Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/AF6.20250130
Published: April 8, 2025

Innovative Model in Industrial Safety for Cutting Machines: Applying Intelligent Protection System Based on Arduino

Alonso Sotomayor-Montero, and Carol Oré-Rodrigo
Facultad de Ingeniería, Universidad de Lima
Lima, Peru
20184512@aloe.ulima.edu.pe, 20172420@aloe.ulima.edu.pe

Javier Saul Cordova Ramos
Facultad de Ingeniería, Universidad de Lima
Lima, Peru
jacordov@ulima.edu.pe

Abstract

Industrial accidents involving cutting machines are a significant issue, with hand injuries being the second most common type of accident. According to the Bureau of Labor Statistics, over 1 million workers require emergency treatment annually, with 110,000 cases leading to lost work time. One of the primary reasons for these incidents is the lack of adequate training and access control, resulting in unauthorized or improper machine usage. This study presents the development of an intelligent safety system designed to mitigate these risks through biometric authentication via fingerprint validation. The system ensures that only authorized and trained personnel can operate industrial cutting machines. Additionally, it records essential data such as user identity, usage duration, and access times, enabling enhanced monitoring and operational efficiency. The proposed prototype integrates seamlessly with existing monitoring systems, offering a user-friendly interface that enhances accessibility and reliability. The research methodology involved defining market requirements, designing a functional model using a prototyping approach, and implementing biometric technologies with microcontrollers like Arduino. Testing was conducted in a controlled environment to validate the system's functionality, assess its reliability, and optimize its performance. The results indicate a significant reduction in unauthorized machine access, improved safety measures, and enhanced compliance with industrial regulations. This study highlights the potential of biometric authentication systems in industrial safety, providing a scalable and innovative solution for workplace risk management.

Keywords
Industrial cutting machines, machine protection systems, Arduino-based control, biometric authentication, workplace safety.

1. Introduction
The increasing incidence of workplace accidents, where hand injuries represent the second most common type, highlights the need for more effective safety systems in the management of industrial machinery. According to the Bureau of Labor Statistics, more than 1 million workers are treated in emergency rooms annually due to workplace accidents, with approximately 110,000 cases leading to lost work time (Bureau of Labor Statistics 2023). One of the

main causes of these incidents is the lack of proper training and control over machine use, generating significant risks for both operators and companies (Alshbtat, Zanoon, & Alfraheed 2019).Recent studies have emphasized the role of biometric security in mitigating workplace hazards by restricting machine access to trained personnel. Implementations of fingerprint recognition and IoT-based monitoring systems have demonstrated their effectiveness in improving industrial safety standards (Sarhan 2020). Additionally, integrating machine safety solutions with cloud-based analytics provides real-time alerts and automated compliance tracking, reducing human error and unauthorized access (Kadhim & MohammedAmeen 2020).

In response to this issue, a safety system based on biometric identification through fingerprint validation has been developed, limiting the use of machinery exclusively to authorized and trained operators. This system not only controls access but also records key information such as user identity, usage time, and access hours, facilitating supervision and improving operational management (Wang et al.2021). The designed prototype includes a user-friendly interface and is compatible with existing monitoring systems, ensuring accessibility and efficiency (Zamri, Kamaluddin, & Zaini 2021).The project followed a structured approach that included defining market requirements, designing a functional model through the prototyping method, and integrating biometric technologies with microcontrollers like Arduino. Tests conducted in a controlled environment validated the system's functionality and optimized its design (Areed 2019). This study presents an innovative solution that contributes to reducing workplace risks and strengthening industrial safety measures, addressing a critical market need (Almomani 2021)

Objectives

Develop an innovation model in industrial safety for cutting machines by applying an intelligent system based on Arduino, which is efficient, easy to use and dynamic.

2. Literature Review

According to a study made in the 28 hospitals in the UK for 2 weeks. There were around 1909 injuries only related to hand injuries. In this case these injuries were divided by Mechanism, being the two most common mechanical fall and labour/machine related as well as being labeled as preventable, highlights the need for more effective safety systems in the management of industrial machinery. The rising awareness of preventable hand injuries underscores the importance of improving safety protocols (Lane et al. 2023).Several studies have highlighted the inefficiencies of traditional industrial safety measures. Conventional access control mechanisms such as passwords and keycards are prone to security breaches, lealshbading to unauthorized machine usage and increased workplace hazards (Najim & Mahmood 2021). The implementation of biometric security systems, specifically fingerprint authentication, has proven effective in mitigating these risks by ensuring only trained and authorized personnel can operate industrial equipment (Govender & Umenne 2021).Arduino UNO works as a micro controller that allows the user to control a diverse range of parts that allows the use for dfference purpose such as wifi/ bluetooth, servo motors and has its own power source by a usb cable (R et al. 2021) .

Research indicates that Arduino-based fingerprint authentication provides an affordable and high-security alternative for access control in industrial environments (Magdin et al. 2018). Various studies have explored its applications in smart home security and industrial automation, demonstrating its potential to enhance workplace safety (Ismail et al. 2020). Furthermore, IoT-driven safety solutions have gained prominence in industrial applications, offering real-time monitoring, automated machine locking, and predictive maintenance features (Kumar et al. 2021). These advancements significantly reduce accident rates by enabling proactive safety management and ensuring compliance with operational protocols (Amoran et al. 2021).Additional research has explored integrating biometric access control with cloud-based monitoring systems, improving efficiency in industrial safety management (Zaheen et al. 2020). The adoption of these technologies offers a promising solution for mitigating workplace accidents, optimizing security measures, and reducing operational downtime (Hoque & Davidson 2019). These findings collectively support the feasibility and effectiveness of implementing a biometric-based access control system for industrial cutting machines. By leveraging Arduino technology and IoT-driven solutions, the proposed system provides an innovative and scalable approach to workplace safety.(Omran et al. 2021).

3. Methods

The experimental methodology was used to identify opportunities for improvement, it is necessary to design a prototype and carry out pilot tests to test its effects, acquire information and opportunities for improvement. For this, 5 operators participated in the use of the prototype for 1 month, using the cutting machine in their facilities.

On the other hand, the result of combining hardware with software in order to obtain a semi-automatic model and in contrast to the objective of using Arduino would be fulfilled since it will have this system in such a way that an almost automated system will be achieved. In this case Arduino UNO was selected due to being an economical option that at the same time provides great versatility, making it one of the most popular options for innovation projects (Kondaveeti et al. 2021). Being programmed using the same Arduino software which uses C++ language which requires a power consumption of 5V being powered by a USB device cable which presents a low power consumption compared to other technologies used for these processes. (De Souza et al. 2024).In this case, it was necessary to create a prototype to have a higher level of control and safety in the cutting machines. For this, the generic design model was chosen by steps for prototyping with Arduino: define the problem, conceptualize and prototype see Figure 1. While the steps for prototyping have the following final processes such as communications, design, modeling and deployment (Kondaveeti et al. 2021).

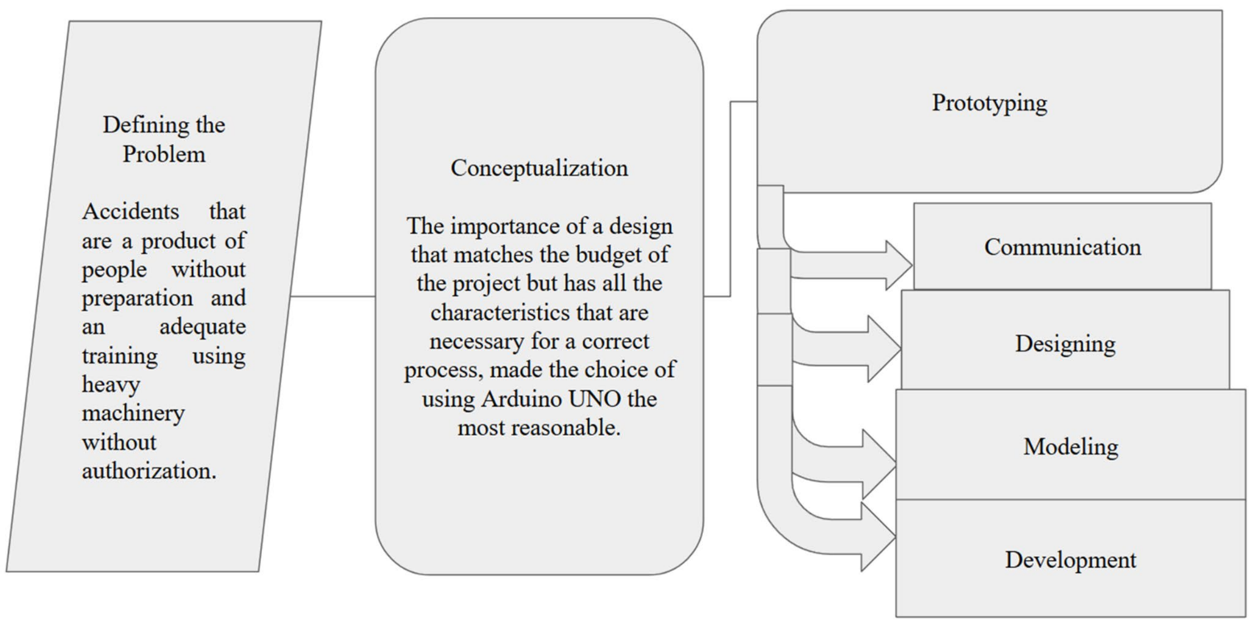

Figure 1. Prototyping Phases

Finally, as a result, the idea was obtained to modify the safety systems so that the issue of human factors is eliminated and thus reduce risks, thus fulfilling the objective of developing the safety system to avoid and prevent workplace accidents.

4. Data Collection

The technological innovation project focuses on developing an intelligent control and management system for industrial cutting machines, with the aim of improving safety, recording operations and optimizing efficiency. This system, based on the Arduino platform, is modular and customizable, incorporating advanced technologies such as sensors, cloud connectivity and an integrated processor. Innovative features include fingerprint recognition applications, an intuitive user interface and multiple fingerprint storage, plus Bluetooth connectivity for remote access management. These features make the system ideal for environments that require secure and convenient access.

The system ensures that only authorized workers can use the machine through fingerprint identification. When a person places their finger on the sensor, the fingerprint is compared with those registered in the database, unlocking the lock if there is a match, which reduces the risk of accidents and prevents unauthorized access. Additionally, during maintenance or repair, an automatic lock is activated that prevents the machine from operating until the process is completed safely, avoiding risks to workers and damage to the machine.

The system also records machine usage and downtime in real time, generating useful information to analyze efficiency and maintenance planning. Recorded data is automatically sent to the maintenance supervisor's processor, allowing quick, centralized access to reports to make data-driven decisions in real time. Regarding the claims, the system improves workplace safety through fingerprint recognition, reducing accident risks and ensuring that the cutter is not accidentally activated during maintenance. Optimizing operational efficiency is possible thanks to real-time logging, which helps identify areas for improvement and reduce downtime. Furthermore, ease of access is achieved without the need for keys or passwords, as all you have to do is place your finger on the sensor.

The system also offers customization and flexibility through its modular design, allowing for specific adaptations such as the integration of additional devices. Remote access management via Bluetooth allows you to add or delete fingerprints and control access from an application on your cell phone. In addition, intelligent maintenance management records downtime and facilitates the scheduling of preventive tasks, reducing the risk of failure and extending the useful life of the machine. Real-time data analysis is possible thanks to the sending of records to the cloud or to the supervisor's processor, allowing exhaustive analysis of the data obtained. Finally, the system is designed to minimize the rate of false positives and false negatives, ensuring a high level of accuracy in fingerprint recognition. It also stands out for its ease of installation, which ensures a simple and quick implementation of the system. For this reason, clear and simple instructions have been included so that at the time of installation there is no need to hire a locksmith specialist.

Finally, our Arduino-based locking system features fingerprint recognition technology to offer a secure, convenient and customizable solution to protect improper access by unauthorized personnel through innovative features. In addition, it has a simple installation to provide the user with a hassle-free access experience and greater peace of mind in terms of security (Youn Kyu Lee, Jongwook Jeong, 2021).
For this work, the problem tree was applied where the problem of accidents that are generated by industrial machines towards unauthorized people is defined and from this, the evidence on the computer system for notifications of accidents produced in industrial machines and the impact that these accidents generate in direct and indirect costs can be seen in Figure 2. Chance tree.

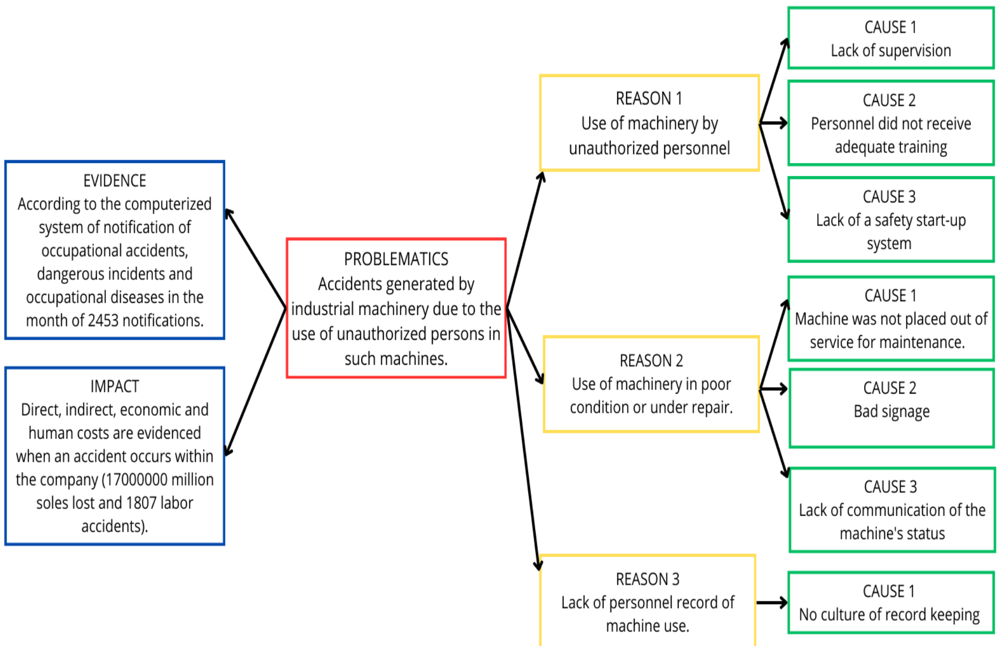

Figure 2. Causality tree

On the other hand, once the problem was defined, we moved on to setting objectives, analyzing the user's needs, past the conceptualization part, budget implementation, prototyping, implementation in a plant-based cutting machine, validation of results; and preparation and writing of the article. The steps to develop the creation of the prototype can be seen in Table.1.

Table 1. Gantt chart

	Time(Weeks)													
Tasks	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Defining the Problem	■													
Key objectives review		■												
Needs analysis			■											
Conceptulization			■	■										
Budget Implementation				■										
Protoyping				■	■	■	■	■	■	■	■			
Communication				■										
Designing				■										
Modelling				■	■									
Deployment						■								
Implementation						■	■	■	■	■	■			
Review and Validation of results											■			

Writing and preparing the article for publication	

5. Results and Discussion

5.1 Numerical Results

For our results, it was necessary to establish the viability of the project, the operation of the Arduino Uno was simulated in Tinkercad, in addition to establishing the diagram, establishing the schematic in Circuito.io as can be seen in Figure 3. Taking into account the state of the art, the considerations were taken of which components are necessary to perform the mentioned functions: SD Module, Arduino UNO, real-time clock (RTC-DS3231), 5V relay and fingerprint reader.

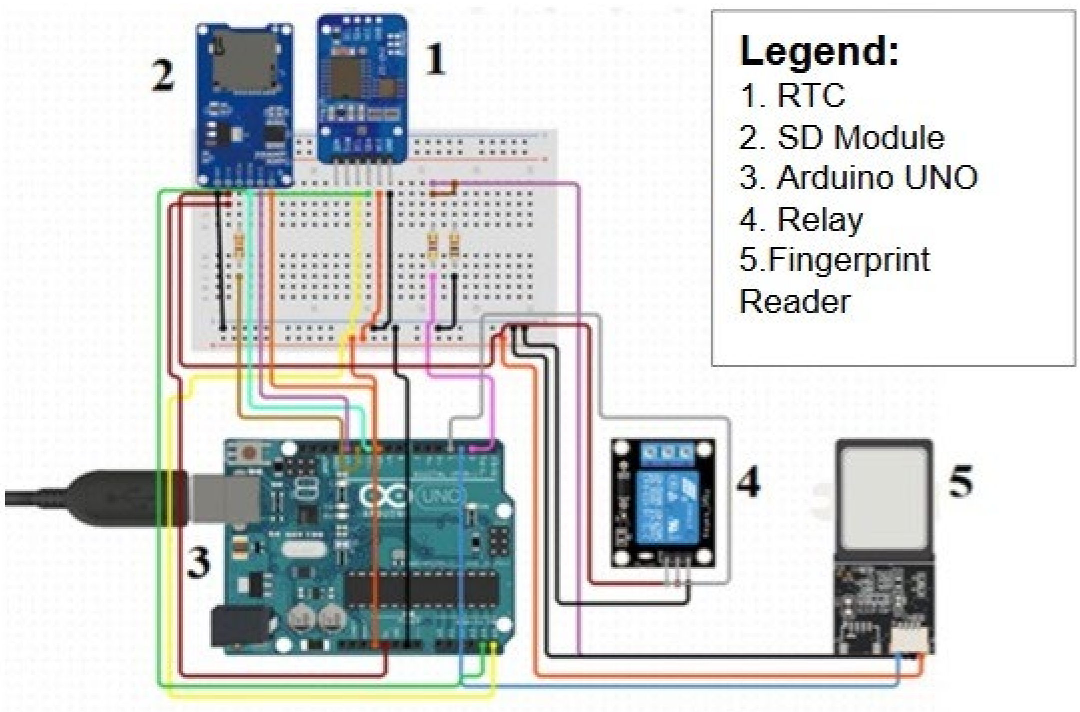

Figure 3. Schematic of the prototype

Once the components of the prototype were simulated, the logic was implemented where the entry of the already registered fingerprint allows the device to be turned on, so that the trained person who has a user to use the machine can access it and in the same way turns off the machine by placing their fingerprint. This system allows you to extract the time it was turned on and the time it was turned off in order to create a database with a user record and its time of use. This information is relevant to have an idea of how long the machine is in use for the purpose of maintenance, which can be observed in the prepared flowchart.

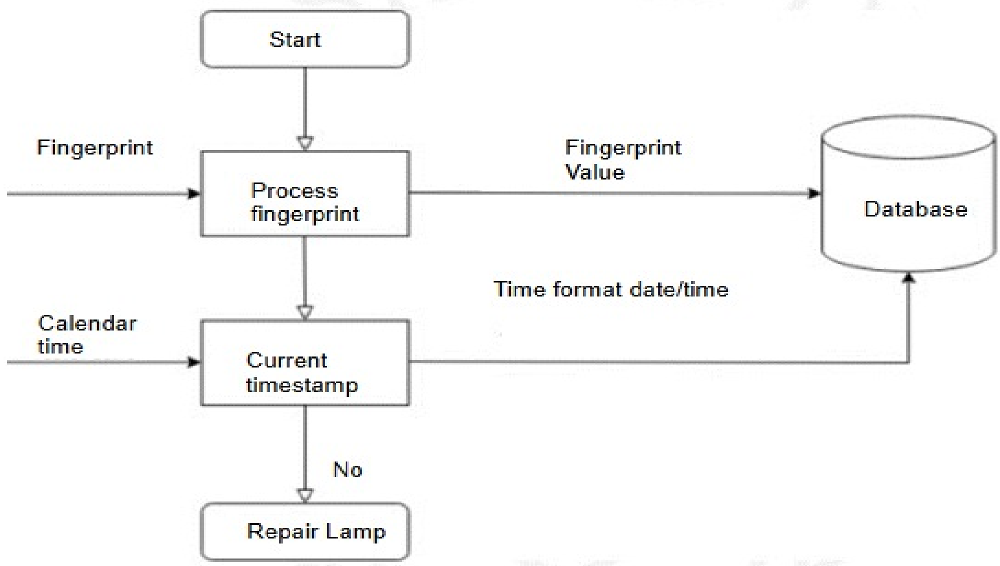

Figure 4. Flowchart of the prototype

After carrying out the tests, the false positive rate could be analyzed as the main criteria, calculated using the following formula.

$$False\ positive\ rate = \left(\frac{\#\ of\ Incorrect\ Authentications\ of\ Unauthorized\ Users}{Total\ Unauthorized\ User\ Authentication\ Attempts}\right) * 100$$

During the testing period, there were no cases of false positives where an unauthorized person could use the machine without having previously registered, the number of false positives being zero with a number of tests of 100 tests during the month and the false positive rate being 0% percent.

While the false negative rate calculated from the following formula.

$$False\ negative\ rate\ = \left(\frac{\#\ of\ Incorrect\ Authentications\ of\ Authorized\ Users}{Total\ Authorized\ User\ Authentication\ Attempts}\right) * 100$$

Where registered persons were unable to access the machine, due to reader failure, during the first 15 days there was a false negative rate of around 54% out of 300 attempts. While the false negative rate went from 54% to 17% in the last 15 days.

$$False\ negative\ rate\ = \left(\frac{\#\ of\ Incorrect\ Authentications\ of\ Authorized\ Users}{Total\ Authorized\ User\ Authentication\ Attempts}\right) * 100$$

Finally, the TRIR (Total Recordable Incident Rate) that was carried out during the month where the test was carried out was taken into account compared to the previous month where it was noted that there was a 6% reduction compared to last month.

$$Total\ Recordable\ Incident\ Rate = \frac{Number\ of\ recordable\ injuries\ and\ illnesses * 192}{Employee\ total\ hours\ worked}$$

$$Total\ Recordable\ Incident\ Rate = \frac{4 * 192}{87.5}$$

Obtaining a result of 8.77% of TRIR, having a reduction of 6%, demonstrating the importance that medium management and control generate can influence the safety of the operator.

5.2 Graphical Results

Once the simulation was carried out in Tinkercad and the development of the prototype with Arduino UNO, Circuito.io, connecting the fingerprint with the Arduino pin number 3, connected to the Breadboard and from the breadboard to the Arduino through pin number 7, with this the prototype circuit is formed. For programming, the Arduino has free software which uses the C + + language. On the other hand, the libraries shown below were used, which are necessary to program the mentioned components: RTC module, SD module and fingerprint. For this, the following libraries were used: Wire.h, RTClib.h, SD.h and Adafruit_Fingerprint.h respectively.

For the correct functioning of the prototype, it was necessary to work with three established scripts where the first is in charge of registering users. For this, a number from 13 to 127 is assigned so that in one of these spaces the user registers their fingerprint in the form of a double confirmation program. This mechanism allows us to have around 114 users with the representation of a fingerprint per user. On the other hand, once a number is chosen, the user must place their fingerprint for a period of 2 seconds. After this, the fingerprint is removed and then the system will ask for the fingerprint a second time to confirm its registration, automatically uploading it to the Arduino memory. One of the aspects is the fact of being able to provide an administrator user who will be in charge of registering authorized personnel, reducing accidents in the workplace.

The second script allows the process where you want to use the machine to request access through your fingerprint, by reading the fingerprint if the program finds that the fingerprint is in the database, which was registered through step one. If the fingerprint is in the system it will be taken as correct access, however; If it is not detected in the database, access will be denied. Additionally, once the machine is on, the user can turn off the machine by placing their fingerprint again. It is worth mentioning that every time access is requested through biometric identification, the RTC module saves the time, day, month and year in the database because this module works independently.

The third script is used to delete the fingerprints from the registry, for this it is simply necessary to enter the fingerprint number registered in step one and carry out the program deleting the fingerprint from the memory of the

Arduino, in this way the person in charge of access can remove users who no longer have access to the machine or do not work for the company.

The proper operation of the fingerprint registration was verified using an LED light. See Figure 5.

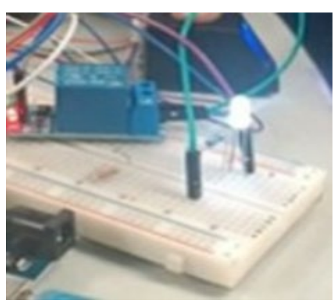

Figure 5. Prototype testing

In the case of the False Negative Rate, a reduction can be observed because the negatives were caused mainly by two main reasons, which were environmental factors and a programming error that generated a loop, which generated not only delays but also identification failures. For this, a simple graph of x and y was used, with the Y axis being the percentages of false negatives and the X axis being the days.

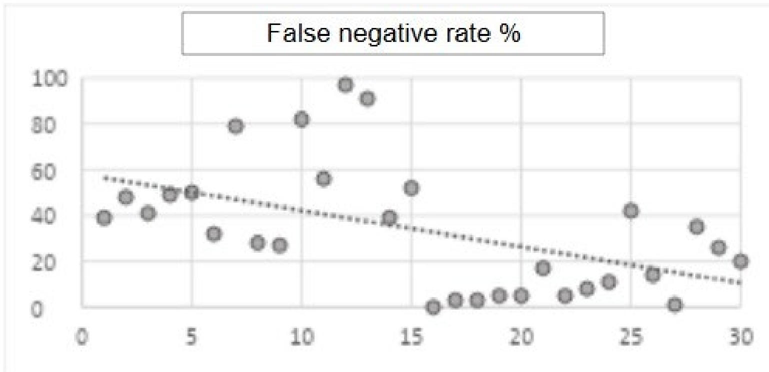

Figure 6. False negative rate

Measures were implemented to reduce environmental factors such as the elimination of particle accumulation in the reader and programming was optimized, the false negative rate was significantly reduced from 54% to 13%. Obtaining an average of this indicator was 33.5% during the month of testing.

5.3 Proposed Improvements

For the proposed improvements, instead of using the Arduino UNO board, you can use a Raspberry board, because Wi-Fi and Bluetooth provide information, records and others. They can be extracted remotely not only waiting for space but also being able to save specific information such as time of use, period of use for specific reports that are relevant to the user.

Another improvement is the management of wiring will help save space by reducing material costs in the production of the equipment's protective box.

The project benefits from an extensive command of C++ and libraries from the fact that shorter, more efficient scripts mean faster processing of this information.

5.4 Validation

For the validation of this project, 20 users have been created, each of them being able to use the system successfully. These tests were carried out on servo motors and LED lights to check that the lock or access to the electrical source works correctly for posterior use in an industrial cutting machine. These accesses receive an input of information from the RTC module, then that information and the fingerprint record represented by a number are stored on a mini SD card connected to an SD module. This information is exported in a .txt format which provides a record of the users' hours of use and hours of work. Due to the capacity of the 8GB card, it provides more than enough capacity for recording information.

```
Initializing SD card...SD Card Ready
Time: 13:25:23  Date:   23/26/2023     ----->FIGERPRINT#1
Time: 13:25:29  Date:   23/26/2023     ----->FIGERPRINT#1
Time: 13:25:29  Date:   23/26/2023     ----->FIGERPRINT#1
Time: 13:25:32  Date:   23/26/2023     ----->FIGERPRINT#1
Time: 13:25:36  Date:   23/26/2023     ----->FIGERPRINT#1
Time: 13:25:41  Date:   23/26/2023     ----->FIGERPRINT#1
```

Figure 7. Record in txt format

A pilot testing phase was carried out in a real industrial environment to evaluate the effectiveness of the system. Metrics were implemented to measure the reduction in accident incidence, access control efficiency, and staff satisfaction.The results of the pilot phase were analyzed to verify if the system met the established objectives. Accident reduction data was collected and feedback surveys were conducted with users to assess system acceptance and performance.Based on the results obtained, adjustments were made to the system to improve its performance and adaptability. Recommendations were developed for large-scale implementation and for the integration of additional features based on the specific needs of different industrial environments.

6. Conclusion

According to the realization of the prototype, it is concluded that it is possible to develop a security system through the Arduino controller that, through correct programming, obtains the expected functionality, with efficiency and effectiveness in its execution as well as versatility and comfort when using it. The conclusion has been reached, thanks to our own research in scientific articles, of the existence of devices involved in the field of security that use the Arduino for their development. In conclusion, it has been verified that both codes and components whose presence has been necessary in this model have been developed based on the criteria that were maintained as objectives within this work. It is also concluded that linking the presented prototype with other applications is possible with some component variations in the assembly of the prototype. 31 Finally, it is concluded that based on a rejected or authorized recognition, the user will receive a direct message depending on the type of recognition that the prototype presents.

References

Alshbtat, A., Zanoon, N., & Alfraheed, M. ,A novel secure fingerprint-based authentication system for student's examination system. International Journal of Advanced Computer Science and Applications, 10(9),(2019). . https://doi.org/10.14569/ijacsa.2019.0100968

Areed, M. F. , A keyless entry system based on arduino board with Wi-Fi technology. Measurement, 139, 34–39, (2019). https://doi.org/10.1016/j.measurement.2019.02.028

De Souza, G. D. S., Lanferdini, F. J., Puntel, F. E., Rossato, C. E., Mota, C. B., & Da Silveira, A. F. , Modified Star Excursion Balance Test: prototype development, correction, and reliability of measurements. Journal of Bodywork and Movement Therapies, 40, 2053–2061, (2024). . https://doi.org/10.1016/j.jbmt.2024.10.071

Govender T. and Umenne P., Design of a Fingerprint Biometric Access Control System with GSM Functionality, International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2021.

Hoque, M. A., & Davidson, C. , Design and implementation of an IoT-Based smart home security System. the International Journal of Networked and Distributed Computing, 7(2), 85,(2019). . https://doi.org/10.2991/ijndc.k.190326.004

Ismail, I. F., Fawzi, M., Jamaludin, W. a. W., Madon, R. H., Abdullah, A. F., & Abdullah, M. A. , Development of a lock biometric authentication system for a battery powered locking device. International Journal of Integrated Engineering, 13(2),(2021). https://doi.org/10.30880/ijie.2021.13.02.003

Information management and IoT technology for safety and security of smart home and farm systems. , Journal of Global Information Management, 29(6), 0, (2021). . https://doi.org/10.4018/jgim.20211101oa22

Kadhim, H. J., & MohammedAmeen, M. J. , Design and implement a smart system to detect intruders and firing using IOT. International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, 10(6), 5932,(2020). https://doi.org/10.11591/ijece.v10i6.pp5932-5939

Kondaveeti, H. K., Kumaravelu, N. K., Vanambathina, S. D., Mathe, S. E., & Vappangi, S. , A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations. Computer Science Review, 40, 100364,(2021). . https://doi.org/10.1016/j.cosrev.2021.100364

Kumar R, Jaya, Chaudhary J., Sensor-based security and alert system for smart home doors, Advances and applications in mathematical sciences, vol. 20, no. 3, pp. 445-457, 2021.

Martin, M., Štefan, K., & Ľubor, F. , Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino. TELKOMNIKA (Telecommunication Computing Electronics and Control), 16(2), 755, (2018). . https://doi.org/10.12928/telkomnika.v16i2.7572

Lane, J. C., Wilkinson, A. L., Giddins, G., Horwitz, M. D., Mason, W., Curtis, A., Jalloh, F., Gomes, K., Gopireddy, R., Sawant, N., Rooker, J., Kurar, L., Jagozinski, N., Wright, A., Hughes, J., Rela, M., Zhu, Y., Teoh, S., Nicholls, A., . . . Sokota, S., Preventable hand injuries: A national audit. JPRAS Open, 38, 305–312,(2023). . https://doi.org/10.1016/j.jpra.2023.10.005

Lee, Y. K., & Jeong, J. , Securing biometric authentication system using blockchain. ICT Express, 7(3), 322–326, (2021). . https://doi.org/10.1016/j.icte.2021.08.003

Najim S. and Mahmood N., Message Alert System for Emergency Situations, International Journal of Computing and Digital Systems, vol. 10, no. 1, pp. 1123-1130, 2021

Omran, M. A., Saad, W. K., Hamza, B. J., & Al-Baghdadi, A. F. , Designing and Manufacturing of Home Automation Monitoring System Using Internet of Things Technology. Journal of Physics: Conference Series, 1973(1), 012081,(2021). . https://doi.org/10.1088/1742-6596/1973/1/012081

Sarhan, Q. I. (2020). Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform. IEEE Access, 8, 128362–128384. https://doi.org/10.1109/access.2020.3008610

R, N. A., Chandru, N., V., & Harish, N., V. , Multilevel security biometric authentication locking system using Arduino UNO. In Advances in parallel computing,(2021b). . https://doi.org/10.3233/apc210121

Wang, R. J., Lai, S. C., Jhuang, J. Y., Ho, M. C., & Shiau, Y. C. , Development of Smart Home Gesture-based Control System. Sensors and Materials, 33(10), 3459, (2021). . https://doi.org/10.18494/sam.2021.3522.

Zaheen, Muhammad Yasir et al. , Exhaustive Security System Based on Face Recognition Incorporated with Number Plate Identification using Optical Character Recognition. Mehran University Research Journal of Engineering and Technology, 39(1), 145-152,(2020) . https://doi.org/10.22581/muet1982.2001.14

Zamri, M. A., Kamaluddin, M. U., & Zaini, N. , Implementation of a Microcontroller-based Home Security Locking System. 2021 11th IEEE International Conference on Control System, Computing and Engineering (ICCSCE),(2021). , . https://doi.org/10.1109/iccsce52189.2021.9530966

Biographies

Alonso Sotomayor-Montero He has a bachelor's degree in industrial engineering from the University of Lima with experience in business intelligence, data analytics, control and management and programming languages. Currently working in the massive consumer sector.

Carol Oré-Rodrigo She has a bachelor's degree in industrial engineering from the University of Lima. My experience includes applying tools to optimize workflows, identifying efficiency opportunities, and proposing innovative solutions to enhance productivity.

Javier Saul Cordova Ramos Holds a Ph.D. in Food Science and is part of the Latin American Center for Teaching and Research in Food Bacteriology (CLEIBA) at the National University of San Marcos (UNMSM). His work focuses on research and education in the field of food bacteriology, contributing to the development of knowledge and practices that enhance food safety and quality