Ceddi Journal of Information Systems and Technology (JST) *ISSN:2829-808X(print)*
Vol. 3 No. 2 December (2024) *ISSN:2829-6575(online)*
https://doi.org/10.56134/jst.v3i2.77

Public Room Door Locking System Using Wireless Technology and Internet of Things

Mahmud Mustapa[1], Irwan[2], Ummiati Rahmah[3], Akbar Iskandar[4*], Ahmed J. Obaid[5]

[1,3]Electronics Engineering Education, Universitas Negeri Makassar, Indonesia
[2]Informatics Engineering, Universitas Teknologi Akba Makassar, Makassar, Indonesia
[4]Information Technology Education, Universitas Teknologi Akba Makassar, Makassar, Indonesia
[5]Informatics Engineering, National University of Science and Technology, Najaf, Iraq

Abstract

Enhancing the efficiency and security of public spaces has become increasingly important, leading to the development of an automatic door lock system utilizing wireless technology and the Internet of Things (IoT). This study aims to design and implement a smart door lock system that provides automated control and improves convenience in managing public room access. The research methodology involves programming the ESP32 microcontroller, integrating IoT applications, and conducting various testing methods. These include manual control through physical switches, automated control via the Sinric Pro platform, and Wi-Fi hotspot-based control using the ESP32 module. Comprehensive hardware and software testing was carried out to ensure system reliability and functionality. The results indicate that the proposed system enables seamless control of public room doors through multiple methods, including an Android-based application and Wi-Fi connectivity. By leveraging IoT technology, the system offers a user-friendly, efficient, and secure solution for managing public space access, addressing modern requirements for convenience and safety.

Keywords: Public Room Door Locking System; Wireless Technology; Internet of Things (IoT); ESP32 Microcontroller; Automated Door Control.

Received: 19 January 2024 Revised: 20 March 2024 Accepted: 29 November 2024

Introduction

Public space security is an important aspect that is of concern in various sectors, such as offices, educational institutions, and public facilities (Gozal, 2021; Guard, 2019; Editor, 2024; Bowers & Manzi, 2006; Button, 2003). Traditional locking systems that use physical keys are often inefficient and prone to problems such as key loss, illegal duplication, and limited accessibility (Locstar, 2024; Pratiwi & Setiawan, 2021; Salam & Bhaskoro, 2021; Wicaksono, 2024). This problem raises the need for more innovative solutions to improve efficiency and security in managing access to public spaces. In this context, wireless technology and the Internet of Things (IoT) emerge as alternatives that offer flexibility and ease in managing room-locking systems (Amane et al., 2023; Rachmad et al., 2023; Visayas et al., 2024).

Wireless technology provides the ability to access and control devices without the need for a direct physical connection (Afra, 2023; Dwi, 2014; Rizki, 2023). While IoT allows devices to connect and communicate with each other via the internet network (Hildayanti & Machrizzandi, 2020; Abdul-Qawy et al., 2015; Alam, 2023; Bello & Zeadally, 2014). The combination of these two technologies provides a great opportunity to develop a more modern, practical, and efficient public room locking system (Shammar & Zahary, 2020; Zheng & Carter, 2015). By utilizing IoT, managers can monitor and control access in real-time through an integrated application, thereby minimizing the risk of losing physical keys and increasing control over who can access a particular room (Anggono et al., 2023; Erwin et al., 2023; Fauzi et al., 2023).

Efficiency is one of the main factors underlying the importance of innovation in room-locking systems (Ablo, 2011; Gann, 2000; Hekkert et al., 2007). The use of wireless and IoT technology allows access to the room to be done in a faster and easier way, such as via a smartphone device or RFID card connected to a cloud system (Domb, 2019; Dudhe et al., 2017; Tan & Sidhu, 2022; Sari et al., 2023; (Ansyah & Winardi, 2022). In addition, this technology also supports the collection of room usage data, which can be analyzed to improve space management and decision-making (Sulistiyo

*Corresponding author.
E-mail address: akbar.iskandar@gmail.com (Akbar Iskandar)

et al., 2021). This is especially relevant in public spaces that are used by many people at different times (Adidrana et al., 2023).

In addition to efficiency, security aspects are also a major concern. IoT-based locking systems can be equipped with data encryption and user authentication features to prevent unauthorized access (Hasan et al., 2024; Pratama et al., 2024; Sahlan, 2024). This system also allows for automatic notification or alarm in the event of a break-in attempt. Thus, this technology not only provides convenience but also provides better protection compared to traditional locking systems (Kurniawan et al., 2021; Fikri & others, 2023; Maulana & others, 2024).

The development of a public room locking system based on wireless and IoT technology is in line with the digital transformation trend that continues to grow in various sectors such as research.The Last Supper (2022)with the title Design of Automatic Room Door Security System Using RFID Based on Internet of Things (IoT) and research Salihi & Rainbow (2022) with the title of Automatic Door Control System for Computer Science Faculty Rooms Based on IoT. This reflects the need for technology integration in everyday life, including in terms of security and space management. Therefore, this study aims to design and implement a public room locking system that utilizes wireless and IoT technology to address the problems of efficiency and security in managing access to public spaces.

Method

The analysis method employed in this research focuses on examining the requirements of the existing system, identifying its weaknesses, and determining the necessary components for system development (Ramdhan et all, 2021; Setyosari, 2010; Tersiana, 2018). The analysis process consists of two primary aspects.

System Weakness Analysis
This stage aims to identify issues in conventional systems, such as the inefficiency of manual door opening, which requires additional time and energy. To address this, the study proposes an Internet of Things (IoT)-based tool that enables automatic control of public room doors via Wi-Fi and smartphones. This system can also operate offline using hotspot tethering, ensuring flexibility and reliability.

System Needs Analysis
This involves identifying hardware, software, and information requirements. Hardware needs encompass the minimal and optimal specifications to support the software, while software needs include data processing applications tailored for the system. Information requirements focus on ensuring effective automatic door lock control through smartphone applications and Wi-Fi facilities.

System Design
The design phase provides a detailed functional overview of the proposed automatic public room door locking system, as depicted in Figures 1 and 2.

Figure 1: Flowchart
The system begins by initializing the ESP32 microcontroller and the door lock device. The ESP32 connects to the office Wi-Fi network as its internet source. When a user enters the Wi-Fi range, the system verifies whether the MAC address of the user’s smartphone is registered. If the MAC address is not registered, the door remains locked. If the MAC address is registered, the door lock opens automatically. This allows users to control the door lock through the internet or hotspot tethering.

Figure 2: Hardware Architecture Design
The ESP32 serves as the core microcontroller for the automatic locking system. When the ESP32 detects a wireless smartphone, it activates the solenoid to unlock the door, accompanied by a buzzer sound. Additionally, the system can be controlled via SMS using the SIM800L module, providing an alternative communication method for enhanced usability.

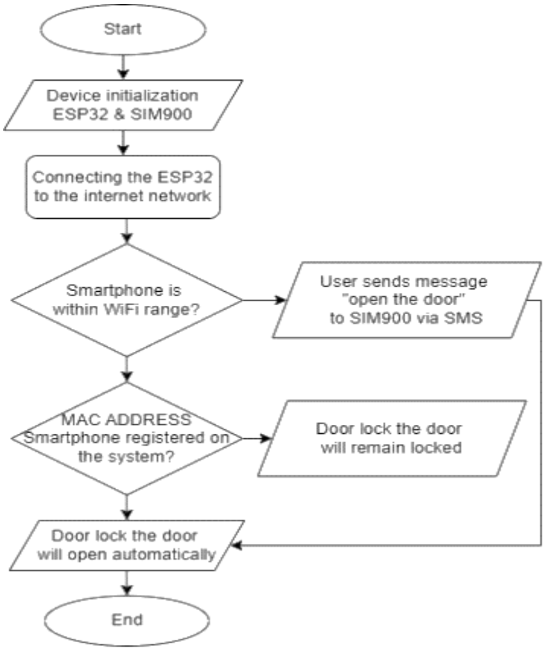


Figure 1. Flowchart

The flowchart illustrates the operational process of the automatic door lock system, integrating the ESP32 microcontroller and SIM900 module for dual control functionality: Wi-Fi and SMS-based control.

Start
The process begins with the initialization of the ESP32 microcontroller and the SIM900 GSM module. These devices prepare the system to establish connections and execute commands.

Connecting to the Internet Network
After initialization, the ESP32 connects to the designated internet network, which serves as the primary communication channel for the IoT functionality.

Check Smartphone Wi-Fi Range
The system then checks whether the user's smartphone is within the Wi-Fi range of the ESP32 module. If the smartphone is not detected, the system remains idle and waits for a valid connection.

Verify Smartphone MAC Address
If the smartphone is within Wi-Fi range, the system verifies whether the MAC address of the smartphone is registered in the system's database:
If the MAC address is registered, the system proceeds to unlock the door automatically.
If the MAC address is not registered, the door remains locked, ensuring unauthorized users cannot access the room.

SMS Command Alternative
In addition to Wi-Fi-based control, the user can send an SMS command ("open the door") to the SIM900 module to manually unlock the door. This provides an alternative access method, especially in scenarios where Wi-Fi is unavailable.

Unlock the Door
If the MAC address is verified or the SMS command is received, the system activates the door lock mechanism to unlock the door automatically, allowing the user to enter.

End:
The process completes, and the system resets to monitor further commands or user interactions.

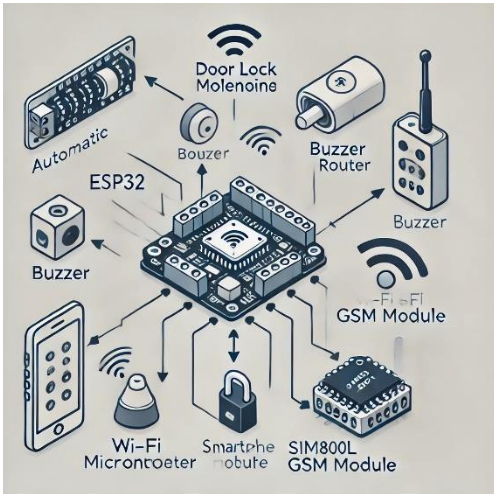


Figure 2. Hardware architecture design

In Figure 2 above, the ESP32 functions as the central microcontroller, or "brain," of the automatic door-locking system. This system operates in two primary modes: wireless control via Wi-Fi and manual control via SMS.

Wireless Control (Wi-Fi)
When the ESP32 detects a smartphone within its Wi-Fi range, it verifies the device's MAC address to ensure it is registered in the system. If the MAC address is valid, the ESP32 sends a signal to activate the door lock solenoid, causing the door to unlock. At the same time, the buzzer sounds to indicate that the door has been successfully unlocked. This feature enables users to control the door lock remotely using their smartphones over the Wi-Fi network.

SMS Control (SIM800L)
In addition to Wi-Fi control, the system can be operated via SMS. The SIM800L GSM module receives an SMS command, such as "open the door," from a registered user. Upon receiving this message, the ESP32 processes the command and triggers the door lock solenoid to unlock the door. This method allows users to control the door lock even when they are outside of the Wi-Fi range. In summary, the system provides flexible and convenient control of the automatic door lock, either via a smartphone app over Wi-Fi or through SMS commands, ensuring ease of access for the user.

Results and Discussion

Results

This section presents the primary findings of the research on the public room door locking system, which is based on wireless technology and the Internet of Things (IoT). The goal of this research is to develop an innovative door-locking solution that is efficient, secure, and user-friendly. The designed system seamlessly integrates IoT devices with wireless connectivity to enable remote control and real-time monitoring (Hartawan & Sudiarsa, 2019; Leander et al., 2024).

The assembled system utilizes the ESP32 microcontroller, which serves as the central processing unit for the system, connecting to the internet via Wi-Fi. The key components of the system include an Electronic Door Lock, which functions as the main locking mechanism, and a power supply to ensure reliable operation. For user feedback, the system incorporates a buzzer that emits sound alerts when the door is locked or unlocked, enhancing its accessibility and ease of use.

The integration of Sinric Pro, a cloud-based IoT platform, allows users to control the door lock remotely via a smartphone application or through voice commands using virtual assistants like Amazon Alexa or Google Home. The system also supports offline operation through hotspot tethering, ensuring flexibility and reliability even in areas with limited internet connectivity. Furthermore, users can monitor the status of the door lock in real-time, providing an added layer of security and convenience. Overall, the results demonstrate that the system effectively combines IoT technology with wireless connectivity to create an automatic door-locking solution that is efficient, secure, and highly functional for public room access management. Figure 3, Overall Hardware Circuit illustrates the complete circuit, showing the interaction between the ESP32 microcontroller, the electronic door lock, the power supply, and other peripherals.

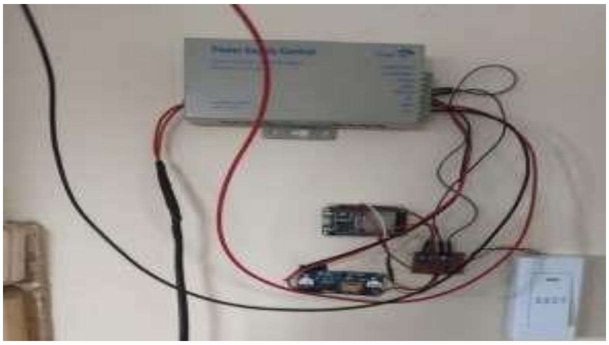


Figure 3. Overall hardware circuit

The software development process consists of two main stages: coding the ESP32 and utilizing Internet of Things (IoT) applications. ESP32 programming is carried out using the Arduino IDE with the C programming language, which includes commands to control the electronic door lock system. Meanwhile, the IoT application employed for this purpose is Sinric Pro, a cloud-based platform designed to simplify the development of IoT projects, particularly for smart home applications (MM Sari et al., 2024). Sinric Pro serves as the interface for opening and closing doors via an Android application.

Sinric Pro enhances smart home experiences by allowing users to connect and control IoT devices in multiple ways, including through voice commands via virtual assistants like Amazon Alexa and Google Home. The platform also provides a user-friendly mobile application, enabling users to manage devices conveniently anytime and anywhere. In this research, Sinric Pro facilitates seamless control of automatic door locks by integrating the application's unique app key and app secret with the ESP32 microcontroller. These credentials allow the application to trigger specific actions, directing commands to designated pins on the ESP32 for operation.

Sinric Pro supports both online and offline device control, enabling users to toggle devices on or off. It also allows users to add new devices to the system, with each device assigned a unique device ID that must be included in the Arduino code. Furthermore, users can generate new app keys and secrets, which act as authentication codes to establish a connection between the Arduino and the door lock control devices. The Wi-Fi network used by the ESP32 is generated by the device itself. To activate this Wi-Fi, the ESP32 must first be powered on. Once the device is active, its Wi-Fi becomes automatically available. Users can then connect to the ESP32 by entering the system password, which, for this research, is set to 11112222.

Discussion

This section discusses the testing process and outcomes of the public room door-locking system, aiming to evaluate whether the implemented system meets the planned specifications and design. The results provide insights into the system's performance, identifying areas for refinement and future development. The system was tested in two main aspects: manual control and automatic control. Table 1 illustrates the results of manual and automatic control testing for the door's open and closed conditions.

Manual Control Testing

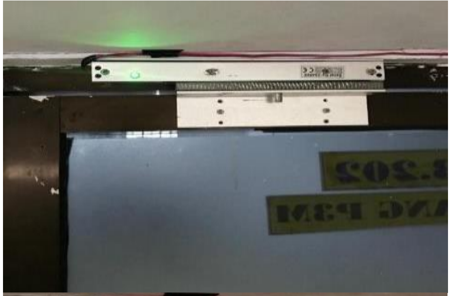
The system was tested using a physical switch to manually control the door's open and closed conditions. The switch performed as expected, with the door successfully locking and unlocking when triggered manually. This test validates the reliability of the manual control mechanism as a backup option in scenarios where IoT-based control may not be feasible.

Sinric Pro Automatic Control Testing

The automatic control functionality was tested using the Sinric Pro application. Commands to open and close the door were sent through the application, with the ESP32 microcontroller processing these commands effectively. The door lock responded as intended, transitioning between open and closed states seamlessly. This confirms the success of the IoT-based control system and its ability to function reliably through Wi-Fi or hotspot tethering.

The results shown in Table 1 demonstrate that the system performed well under both manual and automatic control conditions. This testing verifies that the implemented design meets the specifications for reliable operation and usability. Additionally, these findings highlight the flexibility of the system, which can be operated through multiple control methods, offering convenience and robustness. This system was tested using a control system that has been created with the test results can be seen in Table 1.

Table 1. Manual control testing of open and closed condition switches

Testing	Results
Manual control switch open condition	
Manual control switch closed condition	
Sinric Pro automatic control open condition	

The test results presented in Table 1 demonstrate the performance of the door lock system (EM Lock) under various control conditions. During the manual control testing in the open condition, pressing the manual switch inside the room successfully unlocked the door, as indicated by the EM Lock light turning off. For the closed condition, after the door remains open for 5 seconds, the system automatically reactivates the lock, securing the door. This is visually indicated by the EM Lock light turning green, confirming the lock is active and the system's security feature is functioning as intended. In the automatic control testing using the Sinric Pro application, when the trigger in the application was set to "Off," the door unlocked successfully, as indicated by the EM Lock light turning off. These results highlight the system's ability to operate effectively in both manual and IoT-based automatic control modes.

This study's findings align with those of (Adella et al.,2020), who successfully adopted IoT technology for real-time door lock control. Similarly, (Adidrana et al., 2022) demonstrated the effectiveness and efficiency of integrating IoT into door lock systems. The current research further supports the practicality of IoT-enabled door locks, enhancing both convenience and security for users.

Conclusions and Suggestions

Conclusions

The automatic door lock control system represents a significant innovation aimed at improving energy efficiency and reducing the effort required to manage public room doors. Based on the findings of this study, titled "Public Room Door Locking System Using Wireless Technology and Internet of Things (IoT)," the system effectively replaces traditional manual methods with advanced technological solutions. The results demonstrate that the system enables automatic control of public room door locks through multiple methods, including an Android application connected via a WiFi Hotspot.

Moreover, the integration of IoT technology enhances the system's accessibility, allowing it to be operated both online through IoT-based applications and offline via hotspot tethering. This dual connectivity ensures greater flexibility and reliability in managing public room doors. The implementation of such a system highlights the potential of IoT to revolutionize door lock technology, offering convenience, efficiency, and adaptability for various public spaces.

Suggestions

Based on the research titled "Public Room Door Locking System Using Wireless Technology and Internet of Things (IoT)," the author recommends optimizing the automatic door locking system by incorporating an auto-switch power mechanism. This enhancement would include the addition of a backup battery to ensure the system remains operational during power outages or when the primary power supply is unavailable. This improvement would increase system reliability and ensure continuous functionality, especially in critical situations where consistent access control is essential.

Contribution: The contributions of the following individuals are gratefully acknowledged. Irwan S. was responsible for the conceptualization, design, analysis, and writing of the manuscript. Akbar Iskandar & Ahmed J. Obaid contributed to the data analysis, interpretation, and statistical analysis. Mahmud Mustapa and Ummiati Rahmah played key roles in the critical revision of the manuscript, supervision, and editing/review. Their invaluable support and expertise were crucial in the completion of this research.

References

Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The internet of things (iot): An overview. *International Journal of Engineering Research and Applications*, *5*(12), 71–82.

Ablo, S. (2011). *The global leader in door opening solutions*.

Adella, A. F., Putra, M. F. P., Taufiqurrahman, F., & Kaswar, A. B. (2020). Sistem pintu cerdas menggunakan sensor ultrasonic berbasis internet of things. *Jurnal Media Elektrik*, *17*(3), 1–7. https://doi.org/https://doi.org/10.26858/metrik.v17i3.14958

Adidrana, D., Suryoprago, H., & Hakim, A. R. (2022). Perancangan Sistem Smart Door Lock Menggunakan Internet of Things (Studi Kasus: Institut Teknologi Telkom Jakarta). *Journal of Informatics and Communication Technology (JICT)*, *4*(2), 102–108. https://doi.org/https://doi.org/10.52661/j_ict.v4i2.141

Adidrana, D., Suryoprago, H., & Hakim, A. R. (2023). Perancangan Sistem Smart Door Lock Menggunakan Internet of Things (Studi Kasus: Institut Teknologi Telkom Jakarta). *Journal of Informatics and Communication Technology (JICT)*. https://api.semanticscholar.org/CorpusID:267054728

Afra, F. (2023). *Wireless*. Inet.Detik.Com. https://inet.detik.com/telecommunication/d-6925109/wireless-adalah-teknologi-koneksi-nirkabel-ini-cara-kerja-dan-kelebihannya

Alam, T. (2023). A reliable communication framework and its use in internet of things (IoT). *Authorea Preprints*.

Amane, A. P. O., Sos, S., Febriana, R. W., Kom, S., Kom, M., Artiyasa, I. M., Cahyaningrum, A. O., SE, M. M., Husain, S. T., Abror, M. N., & others. (2023). *Pemanfaatan dan Penerapan Internet Of Things (Iot) Di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.

Anggono, S. U., Siswanto, E., Fajri, L. R. H. A., & others. (2023). User Interface Berbasis Web Pada Perangkat Internet Of Things. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *3*(1), 35–54. https://doi.org/https://doi.org/10.51903/teknik.v3i1.326

Ansyah, M. F. A. T., & Winardi, S. (2022). Mesin Akses Ruangan Menggunakan Fingerprint Dan Rfid (Radio Frequency Identification) Berbasis Iot (Internet Of Things). *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*. https://api.semanticscholar.org/CorpusID:258118998

Bello, O., & Zeadally, S. (2014). Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal*, *10*(3), 1172–1182. https://doi.org/https://doi.org/10.1109/JSYST.2014.2298837

Bowers, B. S., & Manzi, T. (2006). Private security and public space: new approaches to the theory and practice of gated communities. *European Journal of Spatial Development*, *4*(4), 1–17.

Button, M. (2003). Private security and the policing of quasi-public space. *International Journal of the Sociology of Law*, *31*(3), 227–237. https://doi.org/https://doi.org/10.1016/j.ijsl.2003.09.001

Domb, M. (2019). Smart home systems based on internet of things. In *Internet of Things (IoT) for automated and smart applications*. IntechOpen. https://doi.org/https://doi.org/10.5772/intechopen.84894

Dudhe, P. V, Kadam, N. V, Hushangabade, R. M., & Deshmukh, M. S. (2017). Internet of Things (IOT): An overview and its applications. *International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2650–2653. https://doi.org/https://doi.org/10.1109/ICECDS.2017.8389935

Dwi. (2014). Wireless. *Metafora Indonesia Tehnology*.

Erwin, E., Datya, A. I., Nurohim, N., Sepriano, S., Waryono, W., Adhicandra, I., Budihartono, E., & Purnawati, N. W. (2023). *Pengantar & Penerapan Internet Of Things: Konsep Dasar & Penerapan IoT di berbagai Sektor*. PT. Sonpedia Publishing Indonesia.

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., Mm, P. I. A., Mulyanto, M. E., Dulame, I. M., Pramuditha, P., Sudipa, I. G. I., Kom, S., & others. (2023). *Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0*. PT. Sonpedia Publishing Indonesia.

Fikri, R., & others. (2023). Optimalisasi Keamanan Rumah dengan Implementasi Sistem Notifikasi Gerbang Cerdas Berbasis Internet of Things (IoT). *Journal of Computer System and Informatics (JoSYC)*, *4*(4), 816–829. https://doi.org/https://doi.org/10.47065/josyc.v4i4.4004

Gann, D. (2000). *Building innovation: complex constructs in a changing world*. Thomas Telford. https://doi.org/https://doi.org/10.1680/bicciacw.25967

Gozal, R. P. (2021). *Optimalisasi Sistem Akses Kontrol untuk Keamanan Gedung Perkantoran*. Adv.Kontan.Co.Id. https://adv.kontan.co.id/news/optimalisasi-sistem-akses-kontrol-untuk-keamanan-gedung-perkantoran-anda

Guard, B. (2019). *Mendesain Sistem Keamanan Gedung Perkantoran*. Bravo Satria Perkasa. https://www.bspguard.co.id/mendesain-sistem-keamanan-gedung-perkantoran/

Hartawan, I. N. B., & Sudiarsa, I. W. (2019). Analisis kinerja internet of things berbasis firebase real-time Database. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *2*(1), 6–17. https://doi.org/https://doi.org/10.31598/jurnalresistor.v2i1.371

Hasan, M. A., Turnandes, Y., & others. (2024). Rancang Bangun Sistem Keamanan Pintu Ganda menggunakan Password dan Sidik Jari Berbasis Internet of Things (IoT). *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer*, *3*(1), 221–237. https://doi.org/https://doi.org/10.51903/semnastekmu.v3i1.203

Hekkert, M. P., Suurs, R. A. A., Negro, S. O., Kuhlmann, S., & Smits, R. E. H. M. (2007). Functions of innovation systems: A new approach for analysing technological change. *Technological Forecasting and Social Change*, *74*(4), 413–432. https://doi.org/https://doi.org/10.1016/j.techfore.2006.03.002

Hildayanti, A., & Machrizzandi, M. S. (2020). Sistem Rekayasa Internet Pada Implementasi Rumah Pintar Berbasis IoT. *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar*, *6*(1), 45–51. https://doi.org/https://doi.org/10.35329/jiik.v6i1.143

Kurniawan, A., Tama, A. P., Sunni, F., & Febrianto, R. (2021). Kunci Pintu Pintar Terintegrasi Digital "EASY LOCK."

Journal of Entrepreneurship, Management and Industry (JEMI), *4*(2), 75–84. https://doi.org/https://doi.org/10.36782/jemi.v4i2.1991

Leander, D. E., Ashidiqie, M. F., & Udoyono, K. (2024). Perancangan Sistem Monitoring Jarak Jauh Pintu Pintar Rumah Indekos Berbasis Iot (Internet of Things) Menggunakan Platform Blynk. *Jurnal Teknologi Informasi Dan Komunikasi*, *17*(2), 66–79. https://doi.org/https://doi.org/10.47561/a.v17i2.265

Locstar. (2024). *Kunci pintar vs. kunci pintu tradisional: perbandingan dan evaluasi keamanan*. Shenzhen Locstar Technology Co. https://www.locstariot.com/id/blog/smart-locks-vs-traditional-door-locks-security-comparison-and-evaluation

Maulana, M. H., & others. (2024). *Rancang Bangun Keamanan Pintu Rumah Otomatis Menggunakan Sensor PIR Dan RFID Berbasis Iot*. UIN Ar-Raniry Fakultas Tarbiyah dan Keguruan.

Ningrum, N. K., & Basyir, A. (2022). Perancangan Sistem Keamanan Pintu Ruangan Otomatis Menggunakan Rfid Berbasis Internet of Things (IoT). *Jurnal Ilmiah Matrik*. https://api.semanticscholar.org/CorpusID:249363143

Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Kaizen Media Publishing.

Pratiwi, A., & Setiawan, S. R. D. (2021). *Smart Lock Vs Kunci Tradisional, Kelebihan dan Kekurangannya*. Kompas.Com. https://www.kompas.com/homey/read/2021/02/25/134043276/smart-lock-vs-kunci-tradisional-kelebihan-dan-kekurangannya

Rachmad, Y. E., Dewantara, R., Junaidi, S., Firdaus, M., Sulistianto, S. W., & others. (2023). *Mastering Cloud Computing (Foundations and Applications Programming)*. PT. Sonpedia Publishing Indonesia.

Ramdhan, M., & others. (2021). *Metode penelitian*. Cipta Media Nusantara.

Redaktur. (2024). *Cara Meningkatkan Standar Keamanan Gedung Kantor*. Intermezzo.Id. https://intermezzo.id/cara-meningkatkan-standar-keamanan-gedung-kantor/

Rizki. (2023). *Wireless*. R17.Co.Id. https://r17.co.id/insight/article/apa-itu-wireless-tujuan-manfaat-cara-kerja-dan-fungsinya

Sahlan. (2024). *Keamanan Data dalam Sistem IoT*. Nocola.Co.Id. https://nocola.co.id/id/keamanan-data-iot-nocola/

Salam, A., & Bhaskoro, S. B. (2021). Sistem Keamanan Cerdas pada Kunci Pintu Otomatis menggunakan Kode QR. *CYBERNETICS*, *5*(01). https://doi.org/10.29406/CBN.V5I01.2307

Salihi, I. A., & Pelangi, K. C. (2022). Sistem Pengontrol Pintu Otomatis Ruangan Fakultas Ilmu Komputer Berbasis Iot. *Jurnal Ilmiah Ilmu Komputer Banthayo Lo Komputer*. https://api.semanticscholar.org/CorpusID:249877561

Sari, I. P., Basri, M., Ramadhani, F., Manurung, A. A., & others. (2023). Penerapan Palang Pintu Otomatis Jarak Jauh Berbasis RFID di Perumahan. *Blend Sains Jurnal Teknik*, *2*(1), 16–25. https://doi.org/https://doi.org/10.56211/blendsains.v2i1.246

Sari, M. M., Aris, A., Luciana, T., Claudia, C., Nauvaldy, F., & Syahputra, F. R. (2024). Monitoring Pintu Ruangan Server Berbasis IOT. *Seminar Nasional Penelitian (SEMNAS CORISINDO 2024)*.

Setyosari, P. (2010). Metode penelitian dan pengembangan. *Jakarta: Kencana*.

Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): a survey of techniques, operating systems, and trends. *Library Hi Tech*, *38*(1), 5–66. https://doi.org/https://doi.org/10.1108/LHT-12-2018-0200

Sulistiyo, W., Rahardjo, P., Ardian, I. N., & Devina, R. D. K. (2021). *SIMACOL (Smart Access Control Room In Building) Dengan Sistem Kontrol Pintu Dan Monitoring Ruangan Serta Management Booking Ruangan Berbasis Iot Untuk Smart Bulding Energy Efficiency*. https://api.semanticscholar.org/CorpusID:244986460

Tan, W. C., & Sidhu, M. S. (2022). Review of RFID and IoT integration in supply chain management. *Operations Research Perspectives*, *9*, 100229. https://doi.org/https://doi.org/10.1016/j.orp.2022.100229

Tersiana, A. (2018). *Metode penelitian*. Anak Hebat Indonesia.

Visayas, V., Cakra, C., & Supit, Y. (2024). Sistem Kontrol Alat Elektronik Dalam Rumah Berbasis Internet Of Things (Iot). *Simtek: Jurnal Sistem Informasi Dan Teknik Komputer*, *9*(2), 249–261. https://doi.org/https://doi.org/10.51876/simtek.v9i2.1163

Wicaksono, M. A. (2024). *Mengapa Kunci Pintu Rumah Digital Onassis Lebih Aman?* Www.Onassis-Hardware.Com. https://www.onassis-hardware.com/article/kunci-pintu-rumah-digital/

Zheng, D. E., & Carter, W. A. (2015). *Leveraging the internet of things for a more efficient and effective military*. Rowman & Littlefield.