IJIO
(International Journal of Industrial Optimization)
ISSN 2723-3022 (online) | 2714-6006 (printed)
Vol 6, No. 2, 182-194
https://doi.org/10.12928/ijio.v6i2.12892

# Smart door lock design and development using the pahl and beitz approach

Rizky Reynaldy Brahmana *, Mochamad Tutuk Safirin

Department of Industrial Engineering, Faculty of Engineering, Universitas Pembangunan Nasional Veteran Jawa Timur, Indonesia
* Corresponding Author: rbubem@gmail.com

ARTICLE INFO

**Article history**
Received: March 11, 2025
Revised: May 2, 2025
Accepted: May 20, 2025

**Keywords**
Smart door lock;
IoT;
RFID;
Security system;
Product development.

ABSTRACT

Security vulnerabilities in conventional locks and existing smart locks necessitate innovative solutions that integrate robust authentication mechanisms. This study addresses the research gap by developing a smart door lock system that uniquely combines Indonesia's government-issued e-KTP (embedded with an RFID chip) and a capacitive touch sensor for multi-factor authentication, enhancing security while ensuring universal accessibility. The design process employs the Pahl and Beitz systematic engineering methodology, emphasizing iterative optimization through planning, conceptual design, embodiment design, and detail design phases. Key specifications, including e-KTP compatibility, cost-effectiveness <IDR 1 million, and energy efficiency, were prioritized. Prototype evaluations revealed that the final design achieved superior functionality, scoring 87/100 in a multi-criteria assessment. The assessment considered components, space, aesthetics, cost, and manufacturability. The system integrates an Arduino Nano Microcontroller, a 9V battery with a 17-day lifespan, and IoT connectivity for real-time feedback. Comparative analysis demonstrates a 40–60% cost reduction compared to commercial alternatives, alongside tamper-resistant advantages from e-KTP integration system, modularity potential, and rechargeable battery. This study underscores the viability of leveraging national ID systems in IoT security frameworks, offering policymakers and manufacturers actionable insights for scalable, standardized smart home solutions.



## 1. Introduction

Security remains a critical concern in residential areas as conventional locking systems become increasingly vulnerable to unauthorized access. Traditional mechanical locks, while widely used, are susceptible to duplication, bumping, and forced entry, thereby heightening security risks [1], [2]. The increasing incidents of break-ins and unauthorized access in residential areas necessitate the development of advanced security mechanisms to enhance home protection [3]. In recent years, the adoption of smart locks has significantly improved home security by enabling remote access, real-time monitoring, and automated control features [4], [5]. These innovations allow home-owners to manage access to their premises more efficiently [6]. However, despite these advancements, security threats such as hacking, unauthorized RFID tag duplication, and system vulnerabilities persist.

Cybercriminals continue to exploit weaknesses in authentication mechanisms, highlighting the need for more robust security frameworks [7], [8]. Despite advancements in smart locks, existing solutions lack the ability to integrate with government-issued, tamper-resistant authentication tools like Indonesia's e-KTP [9]. This gap limits both security and accessibility in resource-constrained settings.

This study addresses the identified gap by using real-time rechargeable power supply to enhance system resilience, employing multi-factor authentication via Indonesia's e-KTP RFID and capacitive touch sensors for robust security, and rigorously applying the Pahl and Beitz methodology to guide the systematic design process [10]. Unlike proprietary access cards or smartphone-based systems, the e-KTP offers a unique combination of universal availability, tamper-resistant design, and government-backed security, making it an ideal candidate for IoT-based access control [11]. Furthermore, the integration of capacitive touch sensors for internal access and an LCD interface for real-time feedback enhances usability and functionality, setting this system apart from existing solutions [12].

The design and development process follows the Pahl and Beitz systematic design methodology, a structured approach that systematically optimizes the design process by balancing functionality, feasibility, and user-centric innovation [13]–[15]. This methodology ensures that the final product not only meets technical specifications but also aligns with user needs and manufacturing constraints [16]. By applying this framework, the study systematically addresses design challenges, optimizes component selection, and ensures the robustness of the final prototype [17], [18].

The design and development process in this study adhered to the Pahl and Beitz systematic engineering methodology, a structured framework renowned for balancing technical rigor with user-centric innovation. This methodology progresses through four iterative phases: planning, conceptual design, embodiment design, and detail design to systematically address functional requirements, feasibility constraints, and optimization opportunities [19]–[21]. During the planning phase, critical design specifications were established, including cost limitations (<IDR 1 million), e-KTP compatibility, and energy efficiency targets. The conceptual design phase generated three prototypes, evaluated through weighted criteria (e.g., component space, aesthetics), while the embodiment design phase utilized SolidWorks simulations to refine spatial integration and electromagnetic compatibility. Finally, the detailed design phase finalized material selections, manufacturing workflows, and power management strategies, ensuring the final prototype met both security and affordability benchmarks [22].

The adoption of SolidWorks 2017 further streamlined the design process by enabling precise 3D parametric modeling, assembly simulations, and virtual validation of electromechanical integration. Leveraging its advanced tools, such as spatial optimization algorithms and cable routing utilities, the software facilitated iterative refinement of component layouts to ensure ergonomic accessibility, electromagnetic compatibility, and manufacturability [23], [24]. This digital prototyping environment aligned seamlessly with the Pahl and Beitz framework, allowing systematic validation of functional requirements during the embodiment and detail design phases [25]. By simulating real-world constraints such as spatial conflicts, material stress, and power distribution, SolidWorks enhanced the prototype's reliability while minimizing physical prototyping costs [26]–[28]. Its integrated design-analysis capabilities ensured that the final layout adhered to both user-centric and technical specifications, underscoring its pivotal role in bridging conceptual innovation and practical implementation.

The proposed IoT-based Smart Door Lock integrates an RFID reader to authenticate e-KTP data, a capacitive touch sensor for internal access, and an LCD interface for real-time user feedback [29], [30]. Powered by an Arduino Uno Microcontroller and designed to operate on a 9V battery, the system is both portable and easy to install [31], [32]. This innovation not only enhances security but also eliminates the need for physical keys, mitigates duplication risks, and enables seamless access management through IoT connectivity [33], [34].

The product introduced in this study presents a competitively distinct profile in the smart security market, particularly when compared to established brands such as Xiaomi, Yale, and Samsung. Leveraging a government-certified RFID system integrated with Indonesia's e-KTP (electronic

 10.12928/ijio.v6i2.12892

Identity Card) and a capacitive touch sensor, the product prioritizes anti-duplication security measures, a feature absent in competitors' multi-factor authentication systems that rely on conventional RFID, fingerprint recognition, PIN codes, or Bluetooth/Wi-Fi connectivity [35], [36]. Priced at IDR 878,500, it offers a substantial 40–60% cost advantage over competitors' offerings (IDR 1.5–5 million), enhancing accessibility without compromising core security functionalities [37], [38]. While its 9V battery (17-day lifespan) falls short of the extended longevity of competitors' AA/lithium batteries (6–12 months) or rechargeable solutions, the product's affordability and government-backed authentication framework position it as a viable, cost-efficient alternative for markets prioritizing regulatory compliance and budget-conscious innovation [39], [40]. This combination of unique attributes addresses a critical gap in balancing security, affordability, and user-centric design in emerging smart lock ecosystems.

Therefore, this research has objective to develop smart door lock system by using Pahl and Beitz approach. This research contributes to the growing body of knowledge on smart home technologies by demonstrating the feasibility of integrating national ID systems into IoT security solutions. It also provides actionable insights for policymakers, manufacturers, and researchers aiming to develop standardized, secure, and user-friendly access control systems. The following sections detail the design process, prototype development, and performance evaluation, and conclude with recommendations for future advancements in IoT-driven security applications.

## 2. Method

This study employs Pahl and Beitz's systematic research methodology to develop a smart door lock system. The research procedure is represented in a flowchart, which outlines the step-by-step process involved in the design, testing, and evaluation of the system, as shown in Fig. 1.

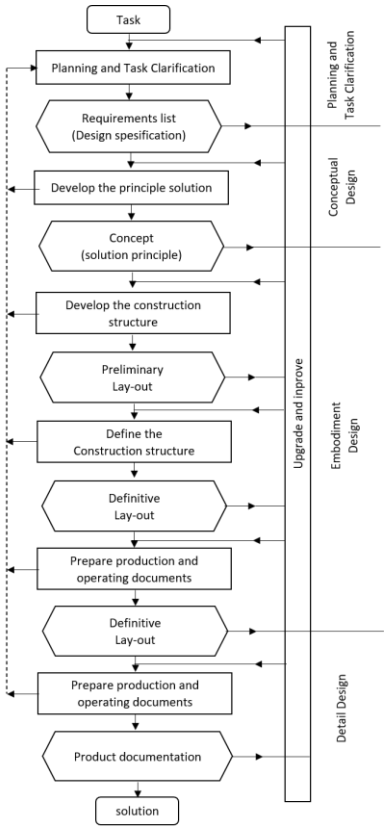


**Fig. 1**. Research procedures

The figure illustrates a systematic design framework structured to guide the development of engineering solutions through a phased and iterative approach. The process begins with Task Planning and Clarification, where project objectives are defined. Requirements List (Design Specification) is

established to outline technical, functional, and user-centric criteria. This phase ensures alignment between stakeholder expectations and design constraints. Subsequently, a Principle Solution is developed, focusing on generating abstract concepts that address core functionalities. These concepts are refined into a Sub-Function Principle, breaking down the solution into modular components to optimize performance and feasibility. The Construction Structure phase translates these sub-functions into a preliminary physical or logical layout, enabling visualization of component interactions. This evolves into a Definitive Layout, where detailed specifications such as dimensions, materials, and tolerances are finalized to ensure manufacturability and operational efficiency. Parallel to this, Production and Operating Documents are prepared, including technical drawings, assembly guidelines, and maintenance protocols, ensuring a seamless transition from design to implementation.

The framework emphasizes iterative refinement, as seen in the feedback loops between the Definitive Layout and earlier stages, allowing for continuous optimization. Finally, Product Documentation consolidates all deliverables, such as user manuals and system messages, while Event Design ensures the solution integrates effectively within its intended operational context. This structured methodology not only streamlines the design process but also enhances traceability, reproducibility, and adaptability, aligning with best practices in engineering design and systematic innovation.

## 3. Results and Discussion

### 3.1. Planning and Task Clarification

In the Planning and Task Clarification phase, the study identified critical vulnerabilities in conventional locking systems. To address these issues, a structured requirements elicitation process was conducted, combining market analysis and literature review of a smart door lock. This stage determined the Design Requirements and Priorities required by the product.

**Table 1**. Design Requirements and Prioritization

| Category | Requirement | Priority | | Target |
|---|---|---|---|---|
| | | ***Mandatory*** | ***Desirable*** | |
| Security | RFID-based authentication | v | | Can read e-KTP |
| Operational | Operating system | v | | Easy to operate |
| Manufacturing | Product model | v | | Aesthetic model |
| | | v | | Meet standard dimensions for components |
| | Cost | v | | Affordable cost |
| | Production process | v | | Simple construction |
| Scalability | Battery | | v | Rechargeable 9V battery with big capacity, suitable for various user needs |

This table outlines the design requirements for a Smart Door Lock system, categorized into Security, Operational, and Scalability criteria. Each requirement is classified as either Mandatory (essential for core functionality) or Desirable (enhancements for user convenience), with specific performance targets. Mandatory requirements include security features such as RFID-based authentication (compatible with Indonesia's e-KTP), alongside cost-effectiveness (below competitor pricing) and user-friendly operation. Scalability is addressed through a desirable rechargeable 9V battery, allowing customizable capacity for diverse user needs. This prioritization underscores the study's focus on balancing robust security, affordability, and operational simplicity in resource-constrained settings, while offering adaptable enhancements for future applications.

### 3.2. Conceptual Design

In this phase, three design concepts were generated and evaluated using the Pahl and Beitz systematic approach, which emphasizes iterative refinement and multi-criteria decision-making. The

 10.12928/ijio.v6i2.12892

concepts were assessed against four weighted criteria: component space (40%), aesthetics (30%), production cost (20%), and manufacturability (10%).

The first product design prototype represents the initial version of the device developed in this study. In this initial design, the overall shape of the product is square, while the handle features a circular design.

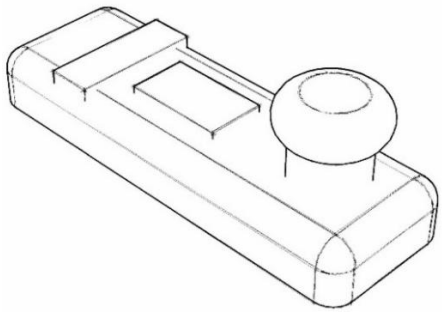

**Fig. 2**. First Product Design

**Table 2**. Advantages and Disadvantages of Alternative 1

| Advantages | Disadvantages |
|---|---|
| Lower production costs due to smaller product size | Has space for a few components |
| The small product size simplifies production | Conventional design |

The second product design prototype exhibits a significant difference, particularly in the shape of the handle. In the initial design, the handle was circular, whereas in this revised design, it has been modified to a rectangular shape.

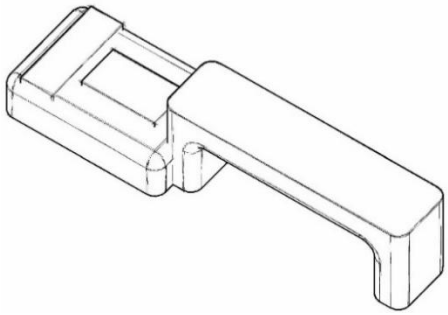

**Fig. 3**. Second Product Design

**Table 3**. Advantages and Disadvantages of Alternative 2

| Advantages | Disadvantages |
|---|---|
| Attractive design | Limited space for narrow components |
| The product is easy to manufacture | Production costs are quite expensive |

The third product design prototype includes adjustments to the upper section and the handle. The upper part has been redesigned into a smaller rectangular shape, while the handle has been elongated and remains rectangular in orientation. This design emphasizes the aesthetic appeal of the product by ensuring that the upper section aligns in height with the handle. Additionally, the edges of the product have been slightly curved to create a softer, more modern appearance, reducing rigidity in its overall design.

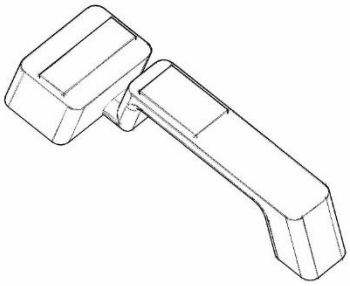

**Fig. 4**. Third Product Design

**Table 4**. Advantages and Disadvantages of Alternative 3

| Advantages | Disadvantages |
|---|---|
| Attractive design | Expensive production costs |
| Relatively easy product manufacturing | |
| Has room for large components | |

To ensure the most optimal design, each of the three product design sketches must be evaluated individually. Evaluation involves determining whether a solution achieves its intended objectives. This process includes comparing different solutions to identify the most ideal design among those developed. The evaluation for each design is as follows:

**Table 5**. Concept Evaluation with Decision Matrix

| Criteria | Weight | Design 1 | Design 2 | Design 3 |
|---|---|---|---|---|
| Component space | 40% | 60/100 | 75/100 | 90/100 |
| Aesthetics | 30% | 70/100 | 80/100 | 95/100 |
| Production cost | 20% | 85/100 | 70/100 | 80/100 |
| Ease of Production | 10% | 90/100 | 60/100 | 75/100 |
| Total Score | | 73 | 71 | 87 |

Table 5 summarizes the evaluation results. Design 3 scored highest (87/100) due to its balance of functionality, aesthetics, and cost-effectiveness.

### 3.3. Embodiment Design

This phase translates the selected Conceptual Design (Prototype 3) into a functional prototype, adhering to the requirements defined in the Planning and Task Clarification phase. The assembly process begins by connecting the 9V battery to a voltage regulator to ensure stable power distribution across the system. The RFID module (configured for e-KTP compatibility) and capacitive touch sensor are integrated into the control unit, enabling user authentication and tactile input. A relay manages power delivery to the solenoid door lock, utilizing an isolated external power supply to prevent electrical interference. User interface components, including an LCD, LED indicators, and a buzzer, are systematically linked to provide real-time operational feedback.

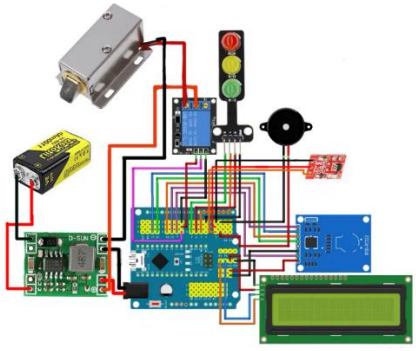

**Fig. 5**. Wiring Components


10.12928/ijio.v6i2.12892

The smart door lock security system was modeled in SolidWorks 2017. The system is primarily powered by a 9V battery, coupled with a step-down module to regulate voltage to a safe level for electronic components. User input interfaces include a capacitive touch sensor for tactile interaction and an RFID module for card/tag authentication on the outside (exterior side). The Arduino Nano serves as the central processing unit, coordinating input signals and managing output devices. These output devices include a solenoid door lock (electromagnetic locking mechanism), a relay for power switching, traffic LEDs (status indicators), a buzzer for auditory alerts, and an LCD to display operational feedback on the outside.

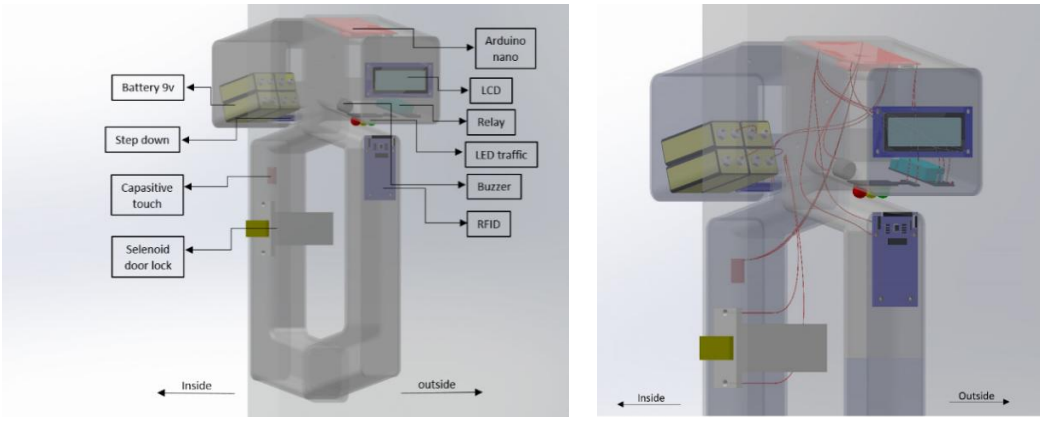


**Fig. 6**. Component Placement

SolidWorks 2017 streamlined the product design process through its parametric modeling tools, enabling precise 3D visualization and iterative adjustments to optimize component placement for ergonomic accessibility and spatial efficiency. The software's assembly features ensured seamless alignment of mechanical parts (e.g., solenoid housing) and electronic modules (RFID, relay), while its cable routing utilities allowed virtual planning of wiring paths to minimize interference, reduce clutter, and enhance system reliability. By leveraging SolidWorks' integrated design-validation tools, the prototype achieved a compact, user-friendly layout with robust manufacturability, demonstrating the software's critical role in harmonizing electromechanical integration and functional aesthetics.

### 3.4. Detail Design

In the final stage, the Detail Design Phase, all technical aspects are finalized, including dimensions, material selection, and manufacturing techniques. The Smart Door Lock prototype is constructed and subjected to a series of functionality tests to ensure compliance with security standards. The final assessment includes a comparison with existing smart locks, a cost estimation, and a power consumption analysis, demonstrating the competitive strengths of this product.

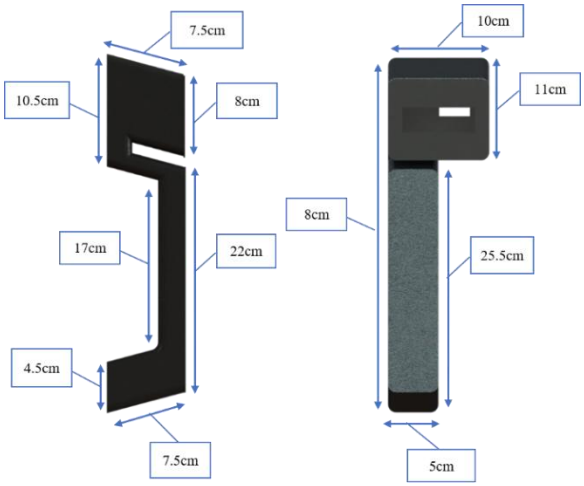


**Fig. 7**. Detailed Design Products

**Table 6**. Components and Product Prices

| No. | Component Name | Specification | Amount | Price |
|---|---|---|---|---|
| 1 | Battery | 9V 1.100mAh | 4pcs | Rp 320,000 |
| 2 | Arduino Nano | Version 3 with shield | 1pcs | Rp 79,000 |
| 3 | Jumper cable | Female to male | 1set | Rp 20,000 |
| 4 | RFID | RC522 | 1pcs | Rp 30,000 |
| 5 | RFID card | 13,56MHz | 2pcs | Rp 10,000 |
| 6 | LCD | 1602 12C | 1pcs | Rp 35,000 |
| 7 | LED Traffic Lights | 5v | 1pcs | Rp 12,500 |
| 8 | Buzzer | Mini 5v | 1pcs | Rp 5,000 |
| 9 | Relay | Single channel (Active High) 5v | 1pcs | Rp 12,000 |
| 10 | Step down | 4R7 5v | 1pcs | Rp 20,000 |
| 11 | Solenoid Door Lock | 5v | 1pcs | Rp 85,000 |
| 13 | Capasitive touch sensor | TTP223 | 1pcs | Rp 5,000 |
| 14 | Switch On/Off | 2pin | 1pcs | Rp 5,000 |
| Total | | | | Rp 638,500 |

**Table 7**. Material Cost Calculation

| No. | Cost information | Price |
|---|---|---|
| 1 | Component | Rp 638,500 |
| 2 | 3D print casing (ABS plastic) | Rp 200,000 |
| 3 | Acrylic | Rp 40,000 |
| Total | | Rp 878,500 |

Quantitative power consumption analysis based on the specified components, the power consumption of the smart door lock security system is calculated as follows:

- Component Specifications and Power Draw

**Table 8**. Component Power Consumption

| Component | Voltage | Power | |
|---|---|---|---|
| | | ***Standby*** | ***Active*** |
| Arduino Nano | 5v | 0.5 mA (0.0025W) | 25 mA (0.125W) |
| RFID | 5v | 15 mA (0.075W) | 30 mA (0.15W) |
| LCD | 5v | 1 mA (0.005W) | 20 mA (0.1W) |
| Traffic LED | 3v | - | 20 mA (0.2W) |
| Relay | 5v | 2 mA (0.01W) | 80 mA (0.4W) |
| Buzzer | 3v | - | 30 mA (0.15W) |
| Capacitive Touch Sensor | 3v | 1 mA (0.005W) | 1 mA (0.005W) |
| Solenoid Door Lock | 5v | - | 500 mA (2.5W) |

- Operational Modes

The system operates in two distinct modes standby mode and active mode, each characterized by specific power consumption profiles. In standby mode, the system maintains minimal power consumption to preserve energy. The Arduino Nano operates in sleep mode, drawing 0.5 mA at 5V (0.0025 W), while the RFID module remains idle at 15 mA (0.075 W). The LCD's backlight is disabled, consuming only 1 mA (0.005 W), and the capacitive touch sensor operates at 1 mA (0.003 W). The relay's status LED adds 2 mA (0.01 W) to indicate its standby state. Collectively, these components result in a total standby power draw of 0.0955 W, translating to a daily standby energy consumption of 2.292 Wh over 24 hours.

During active mode (triggered by user authentication or unlocking), the system briefly enters a higher power state. Each unlock cycle activates the Arduino (25 mA, 0.125 W), RFID module (30 mA, 0.15 W), relay coil (80 mA, 0.4 W), and solenoid lock (500 mA, 2.5 W) for 2 seconds.


10.12928/ijio.v6i2.12892

Additionally, the buzzer (30 mA, 0.09 W) and traffic LED (20 mA, 0.06 W) provide feedback for 2 seconds, while the LCD backlight (20 mA, 0.1 W) remains active for 15 seconds per unlock. A single unlock cycle consumes 0.00234 Wh, and with 10 daily unlocks, the total active energy demand amounts to 0.0234 Wh/day

- Battery Life Calculation

  Total Battery Capacity

  $4\ x\ 1100\ mAh\ x\ 9V\ = 39.6\ Wh$

  Estimated Lifespan

$$\frac{39.6\ Wh}{(2.292 + 0.0234) Wh/day} \approx 17.1 \text{ days}$$

### 3.5. Product Comparison

Previous research gaps analysis in Table 9 highlights the research gaps between this study and the previous research from journal at reference number 10, 11, and 35. This study addresses critical limitations in prior research through four key innovations. First, unlike the rigid Waterfall method [10], unstructured approaches [11], or ad-hoc frameworks [35], our work adopts the Pahl and Beitz methodology, enabling iterative refinement across planning, conceptualization, and detailed design phases to adapt to evolving requirements. Second, while earlier systems depended on fixed 12V adapters [10], [35] or lacked backup solutions [11], we introduce a 9V rechargeable battery with real time charging capabilities, overcoming energy limitations and power outages. Third, replacing single factor RFID [10], basic motion sensors (PIR) [11], or complex password/SMS workflows [35], our RFID + capacitive touch authentication simplifies access while enhancing security. Finally, in contrast to non-upgradable hardware [10], inflexible software architectures [11], or unimplemented biometric proposals [35], our modular design supports seamless integration of future enhancements. These advancements collectively improve IoT security systems by balancing adaptability, energy resilience, user-friendly authentication, and scalability crucial for real-world deployment in dynamic, cost-sensitive environments.

**Table 9**. Previous Research Gaps Analysis

| Criteria | Proposed Product | Previous Research 1 [10] | Previous Research 2 [11] | Previous Research 3 [35] | Gap |
|---|---|---|---|---|---|
| Methodology | Iterative (Pahl and Beitz) | Linear (Waterfall) | No structured design methodology | Ad-hoc development (no structured framework) | Flexible optimization: Iterative phases allow continuous refinement of design and functionality, addressing evolving requirements. |
| Power Management | Rechargeable 9V battery | 12V adapter | Uses external power without backup mechanisms | 12V adapter | Future-ready power resilience: Identifies limitations and proposes scalable power supply, addressing energy dependency gaps. |
| Authentication | RFID + capacitive touch | RFID-only | RFID e-KTP + PIR sensor (no multi-layered authentication) | RFID + password + SMS alerts (complex, requires user input) | Enhanced security: Dual-factor authentication reduces single-point failure risks. |
| Modularity | Cost-driven trade-offs | Fixed hardware design | Centralized on Firebase and | Suggests future biometric | Scalability potential: |

| Criteria | Proposed Product | Previous Research 1 [10] | Previous Research 2 [11] | Previous Research 3 [35] | Gap |
|---|---|---|---|---|---|
| | | | Android app (non-modular) | integration but lacks modular design | Provisions for future upgrades. |

The proposed product comparison outlined in Table 10 highlights key distinctions between the featured product and its competitors (e.g., Xiaomi, Yale, Samsung) across authentication methods, pricing, and power specifications. In terms of authentication, the product utilizes a government-issued e-KTP (electronic Indonesian Identity Card)-integrated RFID system combined with a capacitive touch sensor and a solenoid lock. This approach contrasts with competitors, which typically offer multi-factor authentication, including RFID, fingerprint recognition, PIN codes, and Bluetooth/Wi-Fi connectivity via mobile apps. A significant competitive edge lies in the e-KTP integration, which leverages government-backed anti-duplication technology to enhance security and authenticity.

Regarding pricing, the proposed product is positioned at IDR 878,500, substantially lower than competitors' offerings, which range from IDR 1.5 to 5 million. This translates to a 40–60% cost advantage over global brands, making it a more accessible option in the market.

Power and battery performance differ notably between the proposed products. The featured product relies on a 9V battery with a 17-day lifespan, whereas competitors employ long-lasting AA/lithium batteries (6–12 months) or rechargeable solutions. While the proposed product's battery lifespan is shorter, its affordability and unique authentication features may offset this limitation for specific user segments.

Overall, the product distinguishes itself through cost efficiency, government-certified security integration, and streamlined authentication mechanisms, positioning it as a competitive alternative to higher-priced counterparts.

**Table 10**. Proposed Products Comparison

| Criteria | Proposed Product | Competitors (e.g., Xiaomi/Yale/Samsung) | Competitive Edge |
|---|---|---|---|
| Authentication Methods | - RFID (government-issued e-KTP) + capacitive touch sensor<br>- Solenoid lock | - RFID + fingerprint + PIN code;<br>- Bluetooth/Wi-Fi + mobile app | e-KTP integration (government-backed ID, anti-duplication) |
| Price | IDR 878,500 | IDR 1.5–5 million (varies by brand) | 40–60% cheaper than global competitors |
| Power & Battery | 9V battery (17-day lifespan) | AA/Lithium batteries (6–12 months) | Rechargeable |

## 4. Conclusion

This study successfully designed and developed a smart door lock system that integrates Indonesia's e-KTP RFID authentication, capacitive touch sensors, and IoT connectivity to address security vulnerabilities in conventional and existing smart locks. By applying Pahl and Beitz methodology, the design process systematically balanced technical feasibility, user-centric innovation, and cost optimization, resulting in a prototype that outperformed initial concepts in functionality (87/100 score) and affordability (IDR 878,500). The e-KTP integration provided a government-backed, tamper-resistant authentication layer, while the capacitive touch sensor enhanced usability. Comparative analysis highlighted the system's competitive edge: a 40–60% lower cost than commercial locks, its unique focus on universal accessibility, scalable power supply and modularity potential. The findings emphasize the broader potential of integrating national ID systems into IoT security architectures, particularly in resource-constrained settings. Future research should focus on environmental stress-testing, optimizing RFID detection algorithms under interference, and extending battery life through low-power circuitry. Additionally, exploring


10.12928/ijio.v6i2.12892

blockchain integration for decentralized authentication could further bolster security. These advancements will contribute to standardized, scalable smart home ecosystems, aligning with global trends in IoT-driven security innovation.

## References


[1] Y. Motwani, S. Seth, D. Dixit, A. Bagubali, and R. Rajesh, "Multifactor door locking systems: A review," *Mater. Today Proc.*, vol. 46, pp. 7973–7979, Jan. 2021, doi: 10.1016/j.matpr.2021.02.708.

[2] A. A. Zainuddin *et al.*, "Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology," *Malaysian J. Sci. Adv. Technol.*, vol. 4, no. 4, pp. 360–365, Aug. 2024, doi: 10.56532/mjsat.v4i4.335.

[3] R. Ismail, H. C. Yee, K. Terh Jing, and M. W. M. Shafiei, "Preferences of Security Criteria in Low-Cost Housings among Malaysian Residents," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 13, no. 3, pp. 1170–1176, May 2023, doi: 10.18517/ijaseit.13.3.16956.

[4] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, pp. 1–22, Jan. 2022, doi: 10.1155/2022/9307961.

[5] S. Kaya, E. Aşkar Ayyildiz, And M. Ayyildiz, "Smart Door Lock Design With Internet Of Things," *Int. J. 3D Print. Technol. Digit. Ind.*, vol. 6, no. 2, pp. 201–206, Aug. 2022, doi: 10.46519/ij3dptdi.1074468.

[6] H. Gadupu, O. Mokharji, R. Kankaria, S. Kumar, and K. Jayavel, "ACCESS - IoT enabled smart lock," *Int. J. Reconfigurable Embed. Syst.*, vol. 10, no. 3, p. 176, Nov. 2021, doi: 10.11591/ijres.v10.i3.pp176-185.

[7] M. I. Ahmed and G. Kannan, "Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications," *J. Inf. Knowl. Manag.*, vol. 20, no. Supp01, p. 2140004, Feb. 2021, doi: 10.1142/S0219649221400049.

[8] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[9] M. I. Tawakal and Y. Ramdhani, "Smart Lock Door Using E-KTP Access Based on the Internet of Things," *J. Responsif Ris. Sains dan Inform.*, vol. 3, no. 1, pp. 83–91, Mar. 2021, doi: 10.51977/jti.v3i1.417.

[10] D. Salim, D. N. Salim, N. A. Pujisusilo, and S. P. Manik, "Smart Door Lock Security System Using E-KTP (Electronic Resident Identity Card) Based on Internet of Things (IoT)," *Go Infotech J. Ilm. STMIK AUB*, vol. 27, no. 2, p. HAL. 196-206, Dec. 2021, doi: 10.36309/goi.v27i2.157.

[11] A. A. Najib, R. Munadi, and N. B. Aditya Karna, "Security system with RFID control using E-KTP and internet of things," *Bull. Electr. Eng. Informatics*, vol. 10, no. 3, pp. 1436–1445, Jun. 2021, doi: 10.11591/eei.v10i3.2834.

[12] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," in *2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, Oct. 2022, pp. 453–457, doi: 10.1109/GECOST55694.2022.10010367.

[13] S. Ganesan, B. Esakki, S. Mathiyazhagan, and V. Pandimuthu, "Design Conception And Evaluation Of An Unmanned Amphibious Aerial Vehicle Using Systematic Approach," *Aviation*, vol. 26, no. 1, pp. 41–53, Mar. 2022, doi: 10.3846/aviation.2022.16519.

[14] O. O. Trilian and R. B. Jakaria, "Designing a Lecture Chair Product Using the Pahl and Beitz Method," *Innov. Technol. Methodical Res. J.*, vol. 3, no. 2, pp. 9–9, Feb. 2024, doi: 10.47134/innovative.v3i2.101.

[15] N. AY and M. Bozdemir, "Conceptual Design Process of a Missile Model and Production Using Additive Manufacturing Method," *Def. Sci. J.*, vol. 74, no. 5, pp. 734–742, Sep. 2024, doi: 10.14429/dsj.74.19512.

[16] B. Darmanin, A. Bonello, and E. Francalanza, "A Systematic Design Approach for Cognitively Ergonomic Collaborative Robotic Workspaces," *Procedia CIRP*, vol. 130, pp. 853–860, Jan. 2024, doi: 10.1016/j.procir.2024.10.175.

[17] F. Koppenhagen, T. Blümel, T. Held, C. H. Wecht, and P. D. Kollmer, "Hybrid development of physical products based on systems engineering and design thinking: towards a new process model," *J. Des. Res.*, vol. 21, no. 3/4, pp. 210–261, 2024, doi: 10.1504/JDR.2024.143686.

[18] H. I. Unria, M. I. Hamdy, M. Yola, T. Nurainun, and A. Anwardi, "Design of a Corn Thresher and Corn Cob Chopper Using the Pahl & Beitz Method," *Semesta Tek.*, vol. 27, no. 2, pp. 203–212, Nov. 2024, doi: 10.18196/st.v27i2.23322.

[19] M. Shehata, "Designing Smart Products in The Light of Design Thinking and The Systematic Design Approach," *J. Des. Sci. Appl. Arts*, vol. 5, no. 1, pp. 310–320, Jan. 2024, doi: 10.21608/jdsaa.2023.221509.1312.

[20] J. Rekayasa Material, M. dan Energi, R. Novianty Pasaribu, N. Andri Silviana, N. Siregar, and P. Utama, "Brick Mold Design Using the Pahl and Beitz Method," *J. Rekayasa Mater. Manufaktur dan Energi*, vol. 8, no. 1, pp. 01–05, Feb. 2025. [Online]. Available at: https://jurnal.umsu.ac.id/index.php/RMME/article/view/17866.

[21] B. Triyono, R. Putranto, and D. E. Septiyani Arifin, "Conceptualization of Soft Capsule Shell Material Preparation Tool Using the Pahl and Beitz Method," *Manutech J. Teknol. Manufaktur*, vol. 16, no. 01, pp. 1–8, Aug. 2024, doi: 10.33504/manutech.v16i01.294.

[22] A. K. Agbonkhese, "Application Of Solidworks Simulation To Improve Mechanical Design Skills Of Mechanical Engineering Students In The National Institute Of Construction Technology And Management, Edo State, Nigeria," *Int. J. Funct. Res. Sci. Eng.*, vol. 3, no. 1, pp. 72–79, Apr. 2024. [Online]. Available at: https://www.journalfrse.com/journal/article/view/18.

[23] R. Abdallah *et al.*, "The use of SolidWorks in the evaluation of wind turbines in Palestine," *Energy Nexus*, vol. 7, p. 100135, Sep. 2022, doi: 10.1016/j.nexus.2022.100135.

[24] K. Vardaan and P. Kumar, "Design, analysis, and optimization of thresher machine flywheel using Solidworks simulation," *Mater. Today Proc.*, vol. 56, pp. 3651–3655, Jan. 2022, doi: 10.1016/j.matpr.2021.12.348.

[25] T. S. KERK and mohd azwir Azlan, "Design of A Vertical Conveyor System for Scrap Rubber in FGV Felda Rubber Industry," *Res. Prog. Mech. Manuf. Eng.*, vol. 2, no. 2, pp. 569–579, 2021. [Online]. Available at: https://publisher.uthm.edu.my/periodicals/index.php/rpmme/article/view/4114.

[26] S. Mishra and A. V. Ullas, "Concept Modelling of Small Scale Device for Continuous Production of Graphene using Solidworks," *Mater. Today Proc.*, vol. 79, pp. 345–348, Jan. 2023, doi: 10.1016/j.matpr.2022.12.034.

[27] Y. Lu *et al.*, "Application of SolidWorks software in preoperative planning of high tibial osteotomy," *Front. Surg.*, vol. 9, p. 951820, Jan. 2023, doi: 10.3389/fsurg.2022.951820.

[28] О. С. Мачуга and Т. В. Оляниш ен, "Using Solidworks Simulation tool for automated design of drying chambers and study of their operation parameters," *Sci. Bull. UNFU*, vol. 34, no. 2, pp. 109–115, Mar. 2024, doi: 10.36930/40340214.

[29] M. Q. Mehmood, M. S. Malik, M. H. Zulfiqar, M. A. Khan, M. Zubair, and Y. Massoud, "Invisible touch sensors-based smart and disposable door locking system for security applications," *Heliyon*, vol. 9, no. 2, p. e13586, Feb. 2023, doi: 10.1016/j.heliyon.2023.e13586.

[30] Yulisman, N. Iman, E. Sabna, and H. Fonda, "Automatic Door System Using Internet of Things (IoT) Based E-KTP in Hotel Rooms," *SATESI J. Sains Teknol. dan Sist. Inf.*, vol. 1, no. 2, pp. 85–91, Oct. 2021, doi: 10.54259/satesi.v1i2.60.

[31] Azhari, R. R. Manullang, M. Yanti, C. D. Hasibuan, and E. Yudhistira, "Performance of Secure Door Access System Using Identification Numbers, Fingerprints, and Facial Recognition," *J. Phys. Conf. Ser.*, vol. 2733, no. 1, p. 012003, Mar. 2024, doi: 10.1088/1742-6596/2733/1/012003.

[32] D. Ramadini and H. Hastuti, "Electronic Lock System for Boarding House Doors Using IoT Based on E-KTP," *MASALIQ*, vol. 5, no. 1, pp. 160–174, Dec. 2024, doi: 10.58578/masaliq.v5i1.4475.

[33] N. Hanafiah, C. P. Kariman, N. Fandino, E. Halim, F. Jingga, and W. Atmadja, "Digital Door-Lock using Authentication Code Based on ANN Encryption," *Procedia Comput. Sci.*, vol. 179, pp. 894–901, Jan. 2021, doi: 10.1016/j.procs.2021.01.079.

[34] S. Mansfield-Devine, "Locking the door: tackling credential abuse," *Netw. Secur.*, vol. 2021, no. 3, pp. 11–19, Mar. 2021, doi: 10.1016/S1353-4858(21)00030-1.

[35] S. A. Prity, J. Afrose, and M. M. Hasan, "RFID Based Smart Door Lock Security System," *Am. J. Sci. Eng. Res.*, vol. 4, no. 3, pp. 162–168, 2021, [Online]. Available at: https://iarjournals.com/upload/43162168.pdf.

[36] M. Kumar A., I. Ahamath M., and Gowtham R., "Revolutionizing Home Security: A Comprehensive Overview of an Advanced RFID Door Lock System for Keyless Access and Smart Home Protection," *Asian J. Appl. Sci. Technol.*, vol. 08, no. 01, pp. 01–13, 2024, doi: 10.38177/ajast.2024.8101.

[37] J. Guntur, S. S. Raju, T. Niranjan, S. K. Kilaru, R. Dronavalli, and N. S. S. Kumar, "IoT-Enhanced Smart Door Locking System with Security," *SN Comput. Sci.*, vol. 4, no. 2, p. 209, Feb. 2023, doi: 10.1007/s42979-022-01641-9.

[38] H. Ahmad Taslim, N. A. Md Lazam, and N. A. Mohd Yahya, "Development of Smart Home Door Lock System," in *Advances in Intelligent Systems and Computing*, vol. 1350 AISC, Springer, Cham, 2021, pp. 118–126, doi: 10.1007/978-3-030-70917-4_13.

[39] G. B. A. Svaboe, K. Y. Bjerkan, and S. Meland, "Safe delivery of goods and services with smart door locks: Unlocking potential use," *Transp. Res. Interdiscip. Perspect.*, vol. 29, p. 101309, Jan. 2025, doi: 10.1016/j.trip.2024.101309.

[40] V. P.Datar, A. Tankasali, and K. Chavan, "Smart Door Lock and Lighting System using Internet of Things," *IARJSET*, vol. 8, no. 8, pp. 102–108, Aug. 2021, doi: 10.17148/IARJSET.2021.8820.