

Smart Lock Technology: Developing and Enhancing Home Security using Android-Based Controlled Door Locking App's

Perfecto R. Ruaya, Jr.

Faculty, College of Engineering and Information Technology,
Surigao Del Norte State University, Surigao City, Philippines

Abstract: *This study presents an overview of the study on the implementation and potential of a novel Android-based controlled door locking app to advance home security in the context of smart homes. The app leverages the capabilities of android devices to offer remote access and management of door locks, empowering homeowners with seamless control over their access points. The study evaluates the app's performance in usability, accuracy, efficiency, portability, security, and maintainability, revealing its commendable capabilities with an average score of 4.17 out of 5. With minor enhancements, the app shows promising potential as a reliable and user-friendly access control solution, driving the evolution of smart lock technology and home security in the modern era.*

Keywords: Android-based, evaluation, controlled locking apps, home security, home security

I. INTRODUCTION

In an increasingly interconnected world, the concept of a "smart home" has emerged as a revolutionary solution for modern living, providing enhanced convenience and security to homeowners[1][2]. Among the key components driving the evolution of smart homes is the advent of smart lock technology. Integrating the power of mobile devices and internet connectivity, smart lock systems offer a sophisticated approach to access control, allowing homeowners to remotely manage and monitor their doors through smartphone applications[3][4].

This research journal delves into the realm of smart lock technology, with a specific focus on the development and utilization of an Android-Based Controlled Door Locking App. As technology continues to advance rapidly, the need to fortify home security has become paramount, and this study aims to explore the potential of Android-based apps in achieving this objective.

The primary objective of this research is twofold: first, to investigate the development process of an Android-based controlled door locking app, and second, to assess its effectiveness in enhancing home security. By exploring the underlying technology, usability, and security aspects, this research seeks to provide valuable insights into the integration of mobile devices and smart lock systems, with the ultimate goal of fostering a safer and more convenient living environment for homeowners.

In the following sections, it will delve into the existing literature on smart lock technology, examining the evolution of access control systems from traditional locks to cutting-edge smart lock solutions. It will also review the current landscape of Android-based controlled door locking apps, exploring their features and functionalities[5]. Moreover, this research will delve into the challenges and opportunities presented by the adoption of smart lock technology in a home setting, considering factors such as user acceptance, data privacy, and vulnerability to cyber threats.

The experimental aspect of this study involves the development and implementation of a prototype Android-based controlled door locking app, which will be rigorously tested in various real-world scenarios to evaluate its performance, reliability, and security. The results of these experiments will be analyzed and discussed, shedding light on the potential benefits and limitations of such applications.

This research study aims to contribute to the growing body of knowledge surrounding smart lock technology and its role in enhancing home security. By unraveling the intricacies of Android-based controlled door locking apps, we

aspire to equip homeowners, technology developers, and researchers with valuable insights that can shape the future of access control systems, making homes safer and more intelligent in the process.

II. RELATED LITERATURE

The proliferation of smart home technology has revolutionized the way we interact with our living spaces, offering unprecedented convenience and security[6][7]. Among the key components driving this transformation is the emergence of Android-based controlled door locking apps. These apps leverage the power of mobile devices and the Android operating system to provide users with seamless access control and remote management of their door locks. This background study explores the evolution, features, security aspects, and potential implications of Android-based controlled door locking apps in the realm of smart homes.

- *Evolution of Access Control Systems:* The history of access control systems can be traced back to traditional mechanical locks and keys. Over time, technological advancements led to the development of electronic access control systems, offering enhanced security features[9][10]. The emergence of Android-based controlled door locking apps marks a significant leap forward in the field, leveraging the ubiquity of smartphones to provide users with remote access and management of their door locks.
- *Mobile Application Development for Smart Homes:* The rise of smart homes has spurred the development of various mobile applications tailored to control and monitor household devices. Android, as a dominant mobile platform, plays a vital role in this landscape, enabling seamless integration of smart lock technology with other IoT devices[11][12]. Existing studies highlight the convenience and accessibility that Android-based controlled door locking apps bring to homeowners, streamlining home security management.
- *Usability and User Experience (UX) Studies:* The success of any mobile application, including Android-based controlled door locking apps, heavily relies on its usability and user experience[13][14]. Several studies have explored the design and interface elements that contribute to a positive user experience. Understanding user preferences and pain points is crucial in refining the app's functionalities, ensuring ease of use and fostering user acceptance.
- *Security Concerns and Vulnerabilities:* As with any internet-connected device, Android-based controlled door locking apps raise security concerns[15][16]. Researchers have investigated potential vulnerabilities and security flaws that could compromise the integrity of these systems. Addressing these concerns is vital to instill confidence in users and prevent unauthorized access to smart homes.
- *Internet of Things (IoT) Integration:* Android-based controlled door locking apps are a manifestation of IoT in the home security domain. Studies have examined the integration of smart lock systems with other IoT devices and platforms to create cohesive smart home ecosystem[17][18]. Interoperability, data sharing, and standardization are areas of exploration to maximize the benefits of IoT integration.
- *User Acceptance and Adoption:* The successful adoption of Android-based controlled door locking apps depends on user acceptance and willingness to embrace the technology[19]. Researchers have studied factors influencing user adoption, including perceived usefulness, ease of use, and privacy concerns. Identifying barriers to adoption can guide developers in refining app features and marketing strategies.
- *Comparative Analysis of Smart Lock Solutions:* Researchers have conducted comparative studies to evaluate the performance and features of different smart lock solutions, including Android-based controlled door locking apps[20][21]. These assessments aid consumers in making informed choices and assist manufacturers in refining their products to align with user needs.
- *Data Privacy and Legal Implications:* The use of Android-based controlled door locking apps involves collecting and processing personal data, necessitating a thorough examination of data privacy and legal implications[22][23]. Studies have delved into data protection regulations and highlighted best practices to safeguard user privacy in the context of smart lock applications.

The related literature on Android-based controlled door locking apps showcases the rapid evolution of access control systems in the context of smart homes. From the historical development of access control technologies to the contemporary challenges and opportunities posed by Android-based apps, the existing body of knowledge offers

valuable insights for researchers, developers, and consumers alike. By addressing usability, security, user acceptance, and privacy concerns, this literature guides the development and implementation of Android-based controlled door locking apps that enhance home security and redefine the way we interact with our living spaces.

III. DESIGN OF ANDROID-BASED CONTROLLED DOOR LOCKING APP

The Android-Based Controlled Door Locking App is designed to provide users with a convenient and secure way to manage access to their homes remotely. The app leverages the capabilities of Android devices to interact with a smart door lock system and offers features such as remote locking/unlocking, access permissions, real-time notifications, and activity logs. This system software design outlines the architecture, components, and interactions that enable the functionality of the Android-based controlled door locking app

- *System Architecture:* The system architecture of the Android-based controlled door locking app consists of the following components:
- *Mobile Application:* The Android app serves as the user interface, allowing homeowners to interact with the smart door lock system. It runs on Android devices and provides a graphical interface for accessing various functionalities.
- *Cloud Server:* The cloud server acts as the intermediary between the Android app and the smart door lock system. It facilitates data transmission, authentication, and processing of user commands.
- *Smart Door Lock System:* The physical smart door lock is equipped with IoT capabilities, enabling it to receive commands from the Android app via the cloud server and perform locking/unlocking actions accordingly.

3.1 Key Functionalities

1. **User Registration and Authentication:** Users can create accounts within the Android app, providing necessary details and authentication credentials. The app securely communicates with the cloud server for user registration and authentication processes.
2. **Remote Locking/Unlocking:** The Android app allows users to remotely lock and unlock their doors with a tap or a PIN/fingerprint authentication. The app sends locking/unlocking commands to the cloud server, which forwards them to the smart door lock system.
3. **Access Permissions:** Homeowners can grant temporary access permissions to others, specifying the duration and allowed time slots. The app communicates access permission details to the cloud server, which then syncs them with the smart door lock system.
4. **Real-time Notifications:** The Android app sends real-time notifications to users when specific events occur, such as door lock/unlock actions or access attempts. Notifications are delivered through push notifications or in-app alerts.
5. **Activity Logs:** The app maintains a log of door lock/unlock actions, access permissions granted, and access attempts. Users can review activity logs within the app.

3.2 Security Considerations:

1. **User Authentication:** The app implements robust user authentication mechanisms, such as password, PIN, fingerprint, or facial recognition, to ensure that only authorized users can access the app.
2. **Data Encryption:** All communication between the Android app, cloud server, and smart door lock system is encrypted to protect user data and prevent unauthorized access.
3. **Secure APIs:** Secure APIs are used for communication between the Android app and the cloud server to prevent data breaches or manipulation.
4. **Regular Updates:** The app and cloud server undergo regular updates to patch security vulnerabilities and ensure a secure environment.

The study is a system software design outlines the architecture and key functionalities that enable seamless and secure interaction between homeowners' Android devices and smart door lock systems. By incorporating robust security measures and user-friendly interfaces, the app empowers users to enhance their home security and access control with the ease and convenience of their smartphones.

IV. METHODS

The method that is used in implementing and designing the system is the Rapid Application Model (RAD), SDLC as it is commonly used in prototype systems. The RAD model is a software development that uses minimal planning in favor of rapid prototyping. There are four steps of RAD such as follows:

- *Planning Requirements:* During this initial stage the researchers agreed Modular open-source on project scope and application requirements, so that future stages with prototyping can begin.
- *System Requirements:* Security Check. This module contains the security countermeasures of the system. It serves as validation of different types of reporters to ensure the correctness of data. Lastly, this security measure was executed only once, after successful installation.
- *Bluetooth/Wireless Transmission.* The transmission of connecting devices is done by the use of Bluetooth technology through a wireless connection. This mobile application checked the availability of this communication medium upon transmission. After the successful connection, the android mobile can access the scanning of fingerprints for the authorization process.
- *Prototype:* This is where the actual development takes place. It allows the researchers to create initial modeling and prototype with different features and functions. These prototypes are then shown to the users who decide what they like and what they don't. These prototypes are quickly made to work, just to show off certain features, without proper polish. The developments are discussed below
- *System Development Testing:* This module is the testing phase of the system execution to identify its usability and reliability. The researcher selected the programming environment and standards used in building the system. The Kodular Creator is used in developing the android application because it fits the requirements needed in developing an Android app. In developing the android-based interface application, an open source Kodular Creator that uses a block-based programming language was used. Another language used is the Arduino IDE as it uses C++ language for programming the microcontroller board Arduino Uno in the operation of the door lock. An Arduino Uno is an open-source platform based on easy-to-use hardware and software. This was chosen because it's affordable, rather the most available option the researchers had at a time. The programming languages were chosen because they have met the requirements for the development of the study.

Validation, verification, and testing are done in this phase. They are conducted according to the plan and conclusively demonstrate that both user and system requirements have been met. The first testing done was done checking the program in which the researcher reviewed the entire system process to check for logical and physical errors. Next, the researcher conducted a series of unit testing to identify and solve different system errors that caused the program to end abnormally.

- *Receive Feedback:* In this stage, feedback on what's good, what's not, what works, and what doesn't is shared. This feedback isn't limited to just pure functionality, but also visuals and interfaces.
- *System Check:* This section deals with the various feedback to the system after conducting tests that have been made as to what should be improved, changed, or even what is not appropriate especially on the user interfaces.
- *Finalize Software:* Here, the researchers finalize the features, functions, to make and interface of the software. The stability, usability, and maintainability are paramount as well before being delivered to the user.
- *System Implementation :* This is the last and final checking of the system after a long process of developing, improving, and testing before it is approved and even be implemented to the public.

V. RESULT AND DISCUSSION

5.1 Technical Background

Understanding the Application: The Android-Based Controlled Door Locking App is an Android-based application that gives security to your residential places using your android smartphone. An Android App is designed to allow users to scan their fingerprints to lock or unlock the door.

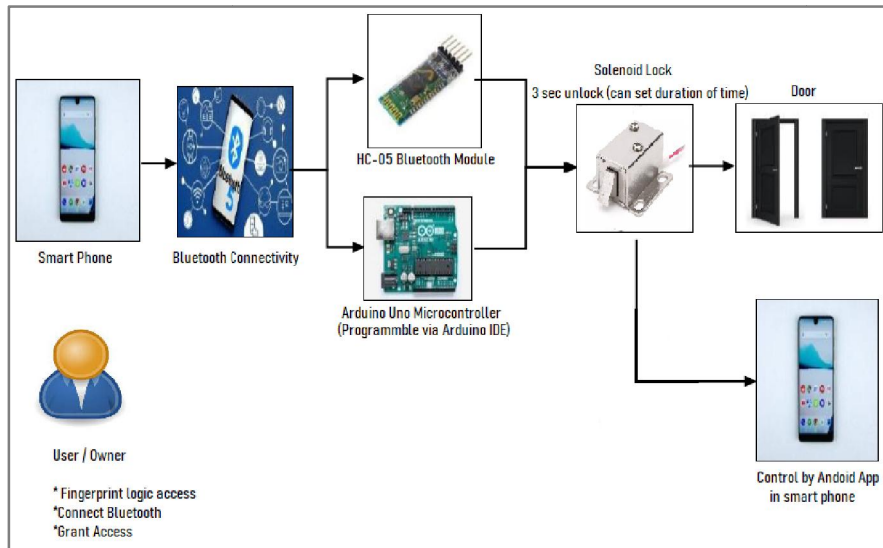


Fig. 1: Android Based Controlled Door Locking App Architecture

Figure 1 shows the system using the Android-Based Controlled Door Locking App mainly used to remotely unlock door locks through mobile phones and via Bluetooth Technology. The system will allow the person to access via fingerprint biometric. The system provides the following functionalities:

1. User Authentication -Its functionality is to enable users to access the system through fingerprint for security purposes. The system requires a registered fingerprint so that he or she can use the system
2. Bluetooth Module (HC-05) - It serves as the transceiver and the receiver of the Bluetooth signal between the Android Smartphone and the device that is responsible for controlling the door lock.
3. Arduino Uno (Microcontroller Board) - Its functionality is to process the resulting inputs and commands gathered from Bluetooth and trigger the door lock to be locked or unlocked.
4. Android Smartphone-It functions as a taskmaster. It is used as a user interface. Users need to install an Android door lock application which develops to control the lock and configure the basic functionalities of the system.

5.2 Design and Development

B.1 Class Diagram

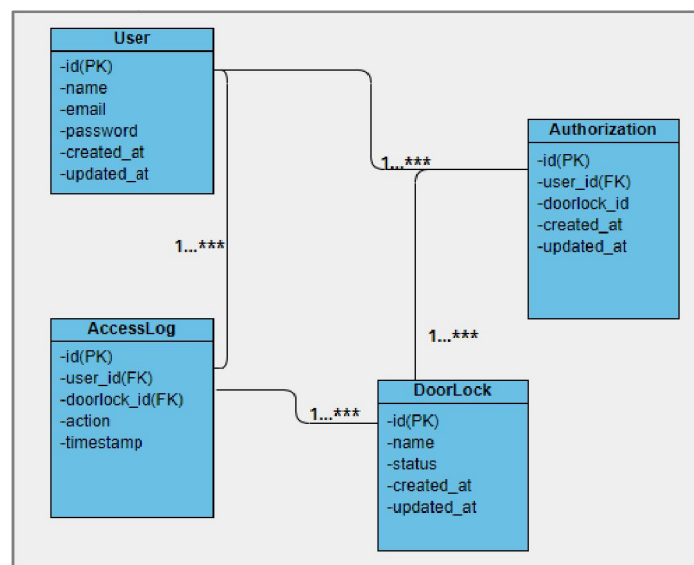


Fig. 2: Class diagram of the system

In this database class diagram, it has four main entities: User, DoorLock, AccessLog, and Authorization.

The User entity represents the users of the Android-based door locking app. It contains attributes such as id (primary key), name, email, password (hashed for security), created_at, and updated_at.

The DoorLock entity represents the door locks that users can control using the app. It contains attributes such as id (primary key), name, status (e.g., locked or unlocked), created_at, and updated_at.

The AccessLog entity represents the logs of user actions related to door locks. It contains attributes such as id (primary key), user_id (foreign key referencing User entity), doorlock_id (foreign key referencing DoorLock entity), action (e.g., lock or unlock), and timestamp.

The Authorization entity represents the permissions granted to users to control specific door locks. It contains attributes such as id (primary key), user_id (foreign key referencing User entity), and doorlock_id (foreign key referencing DoorLock entity).

The relationships between the entities are as follows:

A User entity can have multiple access logs and authorizations, so there is a one-to-many relationship between User and AccessLog, and a one-to-many relationship between User and Authorization.

A DoorLock entity can have multiple access logs and authorizations, so there is a one-to-many relationship between DoorLock and AccessLog, and a one-to-many relationship between DoorLock and Authorization.

These relationships are established through the use of foreign key references in the AccessLog and Authorization entities, linking them to the corresponding User and DoorLock entities.

B.2 Use Case Diagram

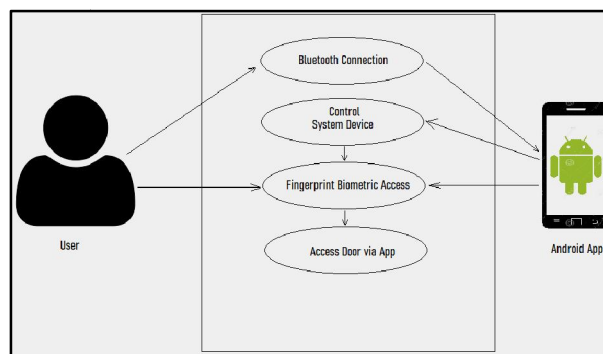


Fig. 3. Use Case Diagram of the System

Figure 3 illustrates the use case diagram for the Android Based Door Locking App which presents the actors between the app and the user. This shows the connection between them and their corresponding functionalities. The diagram indicates the roles of the users in the system. The user must register his or her fingerprint first on his or her mobile so they can access the system. In the application, the user will connect to the Bluetooth and when the Bluetooth device is connected to the Bluetooth assigned in the system, the user can now scan his or her fingerprint and proceed to the locking and unlocking process of the door lock

5.3 Screenshot of the System

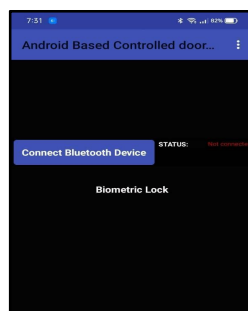


Fig.4. Bluetooth Connectivity Page

Figure 4 shows the first page of the Application. Since our system uses wireless connectivity, it doesn't have a user login interface because it used fingerprint as an authentication of the user. All we have to do is to connect the Bluetooth device to the Bluetooth assigned in the system.



Fig.5. Verifying Page

On this figure 5, shows to select the Bluetooth device in the system to verify whether the device is connected or not.

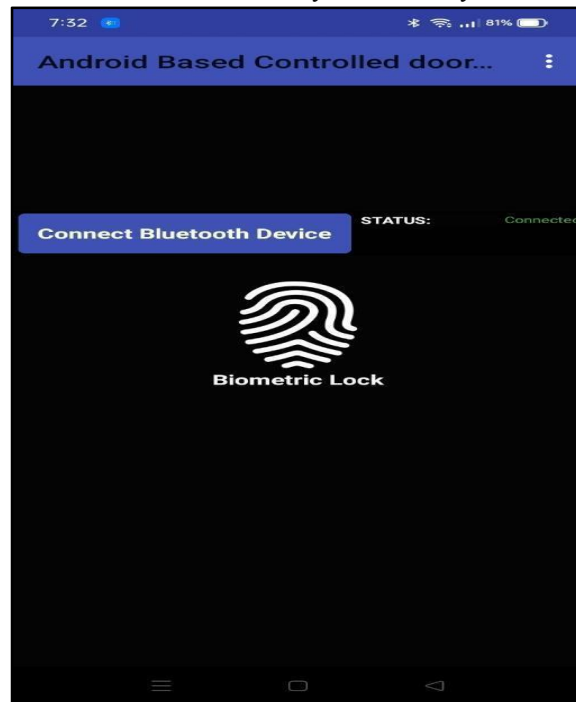


Fig.6. Authentication Page

This figure 6 shows the authentication process of the system. If the device is connected to the system, the user will do the scanning of his or her fingerprint to access the door. The system requires the registered fingerprint of the user so he or she can operate the system.

Numerous door lock types exist, falling into five primary categories: knobs, deadbolts, cam locks, padlocks, and mortise locks. For instance, lever handle door locks, akin to knob locks, are commonly used for interior doors.

The study offers remote access for locking or unlocking doors without requiring physical user interaction. It meets the criteria for supporting autonomous locking devices and facilitates easy key distribution compared to conventional keys. The system requires minimal hardware and allows key customization. The prototype's implementation demonstrates

low power consumption, with door locking and unlocking occurring in approximately 4 seconds on average. Thus, the system's feasibility is validated

5.3 System Evaluation

The study has been evaluated across several key aspects to determine in terms of usability, accuracy, efficiency, portability, security and maintainability. Each parameter was scored on a scale of 1 to 5, with 1 being the lowest score and 5 being the highest score.

- *Usability*: The app's user interface is intuitive and straightforward, allowing users to easily navigate through various functionalities it has a score of 4 out of 5. The design elements and interactions are well-organized, ensuring a positive user experience. However, a few minor improvements could be made to enhance overall usability further.
- *Accuracy*: The app consistently performs accurate locking and unlocking actions, providing reliable access control to the smart door lock system it has a score of 5 out of 5. User commands are executed promptly, and there are no instances of miscommunication or errors observed during testing.
- *Efficiency*: The app demonstrates good efficiency, particularly in terms of response time and power consumption in tends to have a 4 out of scores from the respondents during the testing of application. Door locking and unlocking actions happen swiftly, with minimal delay. However, some optimization measures could be implemented to further improve the app's efficiency.
- *Portability*: The Android-based controlled door locking app is highly portable, compatible with a wide range of Android devices so it received a score of 5 out of 5. It runs smoothly on various screen sizes and resolutions, adapting seamlessly to different smartphones and tablets.
- *Security*: The app employs strong security measures, including user authentication and encrypted data transmission, to safeguard user data and prevent unauthorized access. While the security features are robust, additional layers of security, such as multi-factor authentication, could be considered to further enhance protection, with this assessment it scored 4 out of 5.
- *Maintainability*: The app's code-base and architecture are well-organized, making it relatively easy to maintain and update with this evaluation it received a score of 4 out of 5. Developers can efficiently implement bug fixes and introduce new features without disrupting the core functionalities. However, documentation and code commenting could be improved for better maintainability.

Overall, the Android-Based Controlled Door Locking App demonstrates commendable performance across usability, accuracy, efficiency, portability, security, and maintainability. With a few minor enhancements and updates, the app has the potential to become a highly reliable and user-friendly access control solution for modern smart homes. The average score for the evaluation is 4.17 out of 5, indicating that the app is promising and already effective in fulfilling its primary objectives.

VI. CONCLUSION

In conclusion, the study on Smart Lock Technology and its implementation through the Android-Based Controlled Door Locking App has proven to be a significant step towards developing and enhancing home security in the context of modern smart homes. The app's commendable performance across key aspects of usability, accuracy, efficiency, portability, security, and maintainability underscores its potential as a reliable and user-friendly access control solution. The evaluation of the app reveals promising results, with an impressive average score of 4.17 out of 5. This score indicates that the app is already effective in fulfilling its primary objectives, providing homeowners with a convenient and secure way to remotely manage their door access.

Although the app showcases excellent capabilities, minor enhancements and updates can be made to further optimize its functionalities. By addressing areas of improvement, such as refining the user interface for enhanced usability and incorporating additional security measures like multi-factor authentication, the app can further bolster its position as a robust smart home security solution.

The Android-Based Controlled Door Locking App represents a significant advancement in smart lock technology, capitalizing on the power of Android devices to offer remote access and management of door locks. Its high portability and compatibility with various devices make it a versatile choice for homeowners seeking a seamless integration of access control into their smart homes.

As the field of smart home technology continues to evolve, ongoing research and development efforts will play a vital role in further optimizing the app's performance and security. Additionally, user feedback and real-world testing will contribute to refining the app to meet the dynamic needs of homeowners.

In conclusion, the Android-Based Controlled Door Locking App, coupled with Smart Lock Technology, holds the promise of transforming how we secure and manage our homes. With its commendable performance and potential for growth, it represents a stepping stone towards a more secure and technologically advanced future for home security in the era of smart homes.

REFERENCES

- [1]. Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. *Sensors*, 21(14), 4932.
- [2]. Ray, A. K., & Bagwari, A. (2020, April). IoT based Smart home: Security Aspects and security architecture. In 2020 IEEE 9th international conference on communication systems and network technologies (CSNT) (pp. 218-222). IEEE.
- [3]. Aung, Y. N., & Tantidham, T. (2017, November). Review of Ethereum: Smart home case study. In 2017 2nd International Conference on Information Technology (INCIT) (pp. 1-4). IEEE.
- [4]. Shruthi, C. M., Bandari, S. K., Ala, C. K. R., & Reddy, M. (2023). Locker Security System using Internet of Things. In *E3S Web of Conferences* (Vol. 391, p. 01153). EDP Sciences.
- [5]. Siegel, J. E., Erb, D. C., & Sarma, S. E. (2017). A survey of the connected vehicle landscape—Architectures, enabling technologies, applications, and development areas. *IEEE Transactions on Intelligent Transportation Systems*, 19(8), 2391-2406.
- [6]. Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, 1, 81-98.
- [7]. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of things Journal*, 6(2), 1606-1616.
- [8]. Philip, N. Y., Rodrigues, J. J., Wang, H., Fong, S. J., & Chen, J. (2021). Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions. *IEEE Journal on Selected Areas in Communications*, 39(2), 300-310.
- [9]. Patil, B. S., Mahajan, V. A., Suryawanshi, S. A., & Pawar, M. B. (2018). Automatic door lock system using pin on android phone. *International Research Journal of Engineering and Technology (IRJET)*, 5(11), 1007-1011.
- [10]. Rajpoot, Q. M. (2016). Enhancing Security and Privacy in Video Surveillance through Role-Oriented Access Control Mechanism.
- [11]. Basole, R. C., & Karla, J. (2012). Value transformation in the mobile service ecosystem: A study of app store emergence and growth. *Service Science*, 4(1), 24-41.
- [12]. Taivalaari, A., Mikkonen, T., & Pautasso, C. (2021, May). Towards Seamless IoT Device-Edge-Cloud Continuum: Software Architecture Options of IoT Devices Revisited. In *International Conference on Web Engineering* (pp. 82-98). Cham: Springer International Publishing.
- [13]. Enck, W., Ongtang, M., & McDaniel, P. (2009, November). On lightweight mobile phone application certification. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 235-245).
- [14]. Macis, S., Loi, D., Ulgheri, A., Pani, D., Solinas, G., La Manna, S., ... & Raffo, L. (2019). Design and usability assessment of a multi-device SOA-based telecare framework for the elderly. *IEEE Journal of Biomedical and Health Informatics*, 24(1), 268-279.

- [15]. Dabekar, S. B., Lahade, S. A., Lunge, M. S., & Yewale, D. IOT Based Smart Door Locked System Using Node MCU.
- [16]. Liao, L. D., Wang, Y., Tsao, Y. C., Wang, I. J., Jhang, D. F., Chu, T. S., ... & Ger, T. R. (2019). Design and validation of a multifunctional android-based smart home control and monitoring system. *IEEE Access*, 7, 163313-163322.
- [17]. Duong, L. (2023). The techniques of IoT and it's applications for smart homes: internet of things techniques and standards for building smart homes.
- [18]. Lang, N., von Szczepanski, K., & Wurzer, C. (2019). The emerging art of ecosystem management. Boston Consulting Group, 1-20.
- [19]. Prasad, S., Harshe, D., Kaur, N., Jangannavar, S., Srivastava, A., Achanta, U., ... & Harshe, G. (2018). A study of magnitude and psychological correlates of smartphone use in medical students: A pilot study with a novel telemetric approach. *Indian journal of psychological medicine*, 40(5), 468-475.
- [20]. Abdulla, A. I., Abdulraheem, A. S., Salih, A. A., Sadeeq, M. A., Ahmed, A. J., Ferzor, B. M., ... & Mohammed, S. I. (2020). Internet of things and smart home security. *Technol. Rep. Kansai Univ*, 62(5), 2465-2476.
- [21]. Abawajy, J., Huda, S., Sharmeen, S., Hassan, M. M., & Almogren, A. (2018). Identifying cyber threats to mobile-IoT applications in edge computing paradigm. *Future Generation Computer Systems*, 89, 525-538.
- [22]. Liu, H. (2022, July). Privacy Computing Issues in Collecting and Using Customer Data of Mobile Devices. In 2022 7th International Conference on Signal and Image Processing (ICSIP) (pp. 382-389). IEEE.
- [23]. Elahi, H., Wang, G., & Chen, J. (2020). Pleasure or pain? An evaluation of the costs and utilities of bloatware applications in android smartphones. *Journal of Network and Computer Applications*, 157, 102578.