PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

IOT-BASED SMART LOCKER SECURITY WITH SPEECH RECOGNITION

LUQMAN DANIAL MOHD NIZAR
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA,
2022783135@student.uitm.edu.my

ZAINAL FIKRI ZAMZURI*
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA
zfikri@uitm.edu.my

NUR NABILAH MANGSHOR
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA
nurnabilah@uitm.edu.my

Article Info

Received: March 2025
Accepted: September 2025
Available Online: November 2025

Abstract

The IoT-based smart locker security system with speech recognition functions as an advanced solution to boost environmental security together with convenience across university dormitories and public transportation stations and commercial locations. Users benefit from an Arduino-based system which combines speech recognition to replace conventional key or keypad methods for opening their designated lockers. Users can access the system securely through voice command validation with real-time IoT alert communications. The project uses a variant of the waterfall methodology which guides development through stages starting from system design all the way to implementation testing then evaluation. The incorporation of speech recognition software enhances security as it provides users with a hassle-free experience. Review results show this system delivers enhanced locker security capabilities which support its suitability for general adoption by various organizations. The future development should concentrate on bettering speech recognition precision while adding stronger security functions to enhance total robustness.

Keywords: Arduino, Speech Recognition, Locker, Security

INTRODUCTION

The project uses speech recognition technology with Arduino to develop a locking system which promotes personal item security. Human users can conveniently access their personal lockboxes by simply speaking predetermined verbal instructions. The system becomes adaptable due to Arduino's flexibility which allows customization according to locker

dimensions and setting requirements. A user-friendly and secure system exists as the main objective to transform the way locker protection functions in gyms offices and schools.

Problem Statement

IoT-based smart lockers enhance security in university dormitories, public spaces, and residential areas by preventing unauthorized access and theft. Cases like the jewellery theft at a Colorado university in 2021 highlight the need for better locker security (Rapp, T., 2023). Speech recognition technology eliminates key loss issues and enables real-time alert notifications to university staff. Public spaces such as train stations, airports, and malls benefit from secure storage, with European train stations tightening locker security after multiple incidents over the past three decades (Ahmada, R., 2022). IoT-based lockers further mitigate risks by allowing master key access for law enforcement to prevent illegal item storage (Majid, 2022). In residential areas, smart locks like Ring offer remote connectivity but lack speech recognition, a feature integrated into the proposed system for added security and convenience (Yadav, Tanupriya, and Singh, 2020). Future improvements should focus on enhancing speech recognition accuracy and incorporating additional security features.

Objectives

There are 3 objectives for this project:

i. to design an IoT-based Smart Locker Security using speech recognition.
ii. to develop an IoT-based Smart Locker Security using speech recognition.
iii. to test the functionality and the accuracy of the Smart Locker Security.

Scope

This IoT-based smart locker security system, built on the Arduino platform with speech recognition, allows users to access lockers via voice commands instead of traditional keys or keypads. The system ensures secure authentication by validating registered users' voices while blocking unauthorized attempts. Users receive real-time alerts through push notifications and emails whenever locker access occurs, enhancing security monitoring. Designed for university dormitories, public transport areas, and commercial spaces, the system offers an affordable and customizable solution. Security tests will evaluate the speech recognition accuracy, notification reliability, and resistance to breaches, demonstrating its effectiveness over standard lockers. Deadbolt mechanisms will be used for compatibility with smart locking features, unlike mortise locks that require additional mechanical actions.

Study Significance

This project enhances locker security by integrating Arduino and speech recognition, allowing users to access lockers via voice commands instead of physical keys, which are prone to loss or damage. The system improves security in educational and public settings like university dormitories, train stations, and shopping malls by ensuring only authorized users can access lockers. Its modernized access control framework offers both convenience and protection, with a smartphone application serving as a backup in case of speech recognition failure. Given that there are approximately 6.84 billion smartphone users worldwide (Josh H., 2023), this ensures accessibility and reliability. Ultimately, the project provides a cutting-edge security solution that strengthens protection while enhancing user experience across various environments.

LITERATURE REVIEW

This part represents the literature review section. It serves as a key section in a manuscript, summarizing past research and relevant studies that support the current work.

Locking System

Locks date back over 6,000 years, with the earliest known example being a wooden pin lock from Nineveh, the ancient Assyrian capital. This primitive lock operated by lifting pins with a key to release the bolt, preventing unauthorized access (Hu et al., 2023). The Industrial Revolution in the late 18th century significantly advanced lock design, making them more complex and reliable through improved manufacturing processes. Modern locks, including deadbolts, mortise locks, and rim locks, have evolved from these early designs by incorporating new materials and advanced technology to enhance security and functionality (Hu et al., 2023).

Suitable Locks

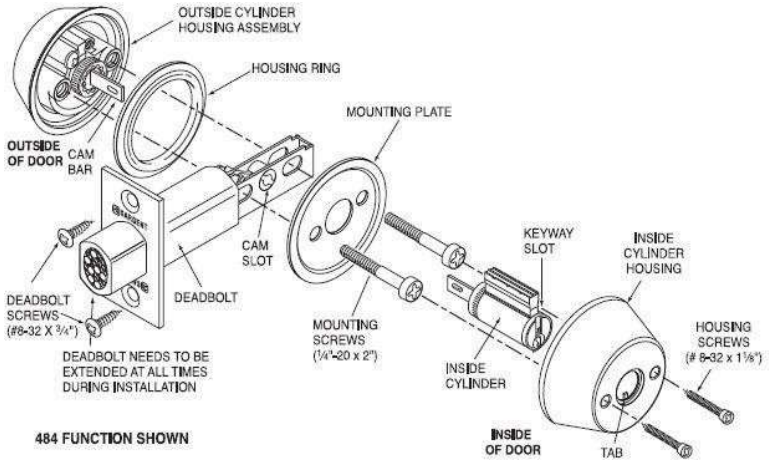

Figure 1: Blowout Diagram of Deadbolt Lock

Figure 1 shows the blowout diagram of a deadbolt lock. Deadbolt locks integrate seamlessly into smart lock systems due to their strong security and user-friendly features. Smart locks like the Ring Doorbell provide keyless entry, remote control, and enhanced protection by using solid metal deadbolts that extend through the door frame, preventing unauthorized entry (Delaney, 2024). These locks add motorized functions to traditional deadbolts and offer multi-layer security through wireless app control, keypad, and fingerprint authentication (Wentland, 2022). They also align with smart home systems, enabling voice control, geofenced notifications, and automatic locking. Their durability and encryption further enhance security and privacy within smart lock frameworks (Paranagama & Hettige, 2022).

Unsuitable Locks

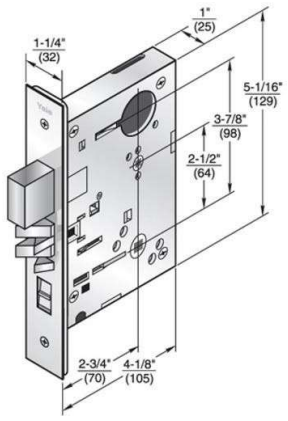

Figure 2: Mortise Lock Diagram

Figure 2 shows the mortise lock diagram. Mortise, rim cylinder, and interconnected locks are unsuitable for smart lock systems like the Ring Doorbell due to their design limitations. Mortise locks are embedded in the door frame, making integration with smart devices difficult, while rim cylinder locks use a simple rotating mechanism that lacks compatibility with smart electronics. Interconnected locks, commonly used in commercial settings, feature dual locking mechanisms that complicate smart lock adaptation. Older locks lack digital connectivity, making smart upgrades impossible. Modern smart locks are specifically designed for integration with mobile apps, home automation, and voice assistants, incorporating essential electronics for remote operation and security monitoring (Caballero-Gil et al., 2023).

Internet Of Things Products

The market offers various IoT-enabled products, including Arduino boards and Raspberry Pi systems, with Arduino requiring an internet module for connectivity. Both platforms are popular for IoT development, though they differ in connectivity and security systems.

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

Arduino

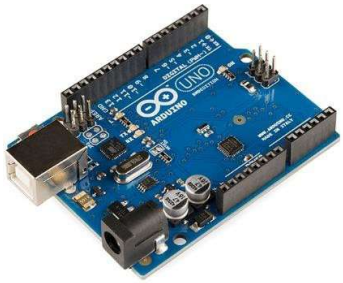

Figure 3: Arduino Uno

Figure 3 shows Arduino Uno. Arduino modules like the Ethernet Shield and Wi-Fi Shield connect to GPIO pins, enabling networking but adding cost and complexity. Arduino excels in real-time control for hardware interaction, such as sensor data collection and actuator control, but its limited processing power and memory make complex IoT features like cloud connectivity and security more challenging (Areed, 2019).

Raspberry Pi

Figure 4: Raspberry Pi5

Figure 4 shows Raspberry Pi5. Raspberry Pi boards come with built-in networking capabilities, including Ethernet, Wi-Fi, and Bluetooth, which simplify setup by eliminating the need for additional modules. As full-fledged computers, they offer robust computational power, enabling advanced IoT features such as cloud integration, data processing, and security measures through a Linux-based operating system. This operating system also supports various IoT frameworks like Node-RED, simplifying application development and providing better security updates compared to Arduino's bare-metal approach (Howser, 2020).

Speech Recognition Algorithms

Speech recognition systems convert spoken words to text using machine learning and deep learning algorithms. They incorporate acoustic models to analyze audio features and detect phonemes, language models to predict word sequences, and decoding methods that integrate both components. Recent deep learning advancements have significantly improved the performance and speed of these systems, making them viable for mobile applications (Reddy et al., 2022).

Deep Learning

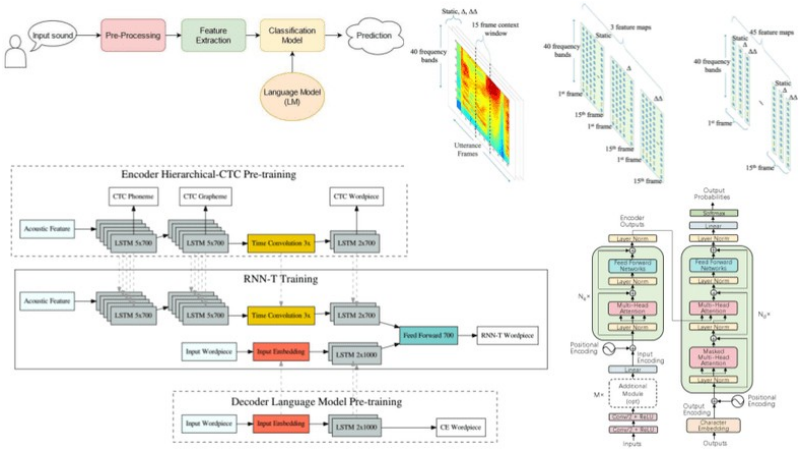

Figure 5: Deep Learning Model for Speech Recognition

Figure 5 shows the Deep Learning Model for Speech Recognition. Speech recognition relies on deep learning techniques that transform auditory waves into spectrograms, extract features, and use neural networks like RNNs and LSTMs to predict verbal output. These systems mimic human hearing by analyzing and cross-referencing stored word sounds, with deep learning significantly improving performance and efficiency (Papastratis, 2021). Multiple processing layers enable advanced tasks such as automatic speech recognition, text-to-speech synthesis, and emotion recognition (Mehrish et al., 2023). Cutting-edge models integrate CNNs, RNNs, and transformers, simplifying training and enabling small deployable models for mobile devices, expanding research and innovation in speech processing (Zeng, 2023).

Machine Learning

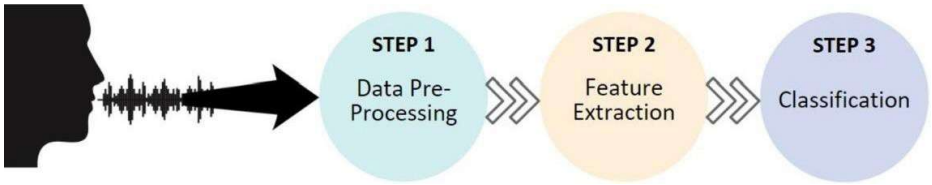

Figure 6: Machine Learning Process

Figure 6 shows the basic process of machine learning for speech recognition. Audio mining begins with acquiring and cleaning extensive recordings and transcripts, structuring data in a frequency-based format for machine learning models to analyze patterns through supervised learning. After training, the system undergoes fine-tuning with new data, using language analysis for improved transcription accuracy before deployment in voice assistants and automated transcription services. Speech recognition relies on Hidden Markov Models (HMMs) for analyzing sound sequence patterns and Gaussian Mixture Models (GMMs) for handling speech variations like pitch, volume, and accents. While deep learning has advanced modern systems, HMMs and GMMs remain foundational in speech recognition by enabling accurate transcription.

Previous Works

Smart locks date back to 1873 when James Sargent invented the first time lock, which only opened at a predetermined time, revolutionizing bank vault security. He later developed a time-delay combination lock in 1880, adding a timer mechanism for enhanced security (Haiston, 2023). Comparing previous research, key differences emerge in unlocking methods, IoT availability, and security. Gupta et al.'s (2022) "Smart Door Locking System Using IoT" and Derbali's (2023) "Toward Secure Door Lock System" use mobile applications, while Singh et al.'s (2020) "OTP-Based Door Lock System" relies on one-time passwords. Unlike these, the proposed IoT-based Smart Locker Security with Speech Recognition integrates speech recognition and mobile applications. It also employs MQTT-TLS encryption via ESP32 for stronger security, distinguishing it from past studies that lack detailed security implementations.

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

METHODOLOGY

The development process of this project receives detailed explanation through a systematic review of its modeling approach stages. The chapter discusses the reasons for the selected research design and data collection methods alongside hardware and software requirements which the project demands.

Modified Waterfall Model

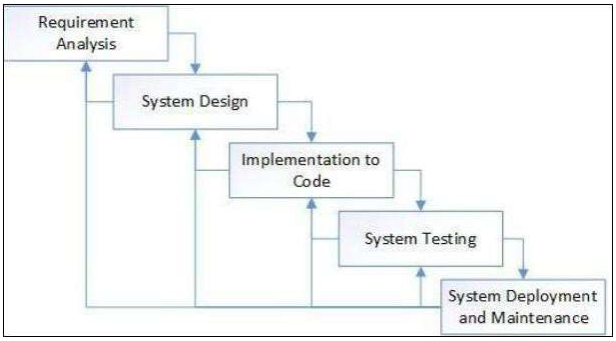

Figure 7: Modified Waterfall Model

Figure 7 depicts the modified waterfall model. The Waterfall method, introduced by Winston Royce in 1970, follows a sequential approach with strict documentation and limited client interaction, making it rigid and prone to poorly designed systems when early-phase issues go unresolved. To address its limitations, the Modified Waterfall Model introduces iterative loops and feedback mechanisms, enhancing flexibility in requirement adjustments and project changes. This model consists of six phases: Requirement Analysis, System Design, Implementation to Code, System Testing, and System Development and Maintenance. Unlike the original, it allows revisiting previous stages for modifications, incorporating prototyping and incremental development to ensure stakeholder involvement. While this project excludes maintenance implementation, thorough documentation replaces its role by covering the entire development process.

Flowchart

Figure 8 and Figure 9 depicts a flowchart. A flowchart visually represents the software system architecture and specifications during the System Design phase, beginning with a "Start" symbol. Rectangular boxes depict key design activities, including architectural, high-level, detailed, and user interface design, while diamond-shaped symbols indicate decision

points that guide designers in selecting alternatives based on predefined criteria. The sequence concludes with an "End" symbol, ensuring a structured representation of the design process. By organizing elements systematically, the flowchart highlights decision-making points and interconnections, simplifying design complexity and providing a clear overview of the system's development path.

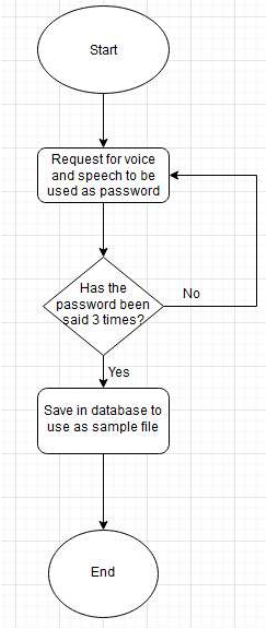

Figure 8: Voice Recognition Training

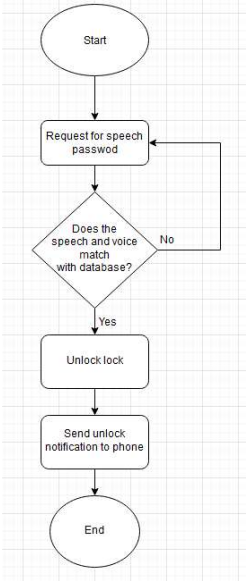

Figure 9: Voice Recognition activation

Table 1: System Library

Library	Functionality
SoftwareSerial.h	Used to enable serial communication on other digital pins of the Arduino.
VoiceRecognitionV3.h	A library to interface with the Elechouse Voice Recognition V3 module for recognizing voice commands.
Wifi.h and WifiClient.h	Used for ESP32 Wi-Fi connectivity.
BlynkSimpleEsp32.h	Part of the Blynk platform, enabling IoT control via a mobile app or web interface.

RESULT AND DISCUSSION

This section presented the findings of the study and explained how the IoT-Based Smart Locker Security with Speech Recognition improves security. The evaluation focused on accuracy, notification system, and overall user experience.

Testing Phase

The testing phase, conducted after system implementation, ensures all components function correctly and are user-friendly. Individual components undergo testing, followed by integration testing to confirm seamless operation. Functionality testing verifies proper system performance, while usability testing assesses user satisfaction and effectiveness. The development strategy incorporates accuracy and usability standards to create a reliable, user-friendly interface, ensuring the system is ready for deployment and meets project objectives. Table 2 details the specific aspects tested to identify and resolve issues before the system goes live.

Table 2: Test Case

Test Case	Expected Result	Success/Failure
Microphone Sensitivity	User must be close to the mic to be able to unlock the locker	User needs to be within 10-15 centimeters of the microphone
Notification System	User gets the notification that the locker has been unlocked	Success
Accuracy Testing	Other users are unable to unlock the locker despite saying the correct password	Needs more training to get better accuracy

Microphone Sensitivity

The microphone performs optimally when users stand 10 to 15 cm away, ensuring proper voice command processing due to its limited reception range. While this range does not impact regular use, it may pose challenges when users cannot approach the microphone. Sensitivity adjustments could extend the range, enhancing system versatility and usability in different situations.

Notification System

The Notification System was tested to ensure it informs users when the locker is unlocked, and results confirmed it successfully sends real-time alerts through the Blynk application. These popup messages provide immediate awareness of locker access, enhancing security by allowing continuous monitoring. Since the system performed reliably, no further adjustments are needed. Figure 10 displays the notification when the lock is in the unlocked state.

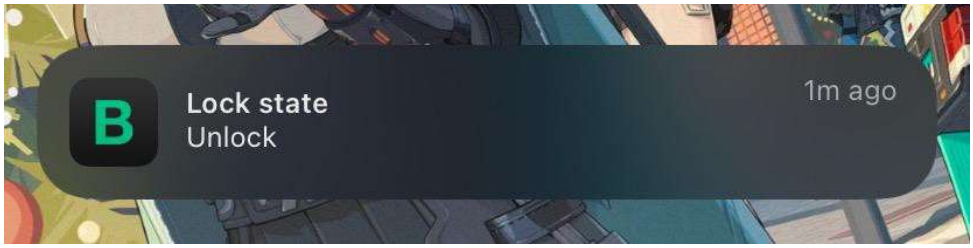

Figure 10: Lock State Notification

Voice Accuracy Training

The Accuracy Testing process revealed occasional difficulties in matching the user's voice with the stored password, likely due to limited training data. Since the system relies on recorded

voice samples for verification, a larger dataset would improve recognition consistency. Insufficient training data may cause issues in distinguishing similar voices or recognizing the user under varying conditions. Increasing training sessions and refining the learning process would enhance accuracy and overall performance.

CONCLUSION

The IoT-Based Smart Locker Security with Speech Recognition system was successfully developed using the ESP32 microcontroller and Arduino Nano, with the Elechouse Voice Recognition V3 enabling voice-responsive security for locker access. The voice recognition system accurately identified authorized commands, providing high security and user-friendly convenience. Users received real-time notifications through the Blynk app interface, enhancing their experience. Testing confirmed the locker's reliable performance under various conditions, highlighting its suitability for daily use. The project showcases the potential of IoT and voice recognition to improve security and pave the way for intelligent connected devices in future developments.

Limitations

This project has a few limitations, including the microphone's limited reception range of 10 to 15 centimetres, which may affect usability in certain situations. The voice recognition system struggles with accuracy due to limited training data, making it less reliable under different voice conditions. Additionally, the notification system relies on an internet connection, meaning it may fail if connectivity is lost. Addressing these limitations through hardware adjustments, increased training data, and offline functionality improvements could enhance the system’s overall performance.

Limitations with Elechouse Voice Recognition V3

The IoT-Based Smart Locker Security with Speech Recognition faced limitations, particularly with the Elechouse Voice Recognition V3 module's sensitivity to background noise, requiring a quiet environment for accurate recognition. The module's fixed set of trained commands limited functionality expansion, as adding new commands required overwriting existing ones. Variations in a user’s voice due to illness, fatigue, or accent changes sometimes reduced recognition accuracy. The system also required close-range usage, as the module

struggled with distant commands, limiting hands-free operation. Additionally, the offline nature of the module prevented cloud-based AI learning, reducing adaptability. Despite these limitations, the project demonstrated the effectiveness of voice-commanded smart security, with future improvements possible through AI integration and noise reduction enhancements.

Limitations with Arduino Nano

The main constraint of using the Arduino Nano as a microcontroller is its limited memory resources, with only 2 KB RAM and 32 KB flash storage, restricting its ability to handle complex voice functions and large digital data. Additionally, it lacks built-in Wi-Fi or Bluetooth, requiring extra components for IoT connectivity. Its 8-bit ATmega328P processor operates at a slower speed, causing delays in voice command processing. While the ESP32 offers superior power with Wi-Fi and Bluetooth, it is incompatible with the Elechouse Voice Recognition V3 due to voltage differences, requiring level shifting for proper operation. The ESP32 also struggles with real-time voice processing due to memory limitations and high processing demands, making Arduino Nano the only viable option despite its constraints.

Future Works

To enhance the Smart Locker Security system, several upgrades are necessary, including switching to superior voice recognition models like Google's Speech-to-Text API and Alexa, and integrating a noise-cancelling microphone for better accuracy in various environments. The system should support multiple user profiles for broader applications, such as offices and dormitories, and include remote access via mobile apps for real-time status updates and alerts. Additionally, adding fallback authentication methods like fingerprint scanning or PIN entry ensures access during voice recognition failures. Expanding the voice detection range and incorporating Bluetooth or Wi-Fi support would improve convenience, allowing users to control the system from a distance, making it more practical and secure for diverse commercial uses.

REFERENCES (APA 7TH EDITION)

Ahmada, R. (2022, August 17). *Why is there no longer left luggage in train stations?*. NannyBlog. https://blog.nannybag.com/en/luggage-storage-train-stations/

Caballero-Gil, C., Álvarez, R., Hernández-Goya, C., & Molina-Gil, J. (2023, May 27). *Research on smart-locks cybersecurity and vulnerabilities*. SpringerLink. https://link.springer.com/article/10.1007/s11276-023-03376-8

Debnath, A., Samanta, S., & Das, P. (2023). *IOT based smart door lock system using Arduino*. RCCIIT. https://www.rcciit.org/students_projects/projects/ee/2023/GR6.pdf

Derbali, M. (2023). Toward secure door lock system: Development IoT smart door lock device. *Authorea (Authorea)*. https://doi.org/10.22541/au.168055385.54003954/v1

Dimitrakakis, C., & Bengio, S. (2011). Phoneme and sentence-level ensembles for speech recognition. *Eurasip Journal on Audio, Speech, and Music Processing*, *2011*. https://doi.org/10.1155/2011/426792

Haiston, J. (2023). *Smart door locks vs. traditional deadbolts*. Symmetry Electronics. https://www.symmetryelectronics.com/blog/smart-door-locks-vs-traditional-deadbolts/

Jiang, S., & Chen, Z. (2023). Application of dynamic time warping optimization algorithm in speech recognition of machine translation. *Heliyon*, *9*(11), e21625. https://doi.org/10.1016/j.heliyon.2023.e21625

Kostadinov, D. (2021, July 30). *Engineering speech recognition from Machine Learning*. Infosec. https://www.infosecinstitute.com/resources/machine-learning-and-ai/engineering-speech-recognition-from-machine-learning/

Papastratis, I. (2021, July 14). *Speech recognition: A review of the different deep learning approaches*. AI Summer. https://theaisummer.com/speech-recognition/

Paranagama, C., & Hettige, B. (2022, July). *A review on existing Smart Door Lock Systems*. ResearchGate. https://www.researchgate.net/publication/362015418_A_Review_on_Existing_Smart_Door_Lock_Systems

Rapp, T. (2023, October 30). *Police investigating after jewelry stolen from Colorado locker room during UCLA loss*. Bleacher Report. https://bleacherreport.com/articles/10095344-police-investigating-after-jewelry-stolen-from-colorado-locker-room-during-ucla-loss

Singh, A., Sachan, A., Gupta, K., Kapoor, G., Singh, H. K., & Singh, A. (2022, May). *IOT BASED SMART LOCK*. International Research Journal of Modernization in Engineering Technology and Science. https://www.irjmets.com/uploadedfiles/paper/issue_5_may_2022/22792/final/fin_irjmets1652445748.pdf

Zeng, T. (2023, January). *Deep Learning in Automatic Speech Recognition (ASR)*. Atlantis Press. https://www.atlantis-press.com/article/125977784.pdf