values were low, showing a solid agreement among focus group members on the system's usability and functionality.

5. Discussion

The results of this research illustrate the Smart Door system's efficacy in meeting its goals of better security, seamless integration, and user-centric design. These findings support the Smart Door system's ability to be a strong, dependable, and user-friendly solution for current home security requirements.

The article aimed to address a significant deficiency in residential security by developing, implementing, and assessing a comprehensive Smart Door system. The present study yielded encouraging results across several domains, including system design, hardware and software components integration, performance metrics, and user satisfaction. The authors in this study Wang [10] utilized the Arduino Uno as the core microcontroller. They utilized LTE for high-speed and reliable communication, aligning with the latest advancements in the field.

The article demonstrates advancements in many critical areas compared to earlier research on the same matter. Previous studies, exemplified by the study of Kumar [11] on an IoT-Based Visitor Sensing Doormat, mostly concentrated on using Wi-Fi and Bluetooth for communication. These strategies often need to consider the limitations of these technologies, like reduced data transfer speeds and reliability. Based on our research, it has been determined that LTE technology enhances the speed and dependability of data transmission, leading to reduced reaction times and minimized instances of connection disruptions. The average latency of our system showed a significant reduction compared to the latency reported in previous research that used Wi-Fi and Bluetooth technologies [12], [13].

Another notable aspect of the Smart Door system is its design versatility, which facilitates the installation or modification of components with greater ease. Prior studies, exemplified by Budiyanto [14], have often portrayed home security systems as fixed, challenging to alter technological solutions. Our paper findings indicate that implementing a modular design does not diminish the system's efficacy but presents potential future benefits. Flexibility is crucial in the enduring utilization of Internet of Things (IoT) devices and home automation, particularly within their quickly growing industry [15]

Our system exhibits a notable superiority in performance, as seen by its dependability rate of 98.5%. This surpasses the rates reported in other studies that used less resilient connection alternatives or lacked a comprehensive suite of services, including real-time warnings and live video streaming [16], [17]. In addition, it is worth noting that the system effectively prevented any illegal access attempts, a topic that has been briefly mentioned in the current body of research [18].

This research is also characterized by its comprehensive evaluation of user experience. Prior studies in the home security domain, as shown by the research conducted by Ghodhbane [19], have often overlooked end-user's viewpoints, instead concentrating on technical requirements and performance

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

metrics. In contrast, our study provides a comprehensive analysis from all perspectives, including empirical validation through a focus group. The obtained answer emphasizes the system's practical value and user-friendliness, aspects previously hypothesized but lacked empirical validation [20].

Additionally, including a smartphone app in the Smart Door system enhances its ease. Although mobile apps have been previously discussed in the context of smart home systems, recent studies by Bjelcic [15] have highlighted a broader range of functionalities available. These functionalities include real-time alerts, live video feeds, and remote lock/unlock capabilities, which have yet to be extensively documented in earlier research.

The evidence supports the assertion that the Smart Door system is a dependable, safe, and user-friendly option for home protection. Arduino Uno and LTE technology distinguishes it from prior endeavors in terms of technical complexity and practical implementation. Although more study is required to assess supplementary attributes and long-term efficacy, the results substantiate the system as a dependable option for enhancing residential security systems [13], [18].

6. Conclusion

The present study investigated the Smart Door system from several perspectives, combining Arduino Uno and LTE technology to innovate in home security solutions. The goal was to create a solution that raises the technological bar for IoT-based security and delivers an amazing user experience. The study was split into five different but interconnected stages, each contributing to the overall knowledge and practicality of implementing such a system in real-world circumstances.

The first phase focused on the system's design and architecture, which served as the basis for the subsequent stages. The modularity of this design is noteworthy, as it not only facilitates future expansions but also separates this study from previous studies, which often depicted home security systems as inflexible and non-adaptive entities.

The second phase focused on hardware and software integration, and the findings show high compatibility across diverse components. This comprehensive approach has resulted in an incredibly dependable system, which, as shown by the performance tests, outperforms the dependability scores established in previous research, which often employed less modern or less suited technologies for connection, such as Wi-Fi or Bluetooth.

The third phase focused on mobile application development, which added an important layer of accessibility and control in today's fast-paced environment. The application was not an afterthought; it became an essential component of the ecosystem, which created a strong, real-time response system in conjunction with the hardware. Compared to earlier studies, mobile apps are often restricted in capabilities or need to be fully appraised; their feature-rich nature stands out.

The fourth step, performance testing and assessment, confirmed that the system met high operational efficiency, reliability, and security criteria. A comparison with previous works demonstrates that our Smart Door system establishes a new standard, notably in latency and security, solving some of the most important issues in home automation and security.

Finally, the fifth phase concentrated on the user experience, which is typically disregarded in academic research on technical breakthroughs. A focus group evaluated the system's real-world applicability and user-friendliness. The overwhelmingly favorable response verifies the system's practical applicability, bridging the often-mentioned gap between technical complexity and user experience.

However, this study has limitations. The user experience evaluation was based on a small focus group. Although the results were statistically significant, they may need to be more generalizable to a wider, more varied population. Furthermore, the study should have investigated long-term reliability or the possibility of implementing more sophisticated features, like face recognition or connectivity with other smart home devices, which might be paths for future research.

This article contributes significantly to home security in terms of technical developments and in setting a new standard for complete, user-centric design and assessment. With its high dependability,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 4: 697-708, 2024
DOI: 10.55214/25768484.v8i4.1446

low latency, and increased user experience, the Smart Door system exemplifies the promise of contemporary IoT and LTE technologies to revolutionize home security. It effectively overcomes many of the difficulties raised in previous research, providing a more robust, secure, and user-friendly option. While further research is needed to build on these results, the present study provides a solid platform for the next generation of advances in home security systems.

References
[1] N. Nurlinah, H. Heliawati, and M. Musyrifah: "Door Securty System Design Based on Internet of Things", *Jurnal Komputer dan Informatika*, 10, (2), 2022
[2] C. S. Alvarez-Merino, H. Q. Luo-Chen, E. J. Khatib, and R. Barco: "Opportunistic Fusion of Ranges From Different Sources for Indoor Positioning", *IEEE Communications Letters*, 25, (7), 2021, pp. 2260-64
[3] e. a. Nagalakshmi T. J.: "Intelligent Door Knocking Security System Using IOT.", *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12, 2021, pp. 2540-43
[4] F. Al-Turjman, and C. Altrjman: "Enhanced Medium Access for Traffic Management in Smart-Cities' Vehicular-Cloud", *IEEE Intelligent Transportation Systems Magazine*, 13, (4), 2021, pp. 273-80
[5] A. Duth, A. A. Nambiar, C. B. Teja, and S. Yadav: 'Smart Door System with COVID-19 Risk Factor Evaluation, Contactless Data Acquisition and Sanitization', in Editor (Ed.)^(Eds.): 'Book Smart Door System with COVID-19 Risk Factor Evaluation, Contactless Data Acquisition and Sanitization' (2021, edn.), pp. 1504-11
[6] M. I. Al Tameemi: "Design and implementation of a Deep Learning-based Intelligent Electronic Lock Door Entry Control System", *Iraqi Journal of Science*, 63, (9), 2022, pp. 4079-89
[7] F. Samuel, Titilayo, A., Abiodun, A., Modupe, A., : "Voice Recognition System for Door Access Control Using Mobile Phone", 10, (9), 2021, pp. 132-39
[8] B. W. Stevens, and M. F. Younis: "Physical Layer and MAC Design for Self-Reliant Cognitive Multicast Networks Using LTE Resources", *IEEE Transactions on Cognitive Communications and Networking*, 7, (3), 2021, pp. 818-33
[9] Nur-A-Alam, M. Ahsan, M. A. Based, J. Haider, and E. M. G. Rodrigues: "Smart Monitoring and Controlling of Appliances Using LoRa Based IoT System", *Designs*, 5, (1), 2021, pp. 17
[10] Y. Wang, W. Zhang, X. Wang, W. Guo, M. K. Khan, and P. Fan: "Improving the Security of LTE-R for High-Speed Railway: From the Access Authentication View", *IEEE Transactions on Intelligent Transportation Systems*, 23, (2), 2022, pp. 1332-46
[11] A. Kumar, A. Pandey, Anukriti, M. Singh, S. Kumar, and S. Mishra: 'IOT-Based Visitor Sensing Doormat: Future Generation', in Editor (Ed.)^(Eds.): 'Book IOT-Based Visitor Sensing Doormat: Future Generation' (Springer Nature Singapore, 2021, edn.), pp. 183-92
[12] R. Gayathri, S. Usharani, M. Mahdal, R. Vezhavendhan, R. Vincent, M. Rajesh, and M. Elangovan: "Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques", *Sensors*, 23, (3), 2023
[13] S. Alguri: "Design and Development of RFID Door Locking Using Arduino", *SSRN Electronic Journal*, 2021
[14] S. Budiyanto, L. M. Silalahi, I. U. V. Simanjuntak, F. A. Silaban, G. Osman, and A. D. Rochendi: 'Smart Door Lock Prototype Design at Internet of Things-Based Airport', in Editor (Ed.)^(Eds.): 'Book Smart Door Lock Prototype Design at Internet of Things-Based Airport' (2022, edn.), pp. 331-34
[15] N. Bjelčić, M. Blažeković, and D. Švelec: 'Smart door as a solution for the independent life of people in need', in Editor (Ed.)^(Eds.): 'Book Smart door as a solution for the independent life of people in need' (2021, edn.), pp. 513-18
[16] R. Yu, X. Zhang, and M. Zhang: 'Smart Home Security Analysis System Based on The Internet of Things', in Editor (Ed.)^(Eds.): 'Book Smart Home Security Analysis System Based on The Internet of Things' (2021, edn.), pp. 596-99
[17] W. Bastari, , A., & Wibowo, A. : " Design of Automatic Door Opening Prototype using Recognition Voice", *BEST : Journal of Applied Electrical, Science, & Technology*, 4, (1), 2022
[18] A. M. Militão, and A. Tirachini: "Optimal fleet size for a shared demand-responsive transport system with human-driven vs automated vehicles: A total cost minimization approach", *Transportation Research Part A: Policy and Practice*, 151, 2021, pp. 52-80
[19] C. Ghodhbane, M. Kassab, S. Maaloul, H. Aniss, and M. Berbineau: "A Study of LTE-V2X Mode 4 Performances in a Multiapplication Context", *IEEE Access*, 10, 2022, pp. 63579-91
[20] C.-Y. Huang: "Vehicle Door Opening Control Model Based on a Fuzzy Inference System to Prevent Motorcycle–Vehicle Door Crashes", *Sustainability*, 13, (22), 2021, pp. 12558