

Product Development

Design and Build “Smart Key Tracking Systems with RFID and Arduino Mega” for Use in Petrochemical Engineering Department PTSN

Ahmad Tulka*, Rozieana Abu, Aminah Ishak, Muhammad Qayyim Jefperi, Rineshnaiidu Ratnasamy, Muhammad Affan Mohammad Noor

Department of Petrochemical Engineering, Politeknik Tun Syed Nasir Syed Ismail, Malaysia, ahmad_tulka@ptsn.edu.my; rozieana@ptsn.edu.my; aminah@ptsn.edu.my; musyimm666@gmail.com; neshrinesh03@gmail.com; muhdaffan276@gmail.com

*Corresponding author: Ahmad Tulka, Department of Petrochemical Engineering, Politeknik Tun Syed Nasir Syed Ismail, Malaysia; ahmad_tulka@ptsn.edu.my

Abstract: The problem concerning key storage at Politeknik Tun Syed Nasir Syed Ismail (PTSN) systems is a lack of systematic administration, leading to uncontrolled and insecure essential management procedures. Consequently, the objective is to create an intelligent key tracking system (SKTS) utilizing radio frequency identification (RFID) and Arduino Mega to establish a secure and properly organized key storage system with efficient data management. This project introduces the monitoring system with automated and real-time data collection. SKTS design uses an Arduino Mega 2560 microcontroller and an ESP8266 Node MCU Wi-Fi module that sends data over the cloud. The project also utilizes the Telegram chat application bot to notify and monitor the keys' retrieval and return. It is also equipped with an RFID reader as a sensor. As the authorized user, once the RFID card is swept, type the selection key number; the solenoid lock for the selected key will open, and the key is free to be picked. The liquid crystal display (LCD) will show the authorized user data and selected room number. A signal will send the information to the Telegram application through a mobile phone to notify the other authorized user. This project successfully achieves its objective by utilizing the Telegram application to notify critical users and authorized individuals when keys are returned. These real-time notifications are visible to all registered group members on the Telegram application. The Likert Scale, which has two points, is established by utilizing data responses from the rubrics form, with evaluators consisting of industrial designers and researchers. The results are subsequently synthesized using qualitative percentages. The responses to the item provided via the rubric assessment form show that the SKTS meets the design, ideal, and functional aspects.

Keywords: Smart key tracking system; RFID; Arduino Mega

Received: 18th March 2024

Received in revised form: 23rd May 2024

Available Online: 1st June 2024

Published: 28th June 2024

Citation: Tulka, A., Abu, R., Ishak, A., *et al.* Design and Build “Smart Key Tracking Systems with RFID and Arduino Mega” for Use in Petrochemical Engineering Department PTSN. *J Workforce Edu Res* 2024; 1(1): a0000514. <https://doi.org/10.36877/jwer.a0000514>

1. Introduction

Radiofrequency identification (RFID) technology can enhance key management in various ways. Firstly, it facilitates precise critical information recording using RFID chips embedded within the keys (Zhang *et al.*, 2021; Baashirah *et al.*, 2018). It enables efficient tracking and identification of keys, simplifying their retrieval and utilization (Lin *et al.*, 2014). Furthermore, RFID-based critical management systems can incorporate features such as fingerprint recognition to prevent unauthorized access (Sadikin & Kyas, 2015).

Meanwhile, the internet of things (IoT) is an innovation combining various innovative systems, frameworks, intelligent devices, and sensors. Moreover, it takes advantage of quantum and nanotechnology in terms of storage, sensing and processing speed, which were not conceivable beforehand (Aloi *et al.*, 2016).

IoT technology is widely used to remove or monitor devices over the internet using a smartphone, laptop, or tablet (Wheelus & Zhu, 2020). The applications of the IoT consist of several parts, such as connectivity and active engagement, such as cloud (Sharma *et al.*, 2021). As smartphones become more ubiquitous in people's pockets and homes, they increasingly serve as ideal candidates for collecting, processing, and forwarding data from wireless IoT devices or sensor networks. In many cases, smartphones are equipped with multiple radio interfaces to facilitate communication with various devices, making them versatile hubs for managing IoT data (Gaggioli *et al.*, 2013).

The issue with crucial storage at Politeknik Tun Syed Nasir (PTSNS) arises from the absence of organized management, resulting in unregulated and insecure critical management practices. Users occasionally employ fictitious names, which can lead to misunderstandings. Additionally, there is a potential risk of the critical user record book being misplaced or stolen, and users frequently neglect to return keys, causing room utilization and class delays. To address this problem, a secure and well-structured key storage system with effective data management is necessary for a resolution.

It can be achieved by designing and building the "smart key tracking systems with RFID and Arduino Mega". In this system, 20 RFID cards serve as "authentication," which means accessing the storage system. The RFID scanner and Arduino Mega cooperate to validate these cards by verifying their registration status. Users can select their desired key using a keypad, while a display screen provides information about the user card and the corresponding key code. Data is stored on an SD card and accessed through the TELEGRAM app when the keys are returned.

In summary, RFID technology offers enhanced efficiency, security, and privacy in key management processes. The IoT encompasses a broad range of technologies, envisioning the connectivity of various objects in our surroundings. These objects can interact and collaborate through unique addressing schemes and standardized communication protocols, working together to achieve shared objectives (Atzori *et al.*, 2010).

2. Literature Review

Based on the summary in Table 1, it has been identified that novel methodologies or approaches were used in research papers. Sadikin & Kyas (2015) introduced a novel key management system tailored to the limited resources of innovative RFID systems. This research proposed a lightweight mutual authentication and identity protection mechanism to mitigate existing threats in innovative RFID systems.

Another innovative approach is using the Combined Symmetric Key and SMS4 algorithm for security authentication in low-cost RFID systems, simplifying crucial management and reducing the requirement of tags (Jiang *et al.*, 2013).

A unique methodology introduced in one of the papers is using a mutual-authentication protocol with synchronously updated keys based on a hash function, which reduces the computational burden and improves the search efficiency of the system. Moreover, integrating RFID tags with sensor nodes in intelligent RFID systems allows for lightweight mutual authentication and identity protection, addressing security and privacy concerns (Vegendla *et al.*, 2014).

In the context of the DASH7 standard, RFID technology supports public key cryptography, enabling the implementation of efficient critical management systems with features like public key infrastructure authentication and non-repudiation (Baashirah *et al.*, 2018; Hakeem *et al.*, 2013).

Table 1. Technology for crucial management based on RFID applications

References	Insights	Results
(Zhang <i>et al.</i> , 2021)	The research aims to address the key tag writing problem by devising a protocol that sends data to all members of each key group accurately within the minimum time.	The K-Write protocol tackles the key tag writing issue by minimizing the activity of normal tags and compressing the reader-to-tag indicator vector. It offers two key benefits: deactivating normal tags in certain situations to decrease interference and transmitting only the necessary slots to inform key tags when to receive their group data, instead of all slots as done in existing studies. This method greatly reduces transmission costs
(Ismail <i>et al.</i> , 2021)	RFID is a passive type, which is lighter and less expensive than active tags	Improvements in reporting and monitoring crucial records using the medium of IoT and ultrasonic detectors and keypads were suggested to improve the product.
(Baashirah <i>et al.</i> , 2018)	RFID can be used to improve key management by implementing the Hacker Proof Authentication Protocol	- Improved cryptographic scheme for RFID authentication

References	Insights	Results
	(HPAP) for secure and efficient authentication of multiple tags.	- Secure and fast authentication with multiple tags Not Applicable (N/A)
(Sadikin & Kyas, 2015)	RFID can create an intelligent key management system by integrating sensor nodes with active RFID systems and implementing lightweight mutual authentication and identity protection.	
(Lin <i>et al.</i> , 2014)	RFID can record critical information accurately, indicate key positions, prevent unauthorized use, and quickly read critical information for efficient management.	N/A
(Vegendla <i>et al.</i> , 2014)	RFID can improve key management by implementing a system that utilizes public key infrastructure authentication and non-repudiation features.	- Proposed vital management system for DASH7 - Analyzed performance criteria such as latency and throughput
(Hakeem <i>et al.</i> , 2013)	Advantages: RFID allows for efficient identification. Disadvantages: RFID poses security and privacy threats.	- The proposed protocol is secure against various attacks. - The protocol has lower storage, computation load, and cost compared to existing RFID authentication protocol
(Jiang <i>et al.</i> , 2013)	The advantages of using RFID for key management include simplified management of large-scale keys and reduced tag requirements. No disadvantages are mentioned in the text.	- Proposed a new security authentication protocol for the RFID system - Resolved security problems and reduced tag requirement
(Zhang <i>et al.</i> , 2012)	The advantages of using RFID for key management include improved social efficiency, while the most significant disadvantage is the security flaws in RFID systems.	- The algorithm is safe and effective - Potential value for social promotion
(Kang & Lee, 2008)	The advantages of using RFID for key management include its speed of recognition and non-touch methods. However, there are risks of information exposure and privacy encroachment.	The proposed method provides security through XOR and OR algorithms. - Proposed method overcomes security threats

Additionally, past researchers highlighted issues or challenges related to the project of a key management system using RFID. The primary obstacles preventing the complete mechanization of the intelligent key tracking system using RFID stems from its inherent limitations and constrained resources (Sadikin & Kyas, 2015).

Integrating RFID tags with sensor nodes in the intelligent RFID system gives rise to security and privacy concerns, including issues related to key management (Sarkar *et al.*, 2017). Updating the security properties of all RFID tags is impractical, and employing heavyweight solutions like transport layer security or secure sockets layer (TLS/SSL) is unfeasible due to the system's resource constraints (Pavithra & Sreenivasa Ravi, 2017). Moreover, current solutions are vulnerable to threats like privacy breaches and Man-in-the-Middle attacks. These challenges impede the comprehensive mechanization of the Smart Key Tracking System using RFID.

3. Methodology

A systematic design methodology utilizing the analysis, design, development, implementation and evaluation (ADDIE) approach was introduced to incorporate circular and intelligent design elements. The methodology encompassed a literature review to identify specific circular and smart design aspects, gathering user preferences for existing products, translating these preferences into design elements, converting them into functional requirements, and generating comprehensive design alternatives. The effectiveness of this methodology was evaluated through a case study on an intelligent key tracking system (SKTS), demonstrating that the developed design surpassed existing local models based on previous research. The advantages include reduced complexity for easy maintenance and troubleshooting, lower cost, and lightweight design. This proposed product innovation process has the potential to enhance customer satisfaction and provide companies with a competitive advantage.

3.1 Case Study

The project has been designed primarily focusing on internal management applications at Politeknik Tun Syed Nasir. The analyses aim to provide insights into essential characteristics of crucial management, addressing challenges posed by diverse systems. The conceptual efforts outlined in the project are geared towards minimizing uncertainties associated with these systems. Ultimately, the primary objective is to enhance decision-making processes at the Politeknik of Malaysia alliance level. It involves establishing a robust framework for developing and securing critical management systems and streamlining activities related to crucial notification, monitoring, retrieval, and return processes.

3.1.1 Product Needs Analysis

The first section was product need analyses. This step has been conducted to obtain an overview from Politeknik Tun Syed Nasir users. A total of 20 individuals among lecturers have offered feedback on the study or research, representing diverse age groups ranging from the late 20s to the elderly.

Approximately 40% of the feedback highlighted challenges in tracking a key when the required key is not inside the storage box (Figure 1a-e). Additionally, an equal percentage, approximately 40%, of the feedback received indicated that registered key borrowers are challenging to identify.

Thus, the lecturers favour the new innovative key tracking system to simplify the critical management process for their daily tasks.

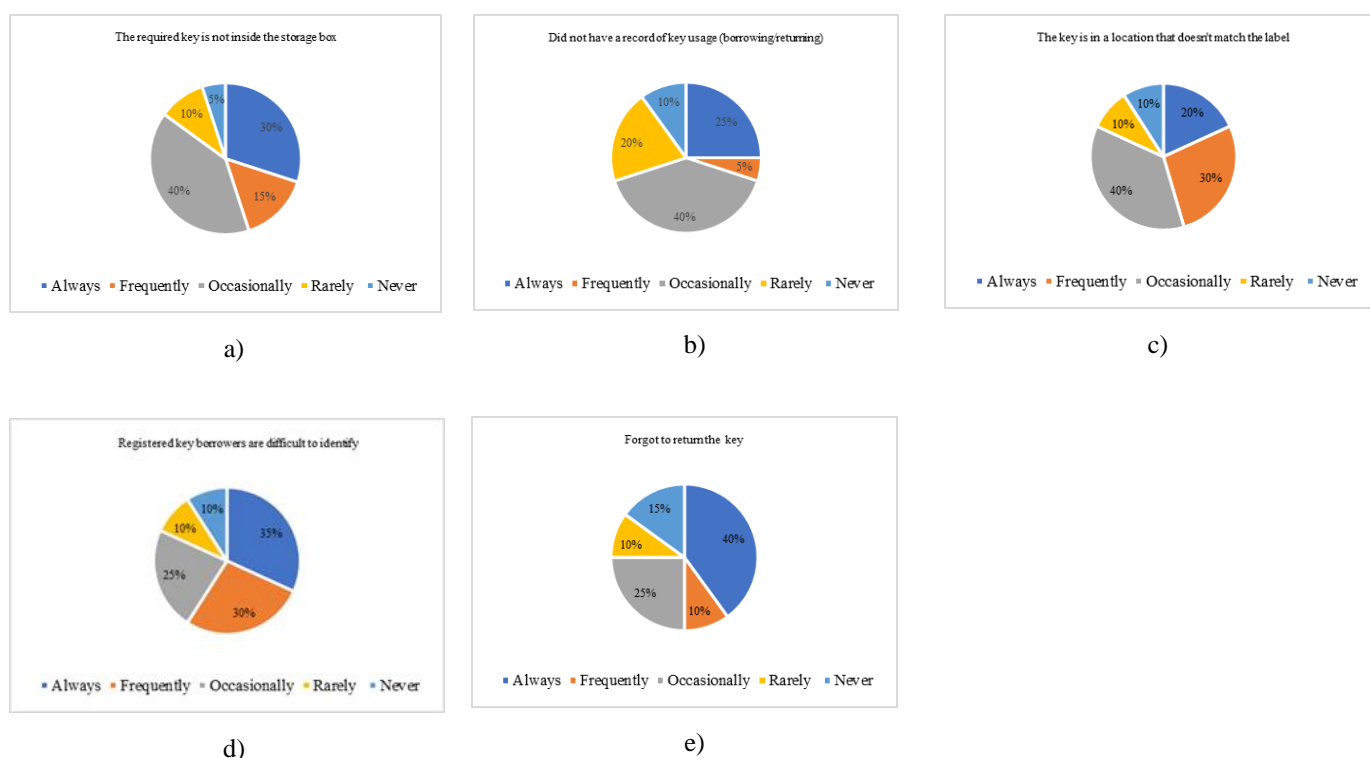
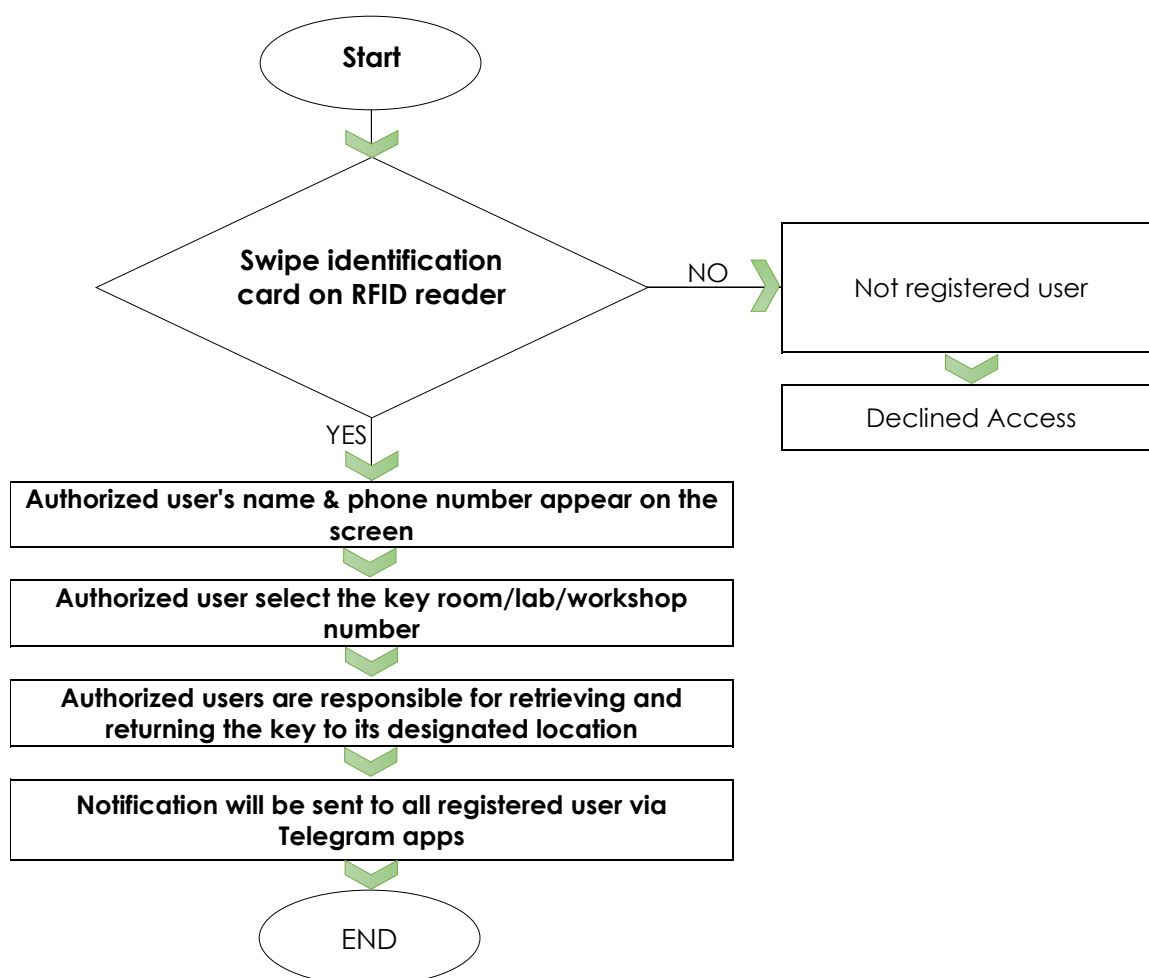


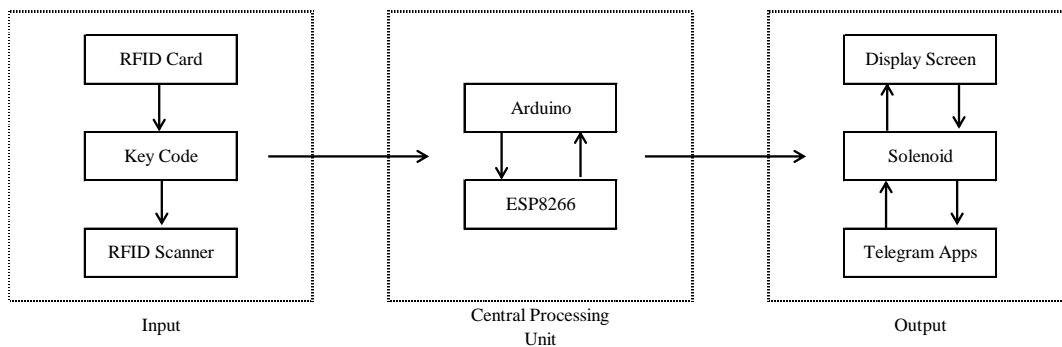
Figure 1 (a–e). Analysis of the need to create an intelligent key-tracking system among the lecturers.

3.2 The Development of The Project

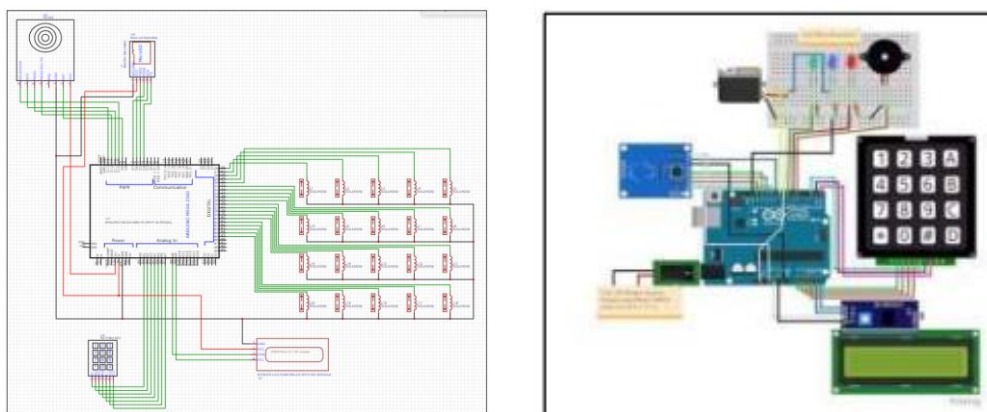
The SKTS is designed, developed, implemented, and evaluated in the second section. This was conducted through an innovation project design process, measurement, and determination of the materials used. Next comes product development, installing accessories, and final innovation product testing. The visual diagram of the SKTS block illustrates how the system operates and the process when keys are taken or returned, including data storage methods as depicted in Figures 2, 3 and 4.



(a) Flow process of the operating system of SKTS



(b) Block Diagram



(c) Wiring Diagram


```
void access()
{
  // Ask for password
  lcd.clear();
  lcd.print("Please enter code...");
  //Serial.println("Please enter password:");
  String password = "";
  while (password.length() < 3) {
    char key = keypad.getKey();
    if (key) {
      password += key;
      //Serial.print(key);
      //lcd.print("...");
      lcd.print(key);
    }
  }
  delay(1000);
  lcd.clear();

  // Check password
  if (password == "101")
  {
    Serial.println("key: 101");
    Serial.println("Bilik Kuliah 1");
    Serial.println("Access granted.");
    Serial.println("=====");
  }
}
```

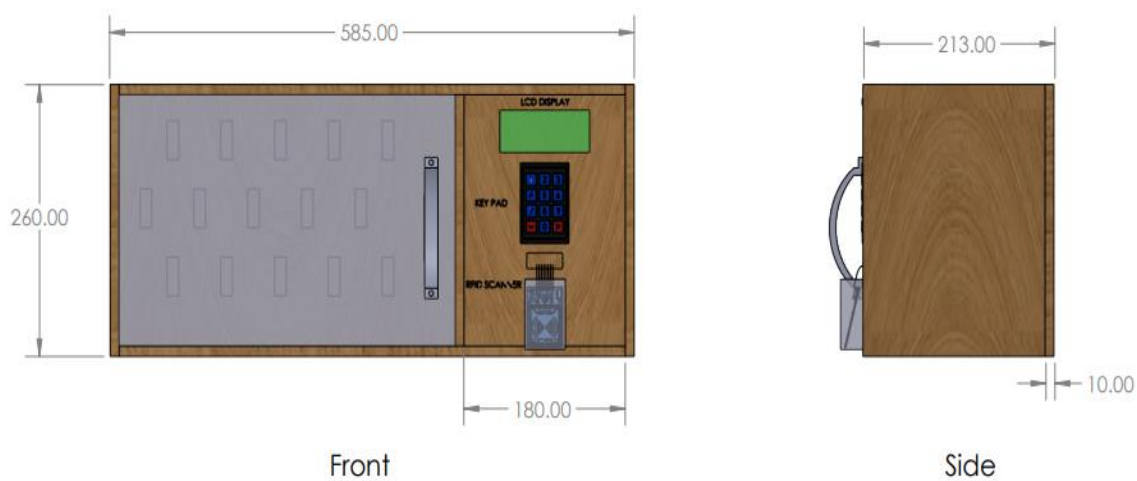
*The central component, which pertains to the coding language, has been intentionally obfuscated to maintain confidentiality, as recommended by the reviewer.

(d) Coding using Arduino Mega

Figure 2 (a–d). The design of flow for the operation system and development of the SKTS



(a) Isometric Drawing



(b) Orthographic Drawing

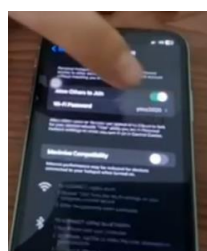


(c) Finish Product Photo

Figure 3 (a–c). The drawings and final feature of the SKTS project



(a) On the power supply.



(b) Activate the Internet Line.



(c) Scanned the authorised card. Detail will appear on LCD.



(d) Type in the key not required.



(e) As the solenoid is active, take out the key.



(f) Information sent to TELEGRAM Apps.



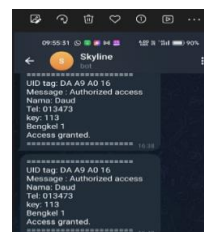
(g) To return the key, tap the authorised card again.



(h) Type in the key number.



(i) Put back the key as the solenoid is active.



(j) Information sent to TELEGRAM Apps.

Figure 4 (a–j). SKTS implementing and evaluation process

The Likert scale, employing two points, is created by collecting data responses from the rubrics form involving evaluators who are both industrial designers and researchers. Data was collected through face-to-face interactions on the project's final assessment day. Following this data collection, the results are then consolidated and expressed in the form of qualitative percentages.

4. Results and Discussions

As per the study, this project successfully achieves its objective by utilizing the Telegram application to send real-time notifications to all the registered authorized users, either when the key is taken out or returned. SKTS makes critical tracking more reliable, easy, and faster for users.

Data was collected through face-to-face interactions on the project's final assessment day, utilizing the rubrics as the evaluation instrument. After this data collection, the results were consolidated and presented as qualitative percentages. Also, based on the analysis in Table 2 (a–c), the data obtained is presented as a percentage. The data given by three experts' confirmation responses to the item provided via the rubric assessment form shows that the SKTS has successfully achieved all its objectives, such as fulfilling all the required safety features but still having ample room for improvement.

Table 2 (a). Analysed part based on design aspects

No.	Item	Yes	No	Percentages
1	Arrangements of key holder is in order.	3	0	100%
2	The design is stable.	3	0	100%
3	This design has a good framework.	3	0	100%
4	This design does not endanger the user	3	0	100%
5	This design has safety features.	3	0	100%

Table 2 (b). Analysed part based on ideal aspects

No.	Item	Yes	No	Percentages
1	Products are developed to save users time.	3	0	100%
2	The product developed convenience for the user.	3	0	100%
3	This product is relevant for development.	3	0	100%

No.	Item	Yes	No	Percentages
4	The product developed features a technological system.	3	0	100%
5	The product was brilliant.	3	0	100%

Table 2 (c). Analysed part based on functional aspects

No.	Item	Yes	No	Percentages
1	Arduino Mega was used ideally.	3	0	100%
2	The LCD the correct data.	3	0	100%
3	The solenoids work well.	3	0	100%
4	The correct data was sent to the Telegram App.	3	0	100%
5	The product works well.	3	0	100%

The evaluators have provided comments on product improvement. The summary of the reviews provided by the evaluators was as follows: (i) As for the convenience to the staff, use the employee card as an authorized RFID card reader; (ii) Limit the number of solenoids in every RFID control box as it will avoid affecting many keys as problems occur; and (iii) The casing of the product should be made from a light and more robust material for its durability and ease of handling.

This product or design outperforms existing alternatives in several aspects. A systematic design methodology utilizing the ADDIE approach was introduced to incorporate circular and intelligent design elements. The methodology encompassed a literature review to identify specific circular and smart design aspects, gathering user preferences for existing products, translating these preferences into design elements, converting them into functional requirements, and generating comprehensive design alternatives.

The effectiveness of this methodology was evaluated through a case study on an intelligent key tracking system, demonstrating that the developed design surpassed existing local research models. A comparison chart from the previous projects or literature regarding usage, specification and costing is shown in Table 3. The SKTS advantages include reduced complexity for easy maintenance and troubleshooting, lower cost, and lightweight design. This proposed product innovation process has the potential to enhance customer satisfaction and provide companies with a competitive advantage.

Table 3. Comparison chart from previous projects or literature in terms of usage, specifications, and costing


Reference	Usage	Specifications	Costing	Limitations
SKTS <i>This study</i>	Notification and monitoring of the retrieval and return of keys, number of keys 15	Arduino Mega 2560, ESP8266, LCD screen I2C, RFID cards (13.56 MHz), Relay, Electromagnetic solenoids (300mA)	Fully described	The project's electromagnet solenoid is vulnerable to tampering, enabling unauthorized key retrieval. To address this issue, it is recommended to use high-quality solenoid and sturdy materials, such as metal, for the critical box's body and cover frame to enhance security.
Zainal (2022)	Notification, reservation and monitoring of the keys, number of keys 3	Arduino IDE, NodeMCU ESP32, IR sensor, LCD, Keypad, Solenoid lock, Ionic framework using Cloud Store for database	Not Applicable	Administrator approval is required, and the instructions for making a reservation or borrowing a key are complex.
Hamzah <i>et al.</i> , (2021)	Notification and monitoring of the retrieval and return of keys, number of keys 9	Arduino Mega 2560 Pro, ESP8266 NodeMCU Wi-Fi module, RFID reader, Buzzer, LED, Relay, solenoid, Telegram apps	Not Applicable	The project fails to clearly outline the types of data analysis, such as design and ideal and functional aspects.
Haris <i>et al.</i> , (2019)	Keys tracing, number of keys 40	Arduino WEMOS Mega + Wifi R3, RFID reader, relay, solenoid, LCD, key lock, body & cover frame of key box	Not Applicable	The solenoid solely manages the front cover frame of the key box; the key can still be accessed independently of the solenoid control, creating the potential for misleading information.


4.1 Cost Estimation

The planning and the cost considerations are crucial aspects of the manufacturing process for any product. Table 4 displays the allocated budget resources for this project, along with the ultimate cost that was incurred. The brand names of the components have been intentionally blurred or left undefined both in the written documentation and accompanying images to uphold confidentiality and align with the recommendations provided by the reviewer.

Table 4. Cost Estimation

No.	Item Photo	Name	Cost
1		Arduino Mega 2560	RM75.00
2		ESP8266	RM20.00
3		LCD screen I2C	RM20.00
4		RFID reader	RM10.00
5		RFID cards (13.56 MHz)	RM2.00 X 20 = RM40.00
6		Keypad 4x3	RM3.00
7		Relay 5 Volt 4-channel	RM10.00

No.	Item Photo	Name	Cost
8		Relay 5 Volt 8-channel	RM17.00 X 2 = RM34.00
9		Electromagnetic solenoids (300mA)	RM10.00 X20 = RM200
10		Power supply 12 Volt 8.5A	RM27.00
11		Wire jumper	RM20.00
12		USB connector (2 slot)	RM7.00
13		PCB board	RM3.00
14		Magnet	RM6.00
15		Hinge	RM5.00

No.	Item Photo	Name	Cost
16		Plywood 12mm	RM70.00
Total			RM550.00

The cost of RM550 in developing this project is deemed affordable, especially compared to the high expenses associated with purchasing existing market models, which typically range from MYR6000 to MYR10,000. For detailed information on the cost breakdown, readers can access the provided link:

https://www.google.com/shopping/product/1?q=www/cost/key/RFID/android+OS.&prds=epd:16415539894090513362,eto:16415539894090513362_0,pid:16415539894090513362&sa=X&ved=0ahUKEwiY_anxwIuDaxWbS2wGHdS2DycQ9pwGCAU

5. Conclusions and Recommendations

The research team has successfully created and built an intelligent essential tracking system prototype. The innovative design illustrates its structure and components, while the fabrication process highlights how the product is physically constructed. Furthermore, the main goal of this research has been accomplished, as this prototype can effectively monitor keys and reduce the chances of missing information while also reducing the time required for key management.

The following research proposal is to find a method or solution for improving this project. Several improvements can be made to enhance the product. Firstly, the electromagnet solenoid is not secure enough. The reason is that the electromagnet solenoid used in this project can be tempered by external individuals, allowing keys to be retrieved without authorization. To overcome this problem, a high-quality electromagnet solenoid is advised.

The hook of the key for the product was made of wood, which is not long-lasting. It is advised that a durable material, such as steel, be chosen for the hook to make it long-lasting.

Author Contributions: Muhammad Qayyim Jefperi: Students research and obtain data contributing to methodology and research. Rineshnaidu Ratnasam: Students research and obtain data to contribute to the writing and production of the original document. Muhammad Affan Mohammad Noor: Students researched and obtained data and contributed to revision and editing. Aminah Ishak: Editing and monitoring articles completed, reviewed, and edited. Rozieana Abu: Text content verification guide and editing. Ahmad Tulka: The primary supervisor and technical advisor contributed during the project, especially in concept, methodology, resources,

writing and revision, supervision, and project management. All authors read and agreed upon the published version of the text.

Funding: No external funding was provided for this research.

Acknowledgments: We are pleased to thank the PTSN for providing the technical support for this innovation development.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Aloi, G., Caliciuri, G., Fortino, G., *et al.* (2016). A mobile multi-technology gateway to enable IoT interoperability. *Proceedings - 2016 IEEE 1st International Conference on Internet-of-Things Design and Implementation, IoTDI 2016*, 259–264. <https://doi.org/10.1109/IoTDI.2015.29>
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787–2805.
- Baashirah, R., Namburi, V., Polisetty, C., *et al.* (2018). An improved novel key management protocol for RFID systems. *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*, 1–5. <https://doi.org/10.1109/LISAT.2018.8378023>
- Gaggioli, A., Pioggia, G., Tartarisco, G., *et al.* (2013). A mobile data collection platform for mental health research. *Personal and Ubiquitous Computing*, 17, 241–251.
- Hakeem, M. J., Raahemifar, K., & Khan, G. N. (2013). A novel key management protocol for RFID systems. *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 1107–1113. <https://doi.org/10.1109/IWCMC.2013.6583712>
- Hamzah, N. H., Amir, F., Harun, H. N. (2021). Design And Development of Key Management System (KeMas) Using RFID Based on ARDUINO MEGA 2560 PRO AND NODEMCU. *Jurnal Kejuruteraan, Teknologi dan Sains Sosial*, Vol. 7 Issue 3.
- Haris, N. I., Hasan, M. Z., Talip, A., *et al.* (2019). Design and development Modish Smart Key Box using RFID based on Arduino WEMOS Mega. *International Research Journal of Engineering and Technology (IRJET)*, 6(06), 551–553.
- Ismail, S., Mustafa, M. Z., & Ahad, R. (2021). RFID application management system in developing key. *Research and Innovation in Technical and Vocational Education and Training*, 1(2), 1–8.
- Jiang, J., Liu, T., Shi, Y., *et al.* (2013). The research on mutual authentication protocol for RFID System based on combined symmetric key. *Advances in Intelligent Systems Research, ICIBET*, 136–139. <https://doi.org/10.2991/icibet.2013.101>
- Kang, S. Y., & Lee, I. Y. (2008). A study on new low-cost RFID system with mutual authentication scheme in ubiquitous. *Proceedings - 2008 International Conference on Multimedia and Ubiquitous Engineering, MUE 2008*, 527–530. <https://doi.org/10.1109/MUE.2008.38>
- Lin, L., Xia, Y., Ji, B., Xie, F., & Jin, Z. (2014). RFID-based intelligent key management device.

- Pavithra, T., & Sreenivasa Ravi, K. (2017). Anti-loss key tag using bluetooth smart. *Indian Journal of Science and Technology*, 10(4). <https://doi.org/10.17485/ijst/2017/v10i4/110669>
- Sarkar, S., Manna, S., & Datta, S. (2017). Smart bag tracking and alert system using RFID. *International Conference on Electrical, Electronics, Communication Computer Technologies and Optimization Techniques, ICECCOT 2017, 2018-January*, 613–616. <https://doi.org/10.1109/ICECCOT.2017.8284576>
- Sadikin, M. F., Kyas, M. (2015). Efficient key management system for large-scale smart RFID applications. *EAI Endorsed Transactions on Energy Web*, 15(6), 1–7. <https://doi.org/10.4108/icst.iniscom.2015.258316>
- Sharma, P., Jindal, R., Borah, M. D. (2021). Blockchain technology for cloud storage. *ACM Computing Surveys*, 53(4), 1–32. <https://doi.org/10.1145/3403954>
- Vegendla, A., Seo, H., Lee, D., *et al.* (2014). Implementation of an RFID key management system for DASH7. *Journal of Information and Communication Convergence Engineering*, 12(1), 19–25. <https://doi.org/10.6109/jicce.2014.12.1.019>
- Wheelus, C., & Zhu, X. (2020). IoT network security: Threats, risks, and a data-driven defense framework. *Internet of Things*, 1(2), 259–285. <https://doi.org/10.3390/iot1020016>
- Zainal, N. (2022). Integration of web-based key booking and monitoring system with smart key rack for university application. *Evolution in Electrical and Electronic Engineering*, 3(1), 225–234.
- Zhang, P. F., Liu, H., & Yu, J. H. (2021). On efficient key tag writing in RFID-enabled IoT. *Sci China Inf Sci*, 64(6): 169305, <https://doi.org/10.1007/s11432-019-2891-3>
- Zhang, Y., Zhang, X., Ao, W., *et al.* (2012). Research of dynamic key management on RFID system. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 1*, 370–372. <https://doi.org/10.1109/ICCSEE.2012.320>

