Project Notes:

Project Title: Autonomous Bicycle Lock
Name: Adnan Dembele

Note Well: There are NO SHORT-cuts to reading journal articles and taking notes from them. Comprehension is paramount. You will most likely need to read it several times, so set aside enough time in your schedule.

Contents:

Knowledge Gaps:

This list provides a brief overview of the major knowledge gaps for this project, how they were resolved and where to find the information.

Knowledge Gap	Resolved By	Information is located	Date resolved
Arduino	Watching videos on youtube + attending the Creative Engineering and Design Club	Control a DC Motor with Arduino (Lesson #16) - YouTube DC Motor Control with an H-Bridge and Arduino (Lesson #17) - YouTube	10/29/2023
RFID	Articles	RFID Security Issues & Challenges Door Lock using RFID and Arduino	12/09/2023
Event (RFID) and action (motors) on Arduino	Watching videos on youtube	DC Motor Control with an H-Bridge and Arduino (Lesson #17) - YouTube	10/29/2023
Locks and how they work	Article	Arduino Integrated Portable RFID Bicycle Lock	10/09/2023

Literature Search Parameters:

These searches were performed between 08/01/2023 and 12/15/2023.
List of keywords and databases used during this project.

Database/search engine	Keywords	Summary of search
Scopus	RFID, Arduino, Bike Lock, Automated Bike Lock, Automation, Smart Lock, IoT, Solenoid, Smart Bike, Bike Automation	I basically looked for anything regarding bicycles, smart locks and projects including Arduino. I mostly found projects related to smart door locks.
ScienceDirect		
Google Scholar		

Tags:

Tag Name	
Bicycle Safety	Bicycle Lock
Electric Lock	Security
Arduino	Smart Lock
Lock	RFID/NFC
Solenoid	Smart Home
Electric Lock	Lock Control

Article #1 Notes: Template

Article notes should be on separate sheets

KEEP THIS BLANK AND USE AS A TEMPLATE

Source Title	
Source citation (APA Format)	
Original URL	
Source type	
Keywords	
#Tags	
Summary of key points + notes (include methodology)	
Research Question/Problem/ Need	
Important Figures	
VOCAB: (w/definition)	
Cited references to follow up on	
Follow up Questions	

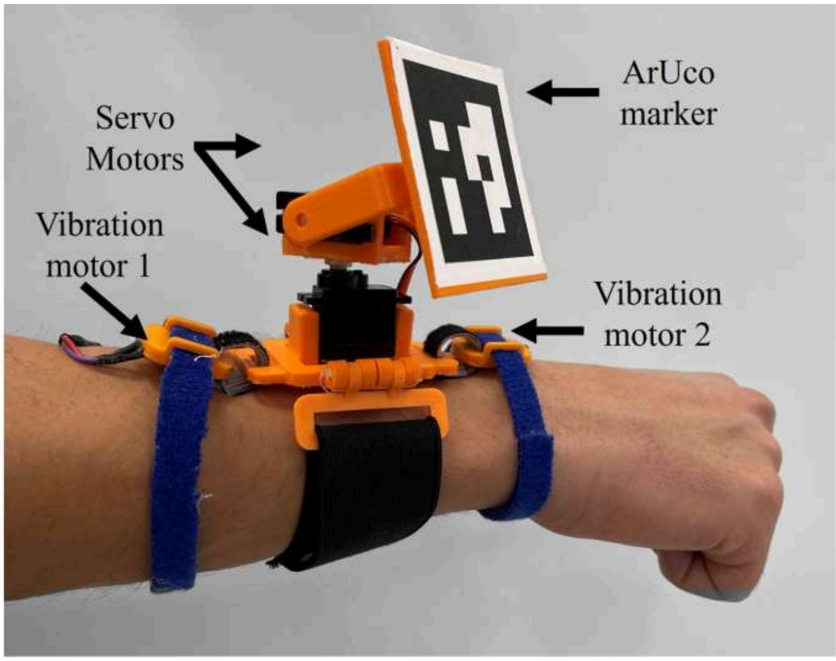
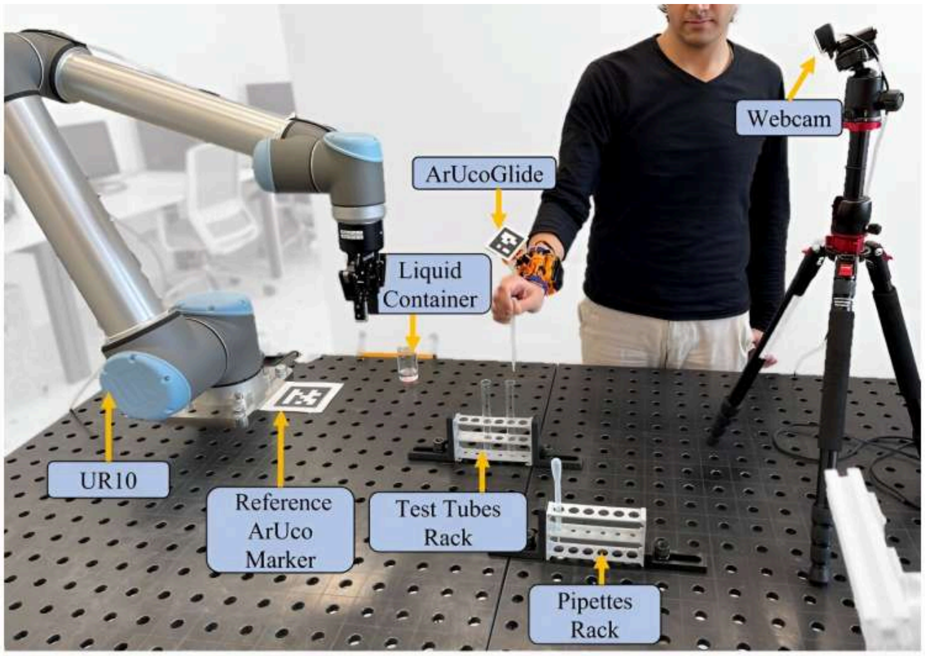
Article #1 Notes: Astronauts get first look at the spacecraft that will fly them around the moon

Source Title	Astronauts get first look at the spacecraft that will fly them around the moon
Source citation (APA Format)	Dunn, M. (2023, August 9). Astronauts get first look at the spacecraft that will fly them around the moon. *Phys.org*. https://phys.org/news/2023-08-astronauts-spacecraft-fly-moon.html
Original URL	https://phys.org/news/2023-08-astronauts-spacecraft-fly-moon.html
Source type	Journal Article
Keywords	Capsule, heat shield, Artemis, Starship, moon
#Tags	Rocket, moon, space exploration, Artemis
Summary of key points + notes (include methodology)	The four astronauts that NASA plans to send around the moon next year inspected the capsule. There are some concerns about the heat shield though, especially after the empty test flight around the moon due to burns and material losses at the bottom of the capsule during reentry, This might delay the trip. The next mission of the Artemis program is a moon landing and might cause even more trouble, delaying it to late 2025 to even 2026. The main problem is the rocket that will bring the astronauts to the moon and back. Starship has had only one test flight, which ended in an explosion right after liftoff. NASA refuses to let astronauts board starship until Elon Musk tests the spacecraft again and again while executing all the necessary maneuvers.
Research Question/Problem/ Need	When will be the next Artemis mission? What are the issues with the spacecraft that need to be resolved?

Important Figures	Picture of the astronauts and the capsule
VOCAB: (w/definition)	Heat shield- an instrument that protects the capsule with the astronauts from burning during reentry
Cited references to follow up on	
Follow up Questions	How will Elon Musk resolve these issues? Are there more effective ways or methods for reentry and landing?

Article #2 Notes: A novel motion-capture system with robotic marker that could enhance human-robot interactions

Source Title	A novel motion-capture system with robotic marker that could enhance human-robot interactions
Source citation (APA Format)	Fadelli, I. (2023, August 10). A novel motion-capture system with robotic marker that could enhance human-robot interactions. *Tech Xplore*. https://techxplore.com/news/2023-08-motion-capture-robotic-marker-human-robot-interactions.html
Original URL	https://techxplore.com/news/2023-08-motion-capture-robotic-marker-human-robot-interactions.html
Source type	Journal Article
Keywords	Human-robot interactions, robots, motors, safety
#Tags	Robot, motors, robotics, robots and safety
Summary of key points + notes (include methodology)	Some Researchers at the Skolkovo Institute of Science and Technology realized that there was a problem with robots and humans working together. Robots would often harm humans during their interactions. Due to this, the researchers developed a system that would ensure the well being of humans during their interactions with robots. By wearing a robot attached to the wrist, just like a watch, the researchers managed to notably ameliorate humans' safety while working with robots. The way the system works is with a camera recording the robot and human interaction, the wrist-worn robot adjusts its marker to always face the camera, and finally, the collision controller moves the robot in a way to make sure to avoid colliding with the human wearing the wrist-worn robot. In the future, the researchers would like to advance this project even more by creating a full-body suit with the same technology. This kind of technology could be useful with robot interactions with medical personnel, and even virtual reality.
Research Question/Problem/ Need	Human-robot interactions are evolving fast and more and more industries work with robots, but robots often hurt humans during their interactions

Important Figures	 ArUco marker Servo Motors Vibration motor 1 Vibration motor 2 Image of the device and all of its parts in action  Webcam ArUcoGlide Liquid Container UR10 Reference ArUco Marker Test Tubes Rack Pipettes Rack Example of how the device could be used to ease human-robot interactions
VOCAB: (w/definition)	
Cited references to follow up on	Ali Alabbas et al, ArUcoGlide: a Novel Wearable Robot for Position Tracking and Haptic Feedback to Increase Safety During Human-Robot Interaction, arXiv (2023). DOI: 10.48550/arxiv.2307.08363

Follow up Questions	How can this project be advanced further? Could the device be expanded into a full body suit in order to have robots everywhere (in the streets (cars), restaurants, etc.)? How cheap can the device become? Is this really the best way to make human-robot interactions more safe?

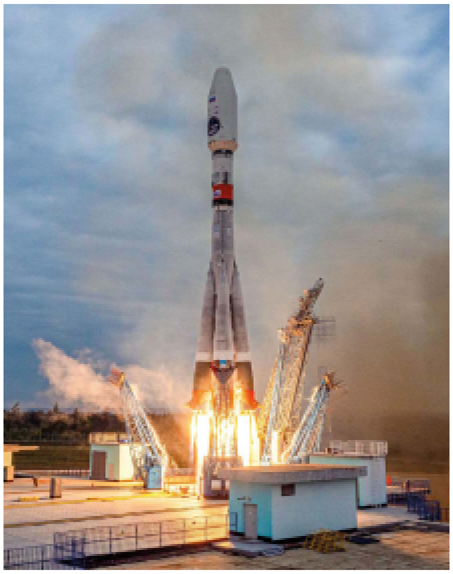
Article #3 Notes: Stacking cells in thin layers could result in higher-performance solid-state batteries

Source Title	Stacking cells in thin layers could result in higher-performance solid-state batteries
Source citation (APA Format)	Swiss National Science Foundation. (2023, August 9). Stacking cells in thin layers could result in higher-performance solid-state batteries. *Tech Xplore*. https://techxplore.com/news/2023-08-stacking-cells-thin-layers-result.html
Original URL	https://techxplore.com/news/2023-08-stacking-cells-thin-layers-result.html
Source type	Journal Article
Keywords	Battery, lithium ion, safety, portability, energy
#Tags	Battery, portable, solid-state battery
Summary of key points + notes (include methodology)	What we imagine today as the optimal battery is portable, safe, high energy, and fast charging. The batteries we use today though, never have all those attributes. For example, lithium ion batteries require several minutes to charge and discharge, which limits the use of high power, and the flammability of those batteries make them relatively unsafe. Scientists at Empa have been working on a thin-film battery that contains those optimal attributes. They used physical vacuum deposition to put the thin-film battery material on a substrate, which led to an increase in the energy storage capacity, but they still had to reduce the substrate's part of the weight. To accomplish this, they stacked two thin-films on top of another on the same substrate and it worked. The prototype was charged in only one minute and could compete against current and future lithium ion batteries. Scientists consider adding more thin-film layers on the same substrate, an optimal amount of 10. Because of the cost of making these batteries, they will be reserved for energy and safety-demanding usage such as aircraft and satellites.
Research Question/Problem/ Need	Batteries today constantly lack at least one attribute, whether it is speed of charging, high capacity, safety, or portability.

Important Figures	 Picture of the battery
VOCAB: (w/definition)	
Cited references to follow up on	Moritz H. Futscher et al, Monolithically-stacked thin-film solid-state batteries, *Communications Chemistry* (2023). DOI: 10.1038/s42004-023-00901-w
Follow up Questions	Why don't the anodes add up when stacked but not touching each other? Where could this type of battery be used? Would we be able to further increase the capacity and availability for the average consumer?

Article #4 Notes: Russia launches first Moon mission in half a century: what it means for science

Source Title	Russia launches first Moon mission in half a century: what it means for science
Source citation (APA Format)	O'Callaghan, J. (2023, August 10). Russia launches first Moon mission in half a century: what it means for science. *Nature*. https://www.nature.com/articles/d41586-023-02536-2
Original URL	https://www.nature.com/articles/d41586-023-02536-2
Source type	Journal Article
Keywords	Luna 25, Water ice, crater, robotic arm
#Tags	Rockets, launch, moon, south pole of the moon
Summary of key points + notes (include methodology)	Russia just launched a spacecraft, heading, like many future missions, to explore the moon's south pole. It is planned to land on August 21, in the Boguslawski crater. The mission is described as being risky, with a 70% chance of success. Luna 25 weighs 1 750 kg, carrying only 30 kg of instruments. Its main instrument is a robotic arm for digging. The purpose of this mission is to try to find water ice, which could be useful in finding out about the formation of our solar system, but also because it might be a valuable resource for other missions by providing hydrogen and oxygen. There are many other missions planned for exploring the moon's south pole and the water ice that can be found there. There is the Chandrayaan-3, which is planned to land there on August 23, the Artemis program from NASA, and China also plans to land a rover there. Landing on the moon will be an issue though. Several missions before this one have crashed on the moon's surface.
Research Question/Problem/ Need	The moon's south pole is still a mystery to humans and could contain valuable resources to learn more about the solar system or to provide fuel for missions to mars and beyond.

Important Figures	 Luna 25 launched from eastern Russia. Image of the launch
VOCAB: (w/definition)	
Cited references to follow up on	
Follow up Questions	When will we build a space station or research station on the moon? How many other space organizations will try to go to one of the moon's poles? How much help could water-ice be?

Article #5 Notes: Addressing the harms of AI-generated inauthentic content

Source Title	Addressing the harms of AI-generated inauthentic content
Source citation (APA Format)	Menczer, F., Crandall, D., Ahn, YY. *et al.* Addressing the harms of AI-generated inauthentic content. *Nat Mach Intell* 5, 679–680 (2023). https://doi.org/10.1038/s42256-023-00690-w
Original URL	Addressing the harms of AI-generated inauthentic content | Nature Machine Intelligence
Source type	Journal
Keywords	Inauthenticity, AI, manipulation, generative AI
#Tags	AI, Computer Science, ChatGPT, generative AI, chatbot
Summary of key points + notes (include methodology)	AI Nowadays can be a very useful tool but also harmful. Current AI tools are able to create inauthentic but convincing content in large amounts, even creating false pictures that seem real. With the amelioration of AI, humans won't be able to distinguish AI-generated content vs real content. We need solutions to slow down and eventually stop these threats to society. AI to detect AI won't work because AI can be trained to avoid detection from other AI, but another way to go is to change the detection from one person to a group of people, algorithms that detect similar content and behavior, a global moderation of the use of technology, or several regulations.
Research Question/Problem/ Need	How can we regulate the harms of AI inauthenticity?
Important Figures	
VOCAB: (w/definition)	AI- artificial intelligence CAPTCHA- a way to differentiate between humans and a program, system, AI, or robot
Cited references to follow up on	1. Marcus, G. Comm. ACM https://cacm.acm.org/blogs/ blog-cacm/267674-ais-jurassic-park-moment/fulltext (2022). 2. Menczer, F. & Hills, T. Sci. Am. 323(6), 54–61 (2020). 3. David, M. J. et al. Science 359, 1094–1096 (2018). 4. Pierri, F. et al. Sci. Rep. 12, 5966 (2022). 5. Ferrara, E., Varol, O., Davis, C., Menczer, F. & Flammini, A. Comm. ACM

	59(7), 96–104 (2016). 6. Else, H. Nature 613, 423 (2023). 7. Pacheco, D. et al. in Proc. International AAAI Conference on Web and Social Media vol. 15 (eds. Pacheco, D. et al.) 455–466 (2012). 8. Yasseri, T. & Menczer, F. Preprint at https://doi. org/10.48550/arXiv.2104.13754 (2023). 9. van Dis, E. A. M., Bollen, J., Zuidema, W., van Rooij, R. & Bockting, C. L. Nature 614, 224–226 (2023). 10. Goldstein, J. A. et al. Preprint at https://doi.org/10.48550/ arXiv.2301.04246 (2023)
Follow up Questions	Should AI be allowed to generate images? How dangerous and harmful to society can AI get?

Article #6 Notes: Cloudy

Source Title	Cloudy
Source citation (APA Format)	Woods, P. Cloudy. *Nat Astron* 7, 1002 (2023). https://doi.org/10.1038/s41550-023-02046-1
Original URL	https://doi.org/10.1038/s41550-023-02046-1
Source type	Journal
Keywords	Computer Science, Simulation, starship, physics, space
#Tags	Simulator, universe, model, nature
Summary of key points + notes (include methodology)	Cloudy is a "starship" made in 1978 to explore the Universe. The areas that Cloudy simulated changed over time to include things like the electromagnetic spectrum and several different events and circumstances. Cloudy has served to write several hundreds of papers per year, and with new technology, it will get better and will continue to serve as a simulation of the nature and the universe.
Research Question/Problem/ Need	What is cloudy and how can it help us understand more about the universe?
Important Figures	
VOCAB: (w/definition)	Quasar spectroscopy- analyzing of quasi(almost)-stellar radio sources
Cited references to follow up on	
Follow up Questions	Can Cloudy be implemented in research outside of astronomy, for example simulating marine biology on Earth or cell reactions in the human body to certain medications? How much can Cloudy be relied on given that it tries simulating environments based on current data? Can Cloudy be merged with other simulation tools or spacecraft to produce better simulations?

Article #7 Notes: Experimental validation of rotating detonation for rocket propulsion

Source Title	Experimental validation of rotating detonation for rocket propulsion
Source citation (APA Format)	Bennewitz, J W. et al. “Experimental validation of rotating detonation for rocket propulsion.” *Scientific Reports*, vol. 13, no. 1, Aug. 2023, p. 14204, https://doi.org/10.1038/s41598-023-40156-y.
Original URL	Experimental validation of rotating detonation for rocket propulsion | Scientific Reports (nature.com)
Source type	Journal Article
Keywords	Rotating detonation, combustion, supersonic, thrust
#Tags	New propulsion systems, rockets, rocket propulsion
Summary of key points + notes (include methodology)	As interplanetary travel becomes more and more popular, the need for more efficient propulsion systems increases. Great ideas have come out for rocket propulsion, one of which is rotating detonation. The researchers developed an engine capable of controlling the detonations in order to produce thrust. To do so, the engine transforms the chemical energy in the fuel into kinetic energy through a detonation combustion process. Why rotating detonation? - 10% increased thrust - Reduce thruster size/weight - Lower injection pressures - Less acoustic instabilities The engine excites multiple detonations that travel through the annular combustor. The strength and number of waves vary the engine performance Designed using instructions from Bykovskii et al. - 76mm long annulus

	- 5mm wide - Ultra high purity methane and oxygen - Fuel and oxidizer injection orifices inclined 30° - Fuel injection orifice has a diameter of 0.787mm - Oxidizer injection orifice has a diameter of 1.245mm Measurements: - Chamber pressure measured using CTAP sensors - Characterization of the acoustic field using two high frequency pressure transducers (in fuel and oxidizer plenum) - Horizontal thrust stand with 1100 load cell to measure thrust - Standardized imaging approach for characterization of operating mode across 4 research locations
Research Question/Problem/ Need	What kinds of propulsion systems are better than the current ones, and how efficient and usable are rotating detonation propulsion systems for future interplanetary travel?
Important Figures	John W. Bennewitz, Jason R. Burr, Blaine R. Bigler , Robert F. Burke , Aaron Lemcherf , Tyler Mundt, Taha Rezzag, EthanW. Plaehn, Jonathan Sosa, IanV. Walters, S.Alexander Schumaker, Kareem A.Ahmed, Carson D. Slabaugh, Carl Knowlen & William A. Hargus Jr.
VOCAB: (w/definition)	Rotating detonation- a form of rocket propulsion where the fuel are detonated (combusted and propagated faster than the speed of sound) in a rotating motion instead of back to back (this creates a continuous detonation)
Cited references to follow up on	doi: 10.2514/2.1156 doi: 10.2514/6.2021-3682 doi: 10.2514/3.28557
Follow up Questions	How much more efficient can we make detonation rotation propulsion systems? Are there more sustainable alternative propulsion systems? Could other fuels be used? How soon are we going to implement this type of propulsion system?

Article #8 Notes: Development of a Liquid-Propellant Rocket Powered by a Rotating Detonation Engine

Source Title	Development of a Liquid-Propellant Rocket Powered by a Rotating Detonation Engine
Source citation (APA Format)	Kawalec, M. et al. “Development of a Liquid-Propellant Rocket Powered by a Rotating Detonation Engine.” *Journal of Propulsion and Power*, vol. 39, no. 4, 2023, pp. 554–61, https://doi.org/10.2514/1.B38771.
Original URL	Development of a Liquid-Propellant Rocket Powered by a Rotating Detonation Engine | Journal of Propulsion and Power (aiaa.org)
Source type	Journal Article
Keywords	Rotating detonation, combustion, supersonic, thrust, liquid
#Tags	New propulsion systems, rockets, rocket propulsion
Summary of key points + notes (include methodology)	About 10 years ago, research was made to use liquid fuel for rocket engines. Doing so did not achieve stable continuously rotating detonation (CRD), or a guarantee of total combustion of the fuel in the detonation zone. To solve this, this research focuses on evaporating the fuel right before putting it in the detonation chamber of RDRE. In this research, nitrous oxide (N_2O) and propane (C_3H_8) were chosen because of their availability and because they are simple to handle and store. During the test, the researchers used “fast” pressure sensors to measure detonation pressure, “slow” pressure sensors to measure average pressure (combustion chamber and feeding lines), and a dynamometer to measure engine thrust Tests were made for three engine designs: annular combustion chamber with aerospike nozzle, disk shaped chamber with classical nozzle, and cone-shaped chamber with classical nozzle.

The cone shaped chamber with classical nozzle achieved the highest performance, so it was chosen to continue the research. (used “bard”, aka google’s AI to help me understand the tests because I thought there were some problems in the tests)

- Cone-shaped had better flow, smaller strain than disk-shaped classic nozzle.
- The annular combustion chamber had a simple slit nozzle without a divergent part, so the exhaust velocity was close to the sonic velocity and the specific impulse was relatively low. (refer to fig. 5)
- Calculations from the NASA CEA code provided that a mixture of $\Phi \approx 1.5$ is the most theoretically performant (measured by specific impulse) and was chosen for the RDRE for the rocket. (refer to fig. 5)
- (refer to fig. 5) Cone-shaped is closer to max performance, which means it is the most performant.

A cone -shaped RDRE with regenerative cooling was built and tested. Tests showed that regenerative cooling made the engine run successfully without evidence of burnout of the engine chamber or nozzle.

Regenerative cooling system:

- Keep the propellants liquid through calibrated orifices in supply lines before the engine
- Both propellants cooling the wall
- During this time, they are heated and evaporated (or partially)
- Injection in combustion chamber (as gas)

This particular architecture was designed and built to maintain the low weight and high efficiency of the propellant supply system.

Supply system:

- Two tanks (big one with N_2O, small one with C_3H_8)
- Tanks pressurized with helium, values selected to match the mixture composition during lab testing (ration gas to propellant liquid 5:1)

More test before launch:

- Fixed to wall and measured propulsion force (engine thrust minus rocket weight) using electronic dynamometer
- Full power 0.05 seconds after ignition

Launch:

- Successful
- Crashed on landing

<table>
<tr>
<td></td>
<td>

- Flight data lost, but estimated flight parameters accurately using flight time, engine operation time, flight range

</td>
</tr>
<tr>
<td>

Research Question/Problem/ Need

</td>
<td>

How to make a liquid propellant rocket powered by Rotating detonation stable continuous rotating detonation (CRD), or a guarantee of total combustion of the fuel in the detonation zone?

</td>
</tr>
<tr>
<td>

Important Figures

</td>
<td>

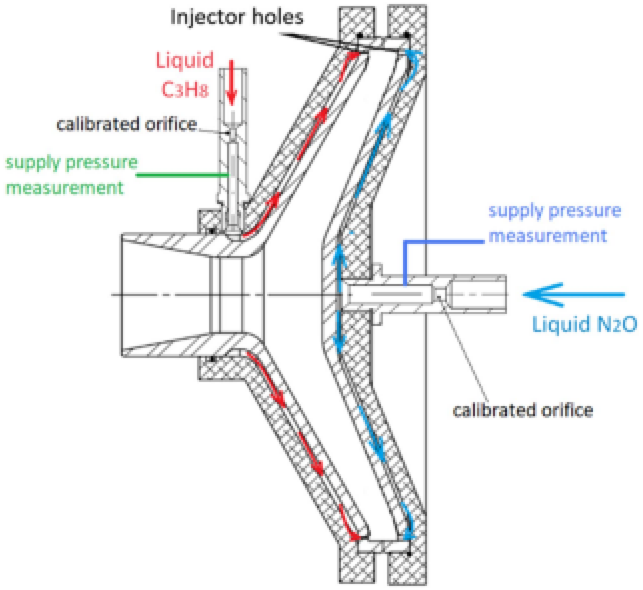


Fig. 4 Schematic of regenerative cooling system in conical combustion chamber. Supply pressure was measured only during tests in laboratory.

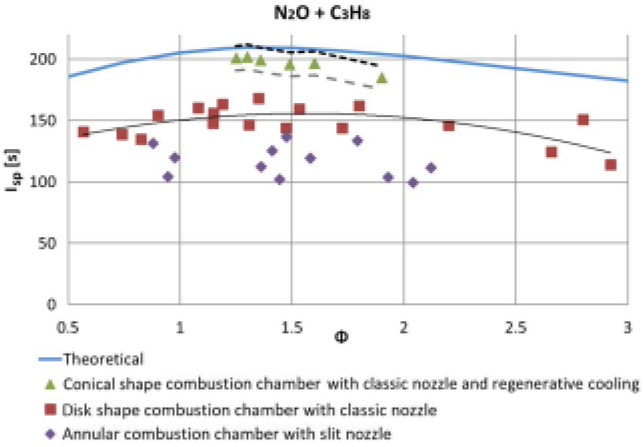
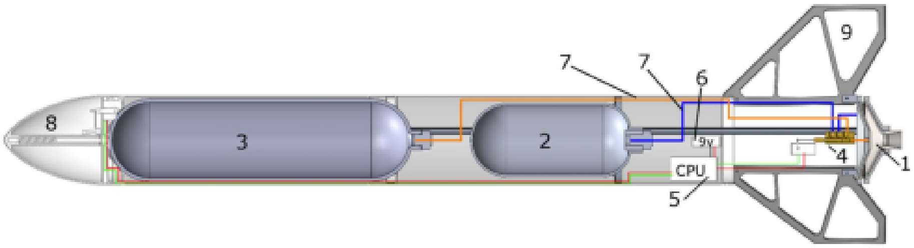
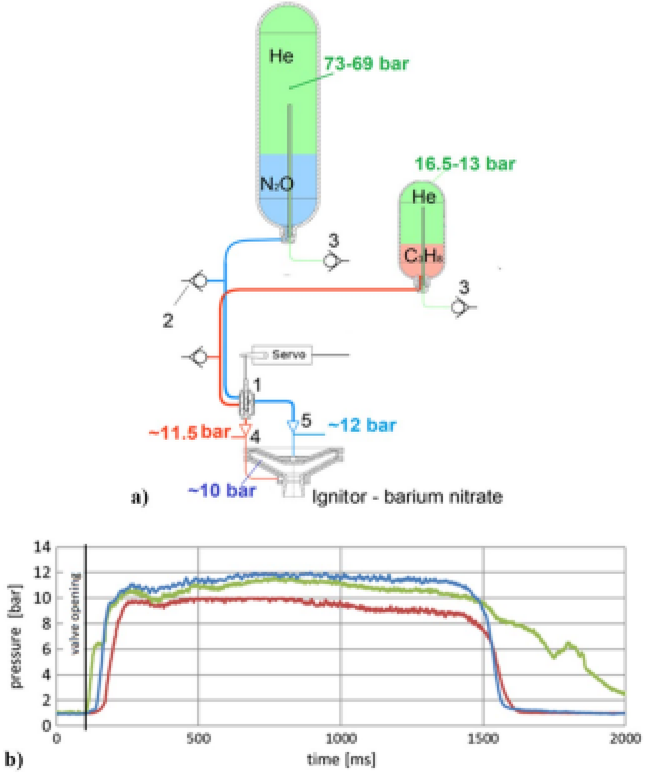


Fig. 5 Variation in the specific impulse in detonation chamber as function of mixture composition of N_2O and C_3H_8. Theoretical specific impulse calculated by NASA CEA code. Dashed lines indicate ±5% range of metering accuracy.

</td>
</tr>
</table>

	 **Fig. 6 Schematic diagram of the rocket structure.**  **Fig. 7 Figure 7a shows schematic diagram of rocket engine supply system. Figure 7b shows variation of supply pressure of nitrous oxide (blue line), propane (green line), and average pressure inside combustion chamber (red line) during laboratory test.**
VOCAB: (w/definition)	Rotating Detonation - Rocket propulsion system where the detonations alternate in a circle for constant propulsion
Cited references to follow up on	Vasil'ev, A. A., "Rotating Detonation: 'History, Results, Problems'," Transactions on Aerospace Research, Vol. 2020, No. 4, 2020, pp. 48–60. https://doi.org/10.2478/tar-2020-0020 [2] Wolański, P., "Detonative Propulsion," Proceedings of the Combustion Institute, Vol. 34, No. 1, 2013, pp. 125–158.

	[3] Xie, Q., Zifei, J., Haocheng, W., Zhaoxin, R., Wolański, P., and Bing, W., "Review on the Rotating Detonation Engine and Its Typical Problems," Transactions on Aerospace Research, Vol. 2020, No. 4, 2020, pp. 107–163. https://doi.org/10.2478/tar-2020-0024 [4] Bykovskii, F. A., Zhdan, S. A., and Vedemikov, E. F., "Continuous Spin Detonations," Journal of Propulsion and Power, Vol. 22, No. 6, 2006, pp. 1204–1216. https://doi.org/10.2514/1.17656 [5] Kailasanath, K., "Review of Propulsion Application of Detonation Waves," AIAA Journal, Vol. 38, No. 9, 2012, pp. 1698–1708. https://doi.org/10.2514/2.1156 [6] Eidelman, S., and Grossmann, W., "Pulsed Detonation Engine: Experimental and Theoretical Review," AIAA Paper 1992-3168, July 1992. [7] Wintenberger, E., and Shepherd, J. E., "Thermodynamic Cycle Analysis for Propagating Detonations," Journal of Propulsion and Power, Vol. 22, No. 3, 2006, pp. 694–698. https://doi.org/10.2514/1.12775 [8] Adamson, T. C., Jr., and Olsson, G. R., "Performance Analysis of a Rotating Detonation Wave Rocket Engine," Acta Astronautica, Vol. 13, No. 4, 1967, pp. 405–415. [9] Ferguson, D., O'Meara, B., Roy, A., Sidwell, T., and Johnson, K., "Experimental Measurements of NOx Emissions in a Rotating Detonation Engine," AIAA SciTech Forum 2020, AIAA Paper 2020-0204, 2020. https://doi.org/10.2514/6.2020-0204 [10] Tsuboi, N., Koichi, H.A., Yoshikazu, T., and Takashi, K., "Numerical Simulation of the Deflagration to Detonation Transition in a Tube with Repeated Obstacles: Experimental Scale Simulation Using the Artificial Thickened Flame Method," Transactions on Aerospace Research, Vol. 265, No. 4, 2021, pp. 41–52. https://doi.org/10.2478/tar-2021-0021
Follow up Questions	How much more efficient can we make detonation rotation propulsion systems? Are there more sustainable alternative propulsion systems? Could other fuels be used?

Article #9 Notes: Electrohydraulic thrust vector control of twin rocket engines with position feedback via angular transducers

Source Title	Electrohydraulic thrust vector control of twin rocket engines with position feedback via angular transducers
Source citation (APA Format)	Lazić, Dragan V., and Milan R. Ristanović. "Electrohydraulic thrust vector control of twin rocket engines with position feedback via angular transducers." *Control Engineering Practice*, vol. 15, no. 5, 2007, pp. 583–94, https://doi.org/10.1016/j.conengprac.2006.10.015.
Original URL	https://linkinghub.elsevier.com/retrieve/pii/S096706610600195X
Source type	Journal Article
Keywords	Thrust vector control, Gimbal nozzle, Electrohydraulic servo system, Servoactuator, Servovalve, Angular transducer
#Tags	Thrust vectoring, rocket propulsion, rockets, thrust
Summary of key points + notes (include methodology)	Aerodynamics are used to decide the trajectory of rockets, but those systems stop working when higher speeds and altitudes come in and are inefficient for agility. This is where Thrust Vector Control comes in. In the past, actuators to gimbal the engine were hydraulic, but research has been done towards electromechanical actuators for replacing hydraulic actuators. Nothing has been done for thrust vector control. Final goal for servo actuators is minimizing size and weight. To control direction, gimbal angles are used. With those, imperfections in the mechanism are considered modeling errors. Thrust Vectoring System: ● Two nozzle engines mounted on frames ● They tilt the gimbal joint ● Each nozzle engine has 2 hydraulic servo actuators

- Servo Actuators give force and control for the gimbal for the nozzle and TVC
- Direction of TV controlled by autopilot
- Servoactuator controlled electro hydraulic servo valve
- Servo valve chosen because availability in industrial market

Analysis:

- Done on only one engine because of symmetry between the two

Testing:

- Servoactuators were put on the body frame
- Cylinder pistons on the gimbal frame
- Measured angale rotations using AT a and b
- Servoactuator and pistons moved to move the gimbal frame, which controlled thrust vector to attain specific direction

Measurements:

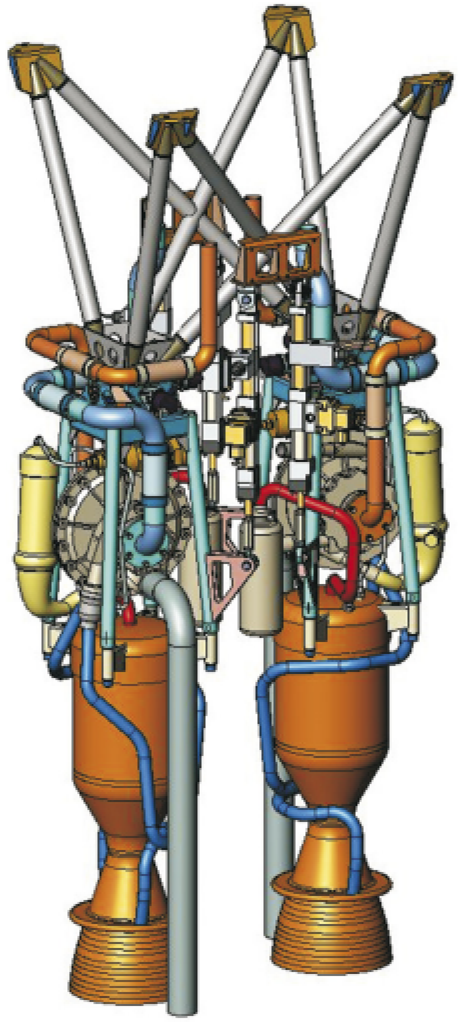
- Incremental encoders (HEIDENHEIN ROD 1020 with resolution of 3600 pulses per revolution) used to measure angle of gimbal frame rotation
- Onboard computer with 2 digital signal processing receives this info
- One DSP for angle measurement
- Other for control algorithm
- Equipped with digital to analog converter
    - 4
    - Converts 2:5V
    - 4-times amplified to go with servo valve amplifier box - V input 10V

Power supply:

- TVC operate dually
    - Hydraulic pump for continuous testing with hydraulic accumulator
    - Hydraulic accumulator filters pressure pulsations (coming from pump), gives more fluid to manage peak flow
- Cylindrical hydraulic accumulator designed for specific amount of oil for stand-alone application. Oil pressure mainainted through pressurized nitrogen.
- Hydraulic pump to fill hydraulic accumulator only once.

Conclusion:

- TVC of twin nozzle
- Solving kinematics problem of TVC with measurement of gimbal angles.
- Position transducers not included in final design of servo actuators
- Position feedback given indirectly

	● All signals digital for reliability, but not analog control voltage toward servovalves
Research Question/Problem/Need	Using/testing electromechanical actuators for control thrust vectoring (thrust direction) on a rocket
Important Figures	 Fig. 1. TVC system. Image of the dual thrust vector control system
VOCAB: (w/definition)	Gimbal: a mechanism, typically consisting of rings pivoted at right angles, for keeping an instrument such as a compass or chronometer horizontal in a moving vessel or aircraft
Cited references to follow up on	Buschek, H. (2003). Design and flight test of a robust autopilot for the IRIS-T air-to-air missile. Control Engineering Practice, 11(5), 551–558.

	Lazic´, D. V., & Ristanovic´, M. R. (2004). Thrust vector control of twin nozzle engine. Proceedings of the VIII triennial international SAUM conference (pp. 94–97). Belgrade, Serbia, November 2004. Meritt, H. E. (1967). Hydraulic control systems. New York: Wiley. Schinstock, D. E., Douglas, S. A., & Haskew, T. A. (1997). Identification of continuous-time, linear, and nonlinear models of an electromechanical actuator. Journal of Propulsion and Power, 13(5), 683–690. Schinstock, D. E., Douglas, S. A., & Haskew, T. A. (1998). Modeling and estimation for electromechanical thrust vector control of rocket engines. Journal of Propulsion and Power, 14(4), 440–446. Schinstock, D. E., & Haskew, T. A. (2001). Transient force reduction in electromechanical actuators for thrust-vector control. Journal of Propulsion and Power, 17(1), 65–72. Skogestad, S., & Postlethwaite, I. (1996). Multivariabile feedback control. England: Wiley. Song, C., Kim, S. J., & Kim, S. H. (2006). Robust control of the missile attitude based on quaternion feedback. Control Engineering Practice, 14(7), 811–818. Zipfel, P. H. (2000). Modeling and simulation of aerospace vehicle dynamics. Reston, VA: American Institute of Aeronautics and Astronautics, Inc.
Follow up Questions	Why were positional transducers omitted from the final design? Wouldn’t they give position feedback directly which would be more precise than indirectly?

Article #10 Notes: Arduino Integrated Portable RFID Bicycle Lock

Source Title	Arduino Integrated Portable RFID Bicycle Lock
Source citation (APA Format)	Lewallen, J. *Arduino Integrated RFID Bicycle Lock*. 10 Oct. 2017, https://oaktrust.library.tamu.edu/handle/1969.1/164491.
Original URL	https://oaktrust.library.tamu.edu/handle/1969.1/164491
Source type	Research Article
Keywords	Wireless RFID Bicycle Lock Arduino
#Tags	Bicycle lock, security, electric lock, bicycle, bicycle safety
Summary of key points + notes (include methodology)	This study used current tools and technology to make a bicycle lock that is easier to unlock without obstacles, such as mechanics in current locks, but also to record information to retrieve the bicycle if it is still stolen. It was done because although there are great locks, it can be complicated to insert the key into the hole while the bike rack is full. An electronic bike lock with RFID would make the entire experience safe and more efficient. It could also help if bicycle is stolen by recording date when it was broken to help the police (cameras) **Methods** **RFID Reader** ● RFID reader focusing on 3 things (constraints): size, range, power ○ should not exceed a maximum area of 8-10 square centimeters ○ Greater range = greater experience, so 100mm range-optimal ○ Power consumption under 2-5V/50mA ● Considerer ID-2LA ○ Small size ○ Allow for specific placement of reader and antenna to optimize signal strength ● Considered ID-12LA ○ Greater signal read range

Used ID-12LA because of larger read range

Battery Composition and Implementation

Constraints

- Battery for ID-12LA should not exceed a 5V limit.
- Use battery available to average person
- Should consider other V source above and below 5V for current and reliability limitations

Regulation

A voltage regulator is a component specifically designed to maintain a consistent voltage level.

Considered two types:

1. Linear regulator. Uses active (ex. Bipolar Junction Transistor) device controlled by a large-gain differential amplifier. Adjusts allowable voltage to keep it constant by comparing output with reference voltage
    a. power dissipation is directly proportional to its output current.
    b. As a result, efficiency around 50% (almost half energy converted to waste heat)
    c. Advantage of low noise at output
2. Switching regulator converts a DC input voltage to switched voltage (applied to BJT of MOSFET switch). Switched output V filtered and brought back to circuit controlling power switch to keep V constant no matter input V and load current
    a. Able to reach peak efficiency of around 90%
    b. Able to drive higher current loads
    c. Output noise much higher

Priority given to:

1. ID-Innovations ID-12LA RFID Card Reader datasheet states that a linear regulator is the ideal power supply for the reader to work properly
2. Primary locking mechanism operates a Zon Hen OpenFrame solenoid: requires large current draw in short time
3. Bike lock should be long-lasting, so efficient power regulator.

With all this, switching regulator chosen for design

Determine whether the regulator should increase or decrease voltage:

- high current draw important
- power efficiency important

Therefore, a CUI Inc. V7805-1500 step-down switching regulator for Vs over 6.5V with 1.5V output (with a typical switching frequency of 340 kHz) selected for design.

Battery Saving

Inefficient to regulate the power when the device is only used a couple times a day.

Used mechanical power slide-switch to fix

Slide switch:

- Operate under less current draw than conventional power button

- Not as convenient though
- Not as esthetic
- Consumer might forget to turn off

Simple power (push) button

- Produce false open/close transitions when pressed because of mechanical issues
- Results in software always checking if button is pressed
- Automatically off unless if pressed on

Additional programming in Arduino done to accommodate for consumer forgetting to turn off.

Test results showed that the average unlock time per trial (power ON stage to LOCK stage) was 10 seconds.
With more Arduino code, the program system goes to sleep mode after 25 seconds, thus conserving battery power, unless if turned off manually by consumer (better option, shuts off Arduino completely to wait for next time it needs to be used and it is turned on)

Dead battery replacement
direct key access
moving bar concept

Solenoid- Key locking mechanism
Solenoid used for primary locking mechanism

- Rod (armature)
- Coil of wire around rod

Current goes through wire, and the rod closes the air gap between cores, which increases flux linkage. Also spring loaded (in this case) to retract when current isn't flowing
Benefits of solenoid:

- Speed (fast locking/unlocking mechanism)
- No mechanical moving parts (odds of breaking are small)

Since solenoids can't change current instantly, so Schottky diode as a flyback diode applied to the system to prevent voltage spike from occurring causing arcing on switch contacts or destroying switching transistors.

RFID tag
Lock will come packaged with 125kHz mastercard (only card that can act in this way because of special program on it)

- Used to unlock bicycle
- Used "write" new card to unlock the bicycle

Visuals
LED in the design for visual feedback (indication of state of the lock):

- Blue = power/standby state

	● Green = unlock state ● Red= denial state ● Flashing RGB = “Write” mode **Battery life-time** 2 testing iterations: 1. Household 9V alkaline battery a. Over 110-minutes b. Calculated to have to replace battery every 220 days (assuming 2 uses of the device per day) 2. Energizer Lithium Ion 9V battery a. Ove 130 minutes b. Calculated to have to replace every 260 days **Materials** Security and rigidity needed: ● Majority produced from hardened steel ● Plastic sleeve for wireless RFID sensor **Conclusion** By adding wireless innovations, this bicycle lock can be unlocked wirelessly using a scanning tag, but also traditionally (lock and key). There is also a card-syncing option for the user to scan already existing RFID tags to reduce the number of tags the user has to carry. During testing, the battery life-time of the lock was about 220 days. This product can be extended to several technologies, such as bluetooth compatibility to connect to a smartphone, for distant unlocking, and tracking The researchers managed to make a convenient method for securely locking and accessing a bicycle by using only pre-existing technologies.
Research Question/Problem/ Need	Unlocking a bicycle with a key is extremely hard, especially when the bike rack is full of other bicycles and other obstacles.
Important Figures	

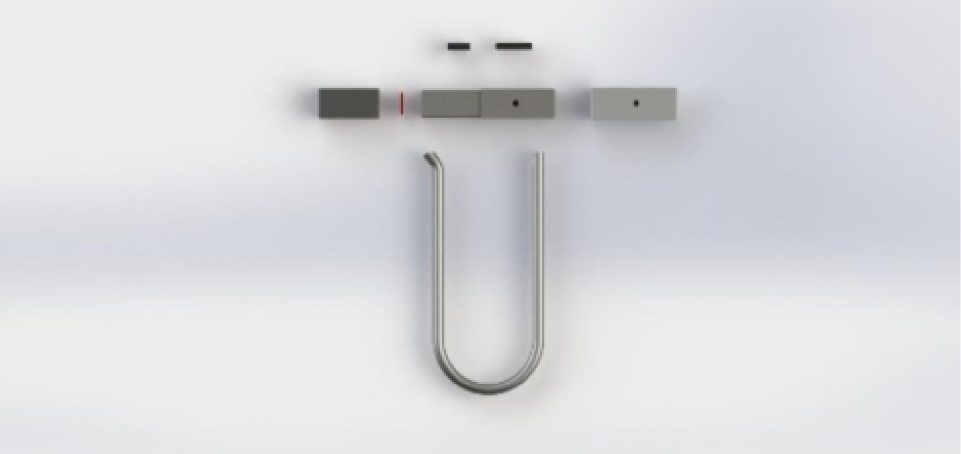


Figure #9. Three sleeve design demonstration.

Image of all the component disassembled

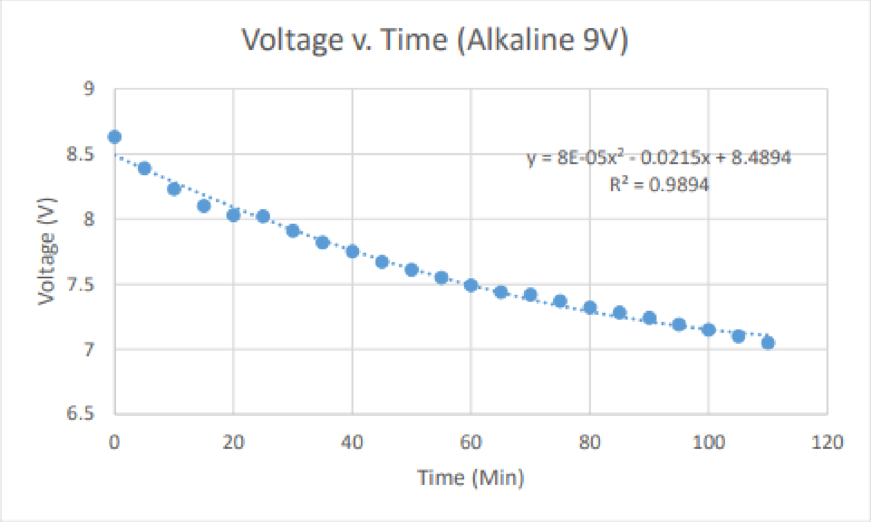
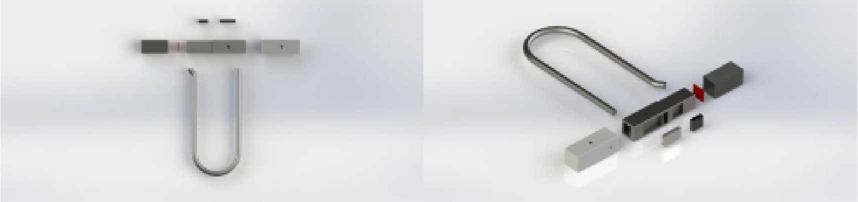
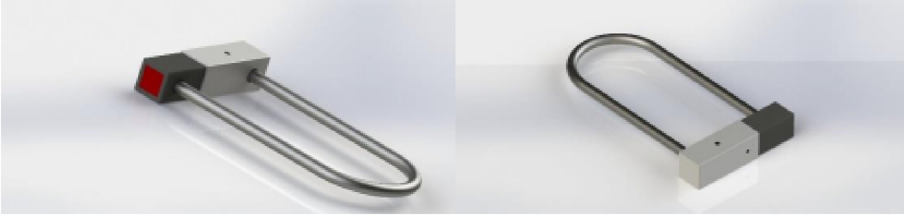


Chart 1. Duracell 9V alkaline battery voltage v. time test results. 120 minute test period.

Graph of the voltage over time results for the 9V alkaline battery

	 Figure #12. Exploded-view renders featuring component placement Image of the components of the lock disassembled  Figure #13. Side and top views of the preliminary lock design Image of the lock assembled
VOCAB: (w/definition)	**RFID:** radio-frequency identification **Solenoid:** a cylindrical coil of wire acting as a magnet when carrying electric current **Voltage regulator:** thing that keeps constant voltage
Cited references to follow up on	M. Morris, 'City to convert lane of downtown street to bike path', Houston Chronicle, 2014 [Online]. Available: http://www.houstonchronicle.com/news/houston-texas/houston/article/Cityto-convert-lane-of-downtown-street-to-bike-5714260.php. [Accessed: 06- Sep- 2015] G. Kulkami, R. Shelke, R. Sutar and S. Mohite, 'RFID security issues & challenges', in 2014 International Conference on Electronics and Communication Systems, 2014, pp. 1-4. T. Hollstein, M. Glesner, U. Waldmann, H. Birkholz and K. Sohr, 'Security challenges for RFID key applications', in 3rd European Workshop on RFID Systems and Technologies, 2007, pp. 1-12. "National Bike Registry - Bicycle Thefts Are up 10%!" National Bike Registry - Bicycle Thefts Are up 10%! Web. 25 Aug. 2015. . C. Floerkemeier and S. Sarma, 'An overview of RFID system interfaces and reader

	protocols', in IEEE International Conference on RFID, 2008, pp. 232-240. J. Muller, M. Schapranow, C. Popke, M. Urbat, A. Zeier and H. Plattner, 'Best practices for rigorous evaluations of RFID software components', in European Workshop on Smart Objects: System, Technologies and Applications (RFID Sys Tech), 2010, pp. 1-10
Follow up Questions	Wouldn’t this kind of system not completely solve the problem? Sure, it helps with unlocking the lock, but the user still needs to get the lock and remove it from the bike rack. Also, the user manually attaches the lock.

Article #11 Notes: IoT-Enabled Smart Bike Helmet with an AI-Driven Collision Avoidance System

Source Title	IoT-Enabled Smart Bike Helmet with an AI-Driven Collision Avoidance System
Source citation (APA Format)	Solus, J., Rakotondraibe, M., Yu, X., Yi, W.-J., Gromov, M., & Saniie, J. (2023). IoT-Enabled Smart Bike Helmet with an AI-Driven Collision Avoidance System. 2023 IEEE International Conference on Electro Information Technology (EIT), 175–179. https://doi.org/10.1109/eIT57321.2023.10187299
Original URL	IoT-Enabled Smart Bike Helmet with an AI-Driven Collision Avoidance System | IEEE Conference Publication | IEEE Xplore (wpi.edu)
Source type	Conference Paper
Keywords	Computer Vision, Artificial Intelligence, Deep Learning, Edge Computing, Internet of Things, Bicycle Safety
#Tags	Bicycle, Bicycle Safety, Arduino
Summary of key points + notes (include methodology)	Although there is an increase in bicycle riders around the world, bicycle accidents, which are sometimes fatal, happen often. In the US per year ● 130 000 injuries ● 1 000 fatalities The design in this study has several components to send and receive data via Bluetooth in order to prevent bicycle riders from getting into accidents. The helmet: ● detects collisions (accelerometer and ultrasonic sensor) ● sends GPS-located messages to emergency contacts following crashes ● deploys an airbag for the crash. ● GPS system also warns users of unsafe drivers ● Barometer for atmospheric shifts to warn for rain ● AI algorithm with a camera on the back of the helmet to detect danger situations outside of the rider's view Research has been done in the past for improving bike helmets: ● Theft protection features ● Detect alcohol before the rider starts riding ● RFID-based security to only start the bike if the helmet is nearby ● Accident avoidance systems to warn users of possible dangers ● GPS systems to send messages to hospitals when accidents have occurred In all of these bike helmets, not many use safety features with the latest advancements in technology.

AI recognition inspired by previous works, but takes a step farther with distance recognition to insure that the helmet only reports dangers that are close to the rider.

Design contains 3 main components (fig. 1):

- **Smart Sensor/Actuator Node (SSAN)**
    - Driven by Arduino Uno
    - Wireless communication through the system are through an HC-06 Bluetooth module connected to Arduino
    - Detection of a collision using an ADXL345 accelerometer and HC-SR04 ultrasonic sensor
    - Simulation of airbag deployment with LED
    - Detection of atmospheric pressure changes indicating rain done through a BMP180 barometer
    - GPS data collected via Neo-6M GPS receiver
    - Two buttons on the helmet:
        - **1.** Allows rider to cancel the sending of the email to emergency contacts (tell the system they are safe)
        - **2.** Alert other riders of the danger.A BMP180 barometer detects changes in atmospheric pressure that could indicate the possibility of future unanticipated rain
    - All sensor node components are connected via pin wiring.
    - SSAN collects data from each sensor and responds accordingly (fig. 2)
- **Vision Node**
    - NVIDIA Jetson Nano with a built-in 128-core GPU with a 10W power consumption rate.
    - Jetson Nano equipped with an IMX 219 8MP camera and an Intel 8265 WiFi/Bluetooth adapter.
- **Backend web server**
    - ThingSpeak web server
    - accessed with a Python script on the Jetson Nano that sends data through HTTP web socket connection.
- Whole system is powered with a 24 000 mAh capacity power source which is portable and rechargeable. A battery with less capacity could be used to improve cost and minimize weight

AI divided into 2 parts:

1. **Analyzing a dangerous situation**
    a. Detects an object
    b. Classifies the object
    c. Determines if it falls in the predefined “dangerous” category

Performance of several DNN evaluated with Jetson Nano camera. (Tested on live elements [in the street] instead of static images to make sure it detects appropriately with the right environment

The DNN

- Detects the “class” of an object with its confidence level
- If it is high enough (can be changed by the user) it will indicate a threat

Testing DNNs:

- 50 live samples for each
- ½ were cars, ½ were not automobiles
- Results in table 1

2. **Defining if the situation is approaching the user, and will potentially harm them**
   After Step 1, finding an object, the researchers created an algorithm analyze each frame to evaluate the distance/collision point
   To prevent the AI analyzing parked objects and things on sidewalks as threats, a threat zone was defined cutting off parking spots and sidewalks (shown in figure 3)
   - After determining a threat in the threat zone, the AI determines its size and whether its direction (getting smaller means going away from the rider, while getting bigger means getting closer)
   - Used OpenCV to determine threats the bounding boxes of the threat and its status
   - If the object is a threat, they used OpenCV to draw a box around it
   - If all the criteria are met, a signal is sent to the SSAN to alert the rider.

   The researchers considered adding other OpenCV features but it would have led to poor performance that would diminish the ability to send a warning message on time to the rider.

Testing

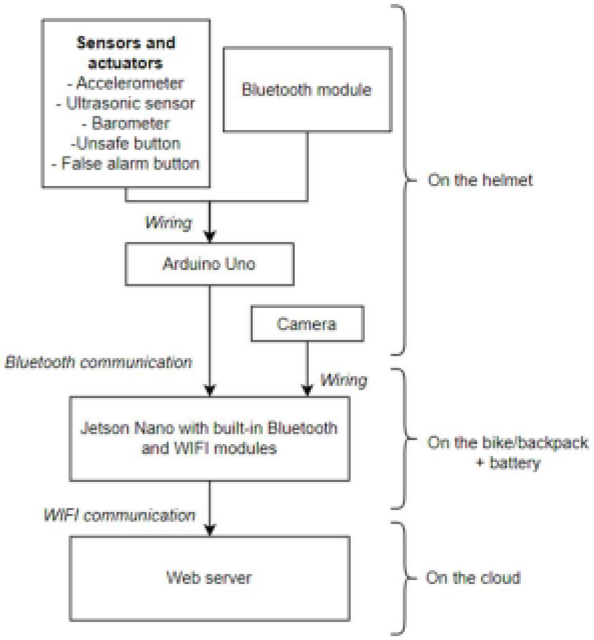
- They made a live demonstration of a rider wearing the helmet getting into a crash and falling to the ground. The system worked as intended

DNN selection

- They eliminated networks with average FPS less than 20 because a higher FPS is needed to detect fast-moving objects
- Eliminated networks without the ability of positional coordinates because the coordinates are an important part of the distance/collision module
- After all those eliminations, they chose the model with the highest average confidence levels on successful prediction and lowest average confidence level on false outputs.
- SSD-mobilenet-v2 selected because of the considerations above
- Research has proved that Yolo v3 has better image recognition accuracy than the one chosen, but the researchers also found computational performance laking

Distance/Collision Evaluation Test

- Brought the device to a busy street
- Analyzed what the vision node determined as object
- It determined everything that needed to be
- Boxed in green what were not threats and boxed threats in red

	User - Can view data from the rides through the ThingSpeak web server - The GPS data can also be viewed on a map thanks to a MATLAB script (made by the researchers) **Conclusion** ● Made a helmet safety system ● Could be improved by replacing the Jetson Nano to a smartphone with the capabilities of running collision evaluation algorithms and integrating an SSAN to the smartphone app.
Research Question/Problem/ Need	There are more and more bicycle riders around the world, and bicycle accidents are not decreasing. How can a bicycle ride become safe for the rider and other riders around him.
Important Figures	 Sensors and actuators - Accelerometer - Ultrasonic sensor - Barometer -Unsafe button - False alarm button Bluetooth module Wiring Arduino Uno Camera On the helmet Bluetooth communication Wiring Jetson Nano with built-in Bluetooth and WIFI modules On the bike/backpack + battery WIFI communication Web server On the cloud Fig. 1. System Flowchart of Smart Bike Helmet **Different parts of the system and where they are located in the design**

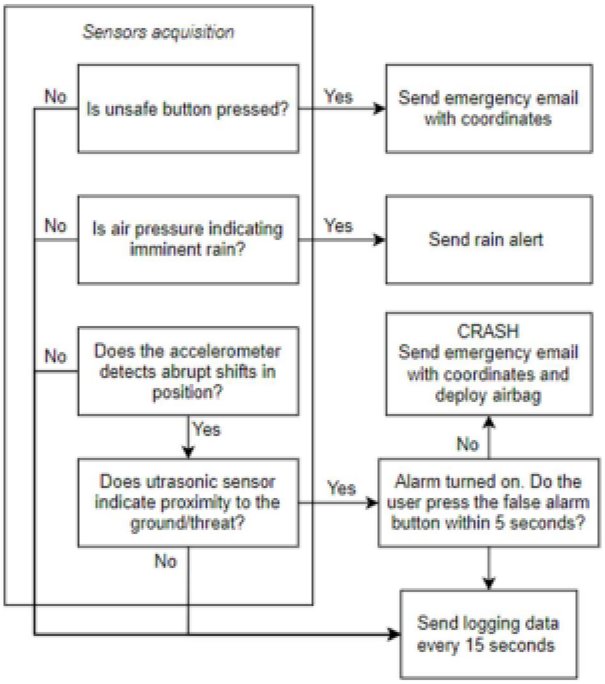
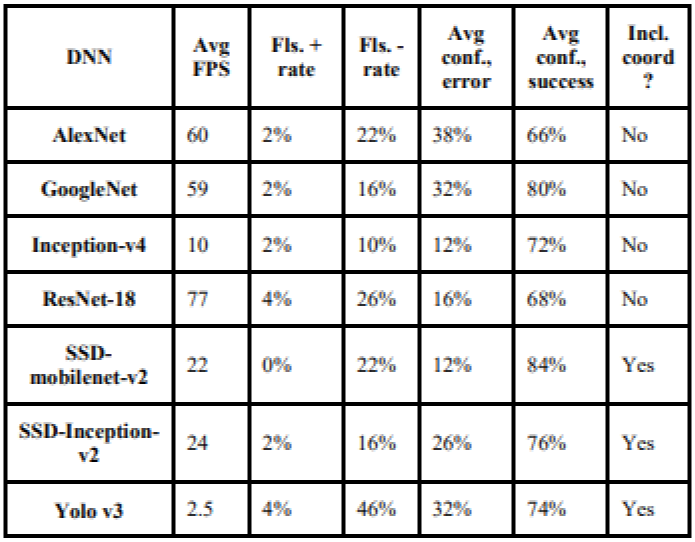

Sensors acquisition
Is unsafe button pressed?
Yes
Send emergency email with coordinates
No
Is air pressure indicating imminent rain?
Yes
Send rain alert
No
Does the accelerometer detects abrupt shifts in position?
No
Yes
CRASH Send emergency email with coordinates and deploy airbag
No
Does utrasonic sensor indicate proximity to the ground/threat?
Yes
Alarm turned on. Do the user press the false alarm button within 5 seconds?
No
Send logging data every 15 seconds

Fig. 2. Operation Flowchart for SSAN

The conditional statements and responses for each sensor and their input

TABLE I. DNN PERFORMANCE COMPARISON



DNN	Avg FPS	Fls. + rate	Fls. - rate	Avg conf., error	Avg conf., success	Incl. coord ?
AlexNet	60	2%	22%	38%	66%	No
GoogleNet	59	2%	16%	32%	80%	No
Inception-v4	10	2%	10%	12%	72%	No
ResNet-18	77	4%	26%	16%	68%	No
SSD-mobilenet-v2	22	0%	22%	12%	84%	Yes
SSD-Inception-v2	24	2%	16%	26%	76%	Yes
Yolo v3	2.5	4%	46%	32%	74%	Yes

Table of the different DNSs tested with their average frames per second (which can be used to find out processing speed), false positive and negative rate (percentage of positive/negative situations determined incorrectly), average confidence levels, and if they included coordinates

(where in the image the object was in)

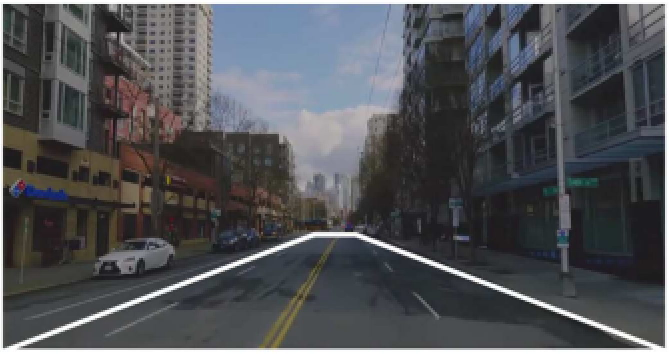


Fig. 3. Evaluated Threat Zone for Distance/Collision Evaluation

Area evaluated as the "threat zone" to prevent the AI from finding things (like pedestrians and parked cars) outside of this area as a threat

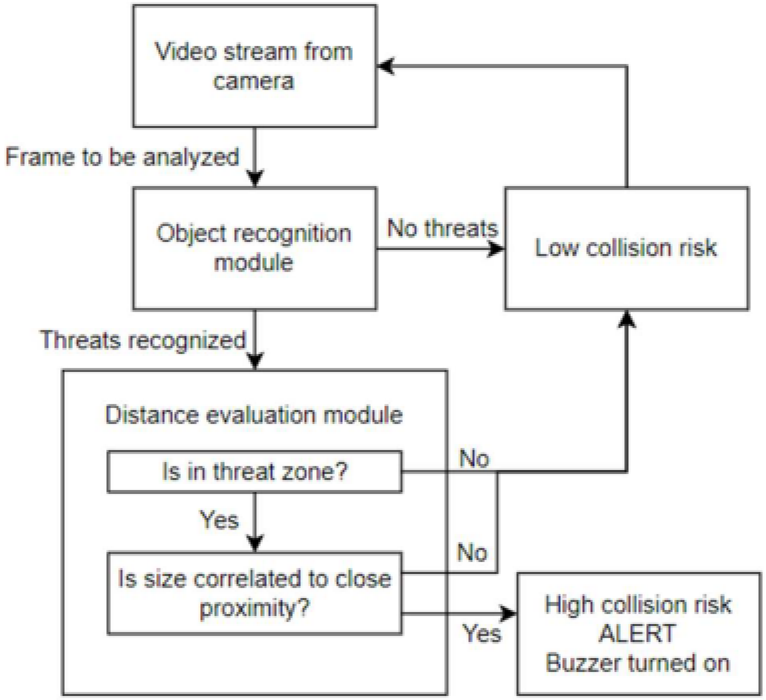

Video stream from camera
Frame to be analyzed
Object recognition module
No threats
Low collision risk
Threats recognized
Distance evaluation module
Is in threat zone?
No
Yes
No
Is size correlated to close proximity?
Yes
High collision risk ALERT Buzzer turned on

Fig. 4. Operation Flowchart for Vision Node

Operation flowchart for the vision part of the system. All the steps that go on over and over before a signal is sent or not

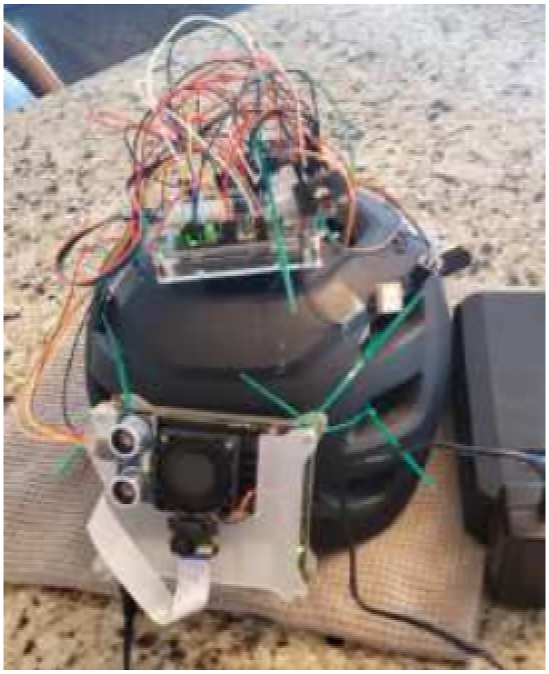


Fig. 5 Picture of Implemented Smart Bike Helmet

Picture of the design they built

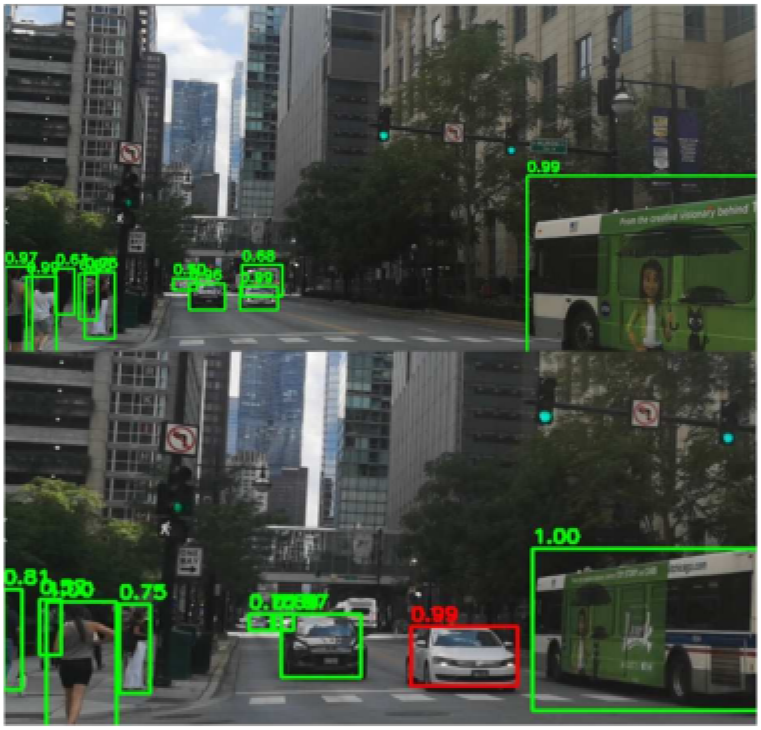


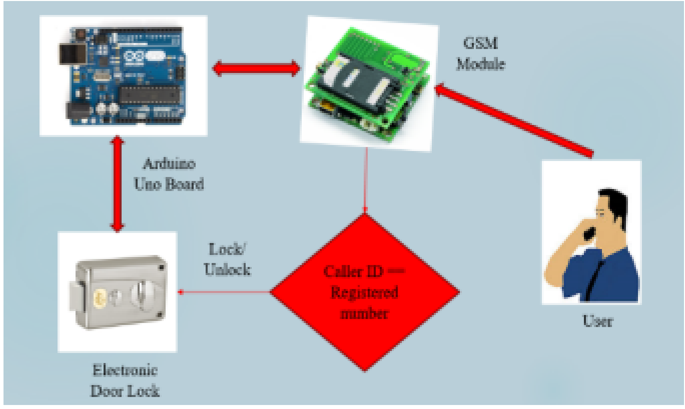
Fig. 6 Output from Distance/Collision Evaluation

	Example of what the vision node would see and output
VOCAB: (w/definition)	Node: a component in a distributed network (Google Bard) Backend web server: portion of a website or program invisible to the user, which is usually operated separately (on another computer) DNN: Deep Neural Network/artificial neural network that uses several different nodes or parts to it to process and learn from data
Cited references to follow up on	Centers for Disease Control and Prevention Web-based Injury Statistics Query and Reporting System (WISQARS). [online] P. C, R. C, P. N. M, R. P. S and S. M, "Smart Bike Helmet with Vehicle Tracking System using Arduino," 2022 International Conference on Edge Computing and Applications (ICECAA), Tamilnadu, India, 2022, pp. 579-582, doi: 10.1109/ICECAA55415.2022.9936590. D. K. P. Gudavalli, B. S. Rani and C. V. Sagar, "Helmet operated smart E-bike," 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Srivilliputtur, India, 2017, pp. 1-5, doi: 10.1109/ITCOSP.2017.8303138. N. Nataraja, K. S. Mamatha, Keshavamurthy and Shivashankar, "SMART HELMET," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 2338-2341, doi: 10.1109/RTEICT42901.2018.9012338. A. Jesudoss, R. Vybhavi and B. Anusha, "Design of Smart Helmet for Accident Avoidance," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0774-0778, doi: 10.1109/ICCSP.2019.8698000. S. Chavan, J. Ford, X. Yu and J. Saniie, "Plant Species Image Recognition using Artificial Intelligence on Jetson Nano Computational Platform," 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 2021, pp. 350-354, doi: 10.1109/EIT51626.2021.9491893. N. Awalgaonkar, P. Bartakke and R. Chaugule, "Automatic License Plate Recognition System Using SSD," 2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA), Goa, India, 2021, pp. 394-399, doi: 10.1109/IRIA53009.2021.9588707. F. K. Noble, "Comparison of OpenCV's feature detectors and feature matchers," 2016 23rd International Conference on Mechatronics and Machine Vision in Practice (M2VIP), Nanjing, China, 2016, pp. 1-6, doi: 10.1109/M2VIP.2016.7827292. A. C. Rios, D. H. dos Reis, R. M. da Silva, M. A. de Souza Leite Cuadros and D. F. T. Gamarra, "Comparison of the YOLOv3 and SSD MobileNet v2 Algorithms for

	Identifying Objects in Images from an Indoor Robotics Dataset," 2021 14th IEEE International Conference on Industry Applications (INDUSCON), São Paulo, Brazil, 2021, pp. 96-101, doi: 10.1109/INDUSCON51756.2021.9529585.
Follow up Questions	How could this project get a safety approval for the helmet? Could this project be combined with the RFID helmet to make sure the rider is wearing this helmet while riding? Does the airbag deploy in the helmet, or around the entire body starting from the helmet?

Article #12 Notes: Smart Lock Controlled using Voice Call

Source Title	Smart Lock Controlled using Voice Call
Source citation (APA Format)	Raju, N. G., Vikas, J., Appaji, S., & Hanuman, A. S. (2018). Smart Lock Controlled using Voice Call. *IEEE International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 97–103. https://doi.org/10.1109/ICSSIT.2018.8748770
Original URL	Smart Lock Controlled using Voice Call | IEEE Conference Publication | IEEE Xplore (wpi.edu)
Source type	Conference Paper
Keywords	Arduino UNO, GSM module, Servo, Smart Lock System
#Tags	Arduino, Smart Lock, Lock
Summary of key points + notes (include methodology)	Smart lock system using voice call Person calls, system verifies the caller ID. If it is valid, the lock will lock/unlock depending on its current state. If it is invalid, the lock will send an alert to all contacts The goal of the project was to develop a smart lock to reduce the heavy and numerous components, while making it easier to use. Mobile phones are everywhere nowadays, so it was chosen as the way to control the system Components: - Arduino Uno as the microcontroller - GSM SIM900A module as the communication controller - MG90S Servo motor for gear control Algorithm: - Check caller ID - If valid - Check lock status - If locked - Unlock the door - If unlocked - Lock the door - If invalid - Send an alert to the owners

	Results ● The system offers greater range ● Ease of use ● Removes the requirement of smartphone ● Eliminates the need for bluetooth or internet Future works ● detect physical attempts to trespass the system ● provide power back up in case of power failure ● keep a check on battery levels to back up necessary records for safety reasons
Research Question/Problem/ Need	The need for smart locks is continuously increasing and the smart locks that are currently on the market require a smartphone, bluetooth or wifi connectivity, and cannot be used for long ranges
Important Figures	 GSM Module Arduino Uno Board Lock/ Unlock Caller ID == Registered number User Electronic Door Lock Graphical abstract of the components of the system and how they work together

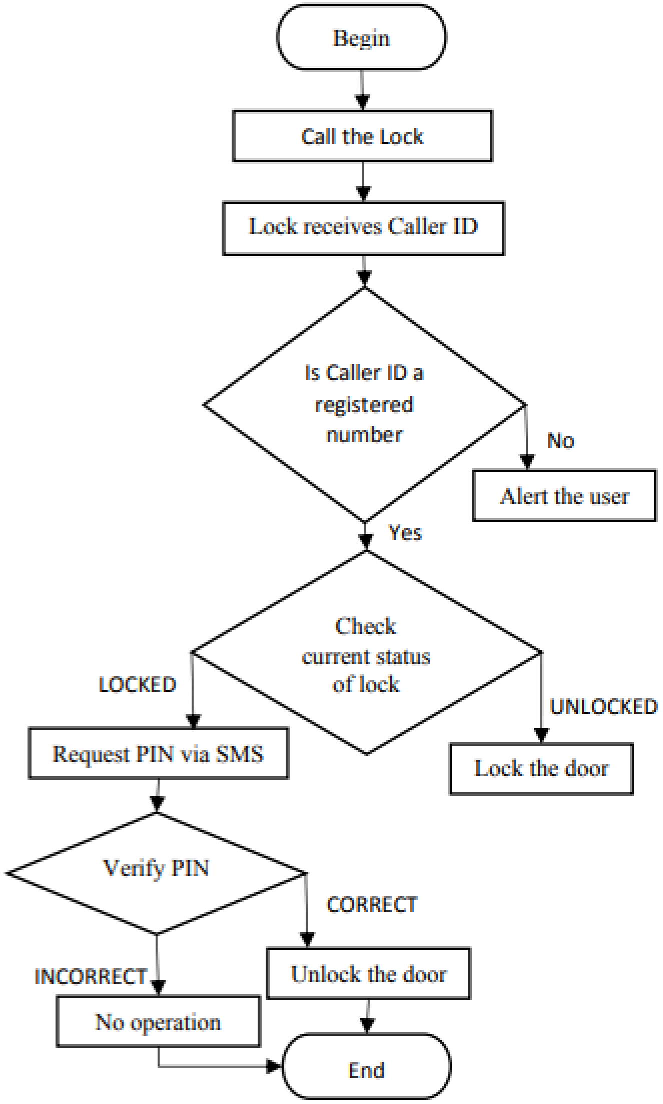
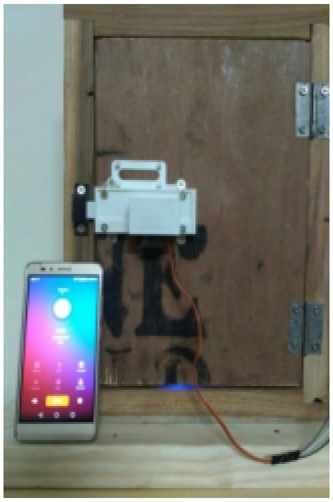


Figure 2. Flowchart of Proposed System

Flowchart of the algorithm and how it would work (what it checks & its response)

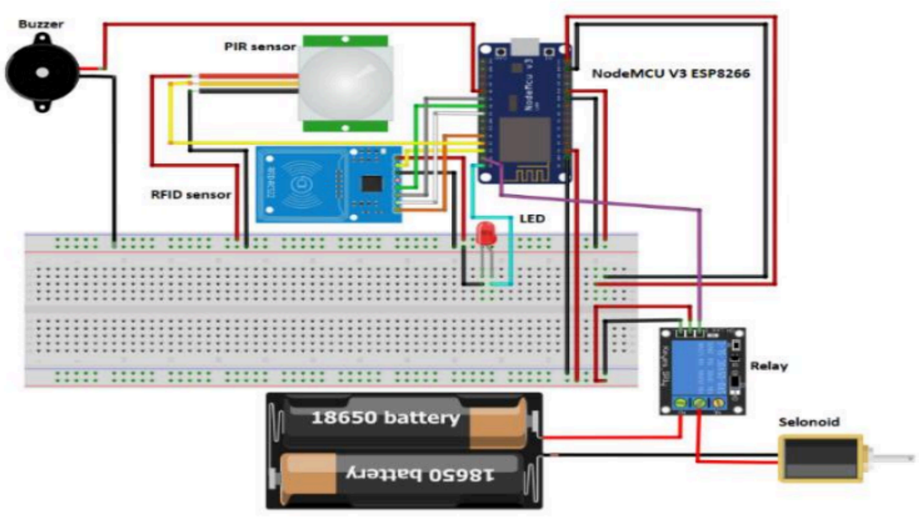
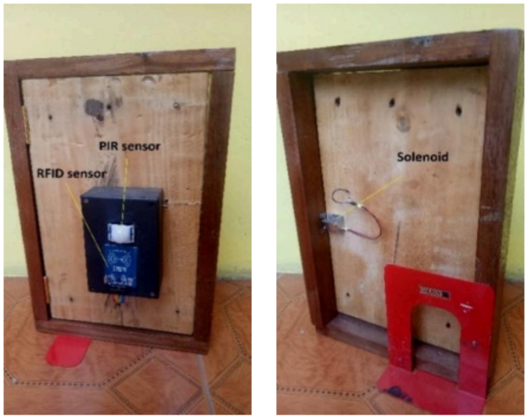
	 Image of the system prototype
VOCAB: (w/definition)	GSM - Global system for mobile communication → a widely used mobile network
Cited references to follow up on	Abdallah Kassem, Sami El Murr, Georges Jamous, Elie Saad, Marybelle Geagea – "A Smart Lock Using Wi-Fi Security", 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA), Beirut, Lebanon, 2016, PP.222- 225 Meera Mathew, R S Divya – "Super Secure Door Lock System for Critical Zones", International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvanthapuram, India, 2017, PP.242-245 Anuradha.R.S, Bharathi.R, Karthika.K, Krithika.S, S.Venkatasubramanian – "Optimized Door Locking and Unlocking using IoT for Physically Challenged People", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2016, PP.3397-3401 S. Nazeem Basha, Dr S.A.K. Jilani, Mr S. Arun – "An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT", International Journal of Engineering Trends and Technology (IJETT) – Volume 33, Number 2, March 2016, PP.84-89 Adnan Ibrahim, Afhal Paravath, P. K. Aswin, Shijin Mohammed Iqbal, Shaeez Usman Abdulla – "GSM Based Digital Door Lock Security System", IEEE International Conference on Power, Instrumentation, Control and Computing (PICC), Thrissur, India, 2015, PP.1-6 Ilkyu Ha – "Security and Usability Improvement on a Digital Door Lock System based on Internet of Things", International Journal of Security and Its Applications Vol.9, No.8 (2015), PP.45-54

	Ohsung Doh, Ilkyu Ha - “A Digital Door Lock System for the Internet of Things with Improved Security and Usability”, Advanced Science and Technology Letters Vol.109 (Security, Reliability and Safety 2015), PP.33-38 Somjit Nath, Paramita Banerjee, Rathindra Nath Biswas, Swarup Kumar Mitra, Mrinal Kanti Naskar – “Arduino Based Door Unlocking System with Real Time Control”, 2nd International Conference on Contemporary Computing and Informatics (ic3i), Noida, India, 2016, PP.358-362 Kaustubh Dhondge, Kaushik Ayinala, Baek-Young Choi, Sejun Song – “Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones”, 12th International Conference on Mobile Ad-Hoc and Sensor Networks, Hefei, China, 2016, PP.251-257 102 Jeong-ile Jeong – “A Study on the IoT Based Smart Door Lock System”, Information Science and Applications (ICISA), Ho Chi Minh City, Vietnam, 2016, PP.1307-1318 https://en.wikipedia.org/wiki/Internet_of_things The design of lock is inspired from: https://www.thingiverse.com/thing:2350856 https://en.wikipedia.org/wiki/Internet_of_things#Manufacturing
Follow up Questions	Could the lock be hacked? What happens when someone does not have any cell service or wifi? Would an electric solenoid be better by having no mechanical movements?

Article #13 Notes: Security system with RFID control using E-KTP and internet of things

Source Title	Security system with RFID control using E-KTP and internet of things
Source citation (APA Format)	Najib A. A. et al. (2021). Security system with RFID control using E-KTP and internet of things. Bulletin of Electrical Engineering and Informatics, 10(3), 1436–1445. https://doi.org/10.11591/eei.v10i3.2834
Original URL	Security system with RFID control using E-KTP and internet of things | Najib | Bulletin of Electrical Engineering and Informatics (beei.org)
Source type	Journal Article
Keywords	Android application, E-KTP, Firebase, Internet of things, NodeMCU V3 ESP8266, PIR sensor, Push notification, RFID sensor
#Tags	Smart lock, RFID, solenoid
Summary of key points + notes (include methodology)	**Components:** ● NodeMCU V3 ESP8266 → microcontroller ○ Less power consumption ○ More memory than arduino ○ Good for prototyping (compared to Raspberry pi) ○ Wireless communication ○ ● RFID sensor ● PIR sensor ● Solenoid ● LED ● Buzzer ● Relay This project developed a secure way to lock and unlock a home using RFID and an android app. For the app, it is connected to the firebase and an alert (sends notifications when PIR sensor detects movement, open, and lock (open & lock for controlling prototype) features are in the app. NodeMCU V3 ESP8266 is connected to the internet and firebase real-time database. Data on firebase stores serial number/UID data from E-KTP, PIR sensor data, and data for relay controllers. The RFID sensor is connected to the NodeMCU for reading the serial number/UID on E-KTP, PIR sensor for detecting motion, led as

	a marker that the prototype is connected to wifi, the buzzer is used when the relay is successfully used it will output sound output, and relays for solenoid controllers. Data was collected through the recording of RFID and application performance (throughput and delay for android app) **RFID** ● Tested different distances (50mm increase each time) ● Detected 4cm or less (table 5) **Android App (lock/unlock features)** ● 30 experiments ● Collected average ● Calculated throughput to be 18366.66667 bps (perfect index based on the standard TIPHON) ● Calculated average delay to be 65.26827336ms (categorized as perfect because <150 ms based on standard TIPHON) **Android App (alert feature)** ● 30 tries ● Collected average ● Average throughput was 18066.6667 bps (perfect index based on standardization TIPHON) ● Average delay was 67.2354995 ms (categorized as berfect because <150 ms based on standardization TIPHON) **Conclusion** This paper provides a design and measures the performance for an RFID and Android App lock. The performance for the RFID was measured by the distance where it could be read. For the app, the two aspects (lock/unlock and alert) were tested. For both, throughput and delay was measured, and everything was perfect according to the standardization TIPHON. With their results, they provide a functional and well-working prototype for a security system using an identity card or an app on a phone.
Research Question/Problem/ Need	Home security is incredibly important because people and families need secure places to live. Home security still uses keys, which are unsafe and allow for thieves to steal from houses.

Important Figures	 Buzzer PIR sensor NodeMCU V3 ESP8266 RFID sensor LED Relay 18650 battery 18650 battery Selonoid Figure 1. Integration of component prototype system security **Prototype and modeled design for the system**  (a) (b) Figure 2. Design prototype, (a) Prototype design from the front, (b) Prototype design from the behind **Prototype of the design from the front and back**

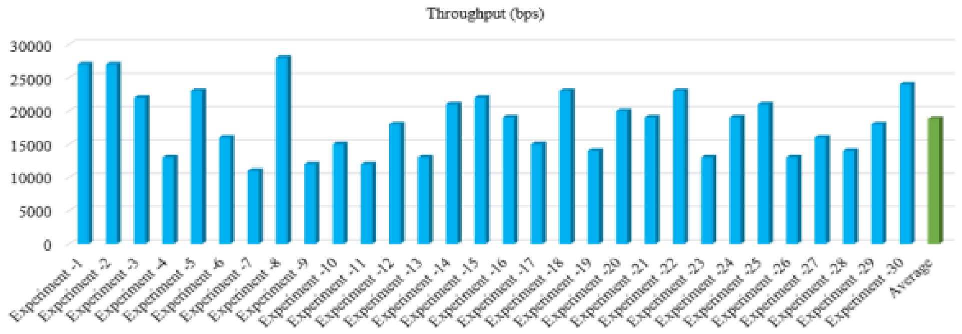
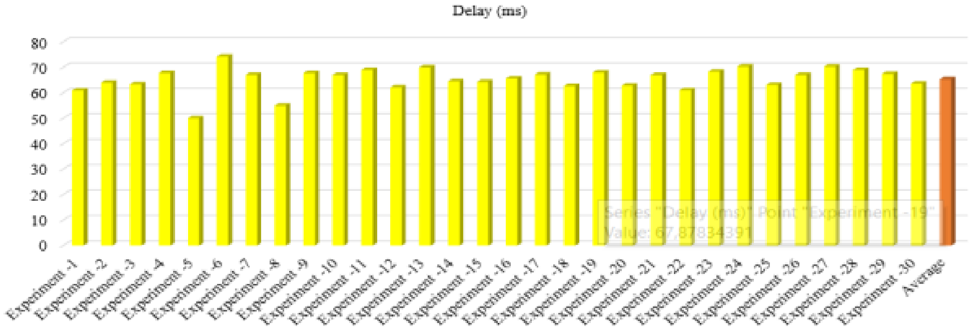


Figure 7. The graph of throughput when open and lock features activated

Throughput measurements and their average (in green) for the lock/unlock features of the app



Delay measurements and their average (in orange) for the lock/unlock features of the app

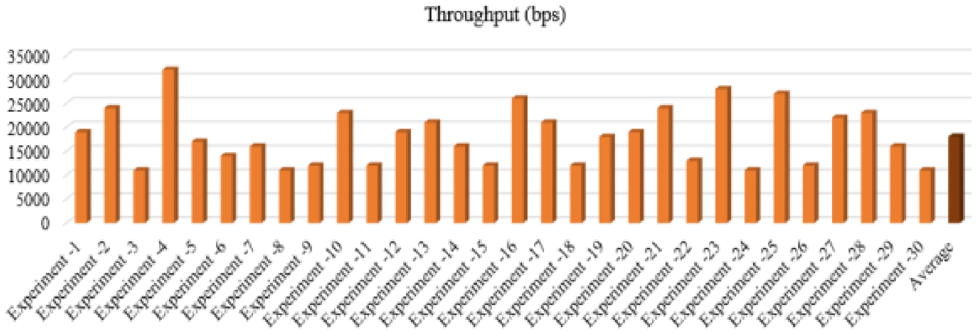
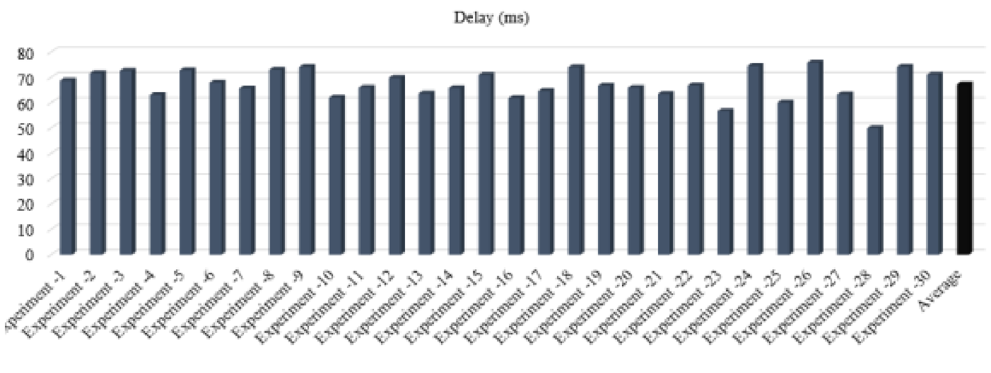


Figure 9. The graph of Throughput when alert feature activated

Throughput measurements and their average (in maroon) for the alert feature of the app

	 Figure 10. The graph of delay when feature activated **Delay measurements and their average (in black) for the alert feature of the app**
VOCAB: (w/definition)	IoT - Internet of Things PIR sensor - Passive Infrared sensor QoS - quality of service UID - unique identifier - unique identification code of numbers contained in RFID/NFC - radio-frequency identification/near field communication Throughput - the amount of material or items passing through a system or process
Cited references to follow up on	M. Husni, H. T. Ciptaningtyas, R. R. Hariadi, I. A. Sabilla, and S. Arifiani, “Integrated smart door system in apartment room based on internet,” TELKOMNIKA Telecommunication Computing Electronics Control, vol. 17, no. 6, pp. 2747-2754, 2019, doi: 10.12928/TELKOMNIKA.V17I6.12322. Taryudi, D. B. Adriano, and W. A. Ciptoning Budi, “Iot-based Integrated Home Security and Monitoring System,” Journal of Physics: Conference Series, vol. 1140, no. 1, pp. 0-7, 2018, doi: 10.1088/1742-6596/1140/1/012006. M. Andriansyah, M. Subali, I. Purwanto, S. A. Irianto, and R. A. Pramono, “e-KTP as the basis of home security system using arduino UNO,” in 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320693. E. Saputro, “Design of Automatic Door Security Using E-KTP Based on Microcontroller Atmega328 (in bahasa: Rancang Bangun Pengaman Pintu Otomatis Menggunakan E-KTP Berbasis Mikrokontroler Atmega328),” Journal Tenik Elektro Unnes, vol. 8, no. 1, pp. 1-4, 2016, doi: 10.15294/jte.v8i1.8787. L. Kamelia, M. R. Effendi, and D. F. Pratama, “Integrated Smart House Security System Using Sensors and RFID,” in 2018 4th International Conference on Wireless and Telematics (ICWT), 2018, pp. 1-5, doi: 10.1109/ICWT.2018.8527803 Z. Mu, W. Li, C. Lou and M. Liu, "Investigation and Application of Smart Door Locks based on Bluetooth Control Technology," 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2020, pp. 68-72, doi:

	10.1109/IPEC49694.2020.9115189 J. Pacheco and K. Miranda, "Design of a low-cost NFC Door Lock for a Smart Home System," 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/IEMTRONICS51293.2020.9216409 V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga and S. Bojewar, "Intelligent security lock," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, India, 2017, pp. 713-716, doi: 10.1109/ICOEI.2017.8300795
Follow up Questions	What would happen if the battery runs out?

Article #14: Design of a low-cost NFC Door Lock for a Smart Home System

Article notes should be on separate sheets

KEEP THIS BLANK AND USE AS A TEMPLATE

Source Title	Design of a low-cost NFC Door Lock for a Smart Home System
Source citation (APA Format)	Pacheco, J., & Miranda, K. (2020). Design of a low-cost NFC Door Lock for a Smart Home System. *IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–5. https://doi.org/10.1109/IEMTRONICS51293.2020.9216409
Original URL	Design of a low-cost NFC Door Lock for a Smart Home System | IEEE Conference Publication | IEEE Xplore
Source type	Conference Paper
Keywords	Prototypes, Microcontrollers, Internet of Things, Pins, Smart homes, Hardware
#Tags	NFC, Door lock, electric lock, Smart Home
Summary of key points + notes (include methodology)	IoT is mainly used in Smart Home applications to aid humans interact with technologies and make daily life easier. Something that is really important to humans is the safekeeping of precious objects. To do that, locks are constantly being used, which creates the incentive to invent more strong, durable locks, and easy to manufacture locks. Plenty of IoT and more “modern” locks have been created, with a variety of interfaces: PIN pad, touchpad, signature pad, biometrics, ZigBee, Bluetooth, QR code, RFID This paper presents a low-cost, scalable, and easy to install door lock controlled using an Arduino Mega and NFC. **Why Arduino as microcontroller:** ● Wide use for prototyping and quick building of digital devices ● Suitable for a variety of applications ● Allows for a variety of modules to be used ● Low-cost ● Multi platform (can be used on several operating systems: Windows, Linux, MacOS) ● Small size

- Shields/Modules

NFC:

NFC allows for people to trade information with NFC devices, such as NFC tag, NFC reader, and NFC enabled smartphone

- Device decides what to do with info received
- Different operating modes
    - *reader/writer* - exchange of information between NFC mobile and NFC tag
    - *Peer to peer* - exchange of information between two NFC mobiles
    - *Card emulation* - exchange of information between NFC reader and NFC mobile

Interested in card emulation because the specific aim for the NFC is for access control (determine if it should allow access or not), to open or deny access to the lock.

- NFC can be easily paired with Arduino
- NFC tags are low-cost

Parts of the system:

The purpose of the study is to create a low-cost, and easy to use and install door lock. To achieve this, the combination of NFC, Arduino, and actuator nodes are necessary.

- *Arduino module* - Arduino Mega 2560 as a microcontroller because it is easily programmable and adaptable
- *NFC module* -
    - bidirectional
    - 13.56MHz
    - <=424 Kb/s bandwidth
    - NFC Shield ITEAD PN532 (NFC tag reader)
    - effective distance = 3cm
- Software module -
    - used Unity (a cross-platform game engine)
    - Used it to create an app for graphical feedback when the user uses the NFC tag

Prototype:

- NFC shield receives information from the NFC tag or mobile
- NFC shield sends the information to the Arduino
- Arduino verifies the information (Arduino has memory, so the database of authorized users is stored directly on the board)
- Arduino directly connected to the lock
- Arduino will action the lock to lock/unlock if authorized user

Regarding power supply, Arduino Mega can be powered via USB, AC/DC adapter, or battery, so they decided that a power supply was not a criteria or concern for the design.

Methodology:

	● Built a prototype diagram of the connection between the NFC shield and the Arduino ● Included an LED in the diagram to make sure the connection worked ● Connected the Clock signal from master to slave (SCK), Master Out Slave In (MOSI), Master In Slave Out (MISO), Slave-enabled signal, the whole thing controlled by master devices (NSS) protocols for the Serial Peripheral Interface (SPI), supported by Arduino' library for NFC module ○ Advantages of SPI: The protocol is ■ Simple ■ Fast compared to UART and 12C ■ Data can be transmitted and received at the same time **Testing:** Implemented the prototype and tested it using both an authorized NFC tag and an unauthorized one. Used a screen to see and test the different results. 1. When an unauthorized user tried unlocking the door a. Without an NFC tag, it is impossible to open the door b. With an unauthorized NFC tag, the screen displayed a closed lock symbol to demonstrate denied access 2. When an authorized user tried unlocking the door a. The screen displays an open lock to show that the door is unlocked **Conclusion:** This paper presents an inexpensive, easy to use and install door lock with the use of NFC technology and Arduino. Both were chosen for specific reasons: NFC because of its promising uses and rising popularity, and Arduino because of its ease of use for developing prototypes and flexibility. The researchers believed that the NFC tags could be changed to also be able to be read through smartphones. This study sets a basis for improving home security, which could further be improved with fingerprint unlocking, and facial recognition.
Research Question/Problem/ Need	IoT is becoming more and more present in humans' daily lives because of monitoring accessibility and the fact that things can be used while a person is next to them or miles away. Humans constantly have the need to protect their belongings in their homes. To do so, they use locks. Because of this, locks need constant improvement and more modern, durable, accessible, and easy to use and manufacture designs.

Important Figures

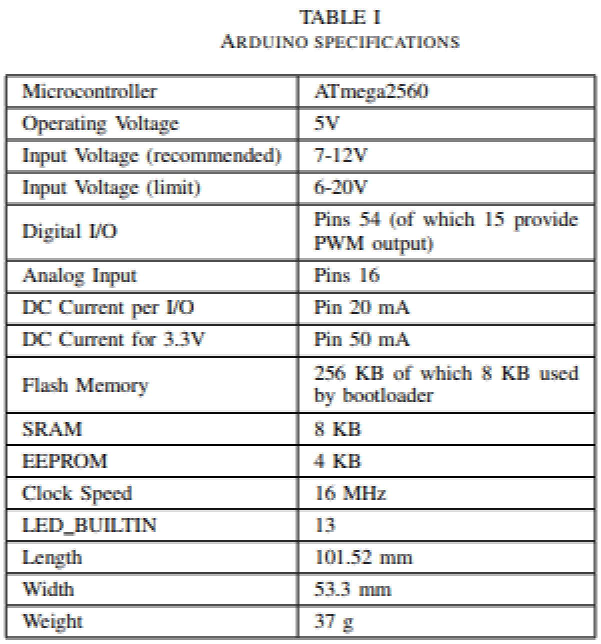


TABLE I
ARDUINO SPECIFICATIONS

Microcontroller	ATmega2560
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O	Pins 54 (of which 15 provide PWM output)
Analog Input	Pins 16
DC Current per I/O	Pin 20 mA
DC Current for 3.3V	Pin 50 mA
Flash Memory	256 KB of which 8 KB used by bootloader
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz
LED_BUILTIN	13
Length	101.52 mm
Width	53.3 mm
Weight	37 g

Details about the Arduino Mega used in this project

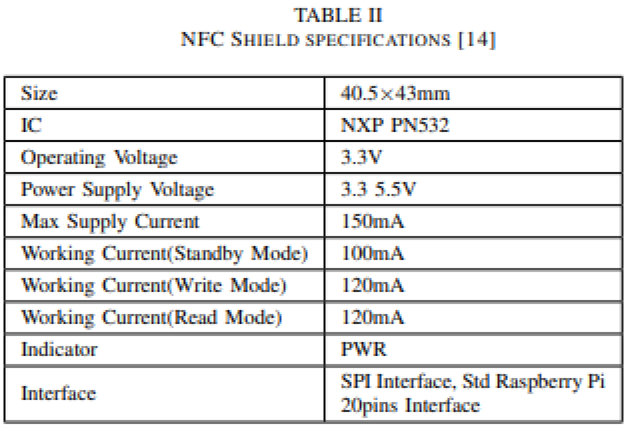
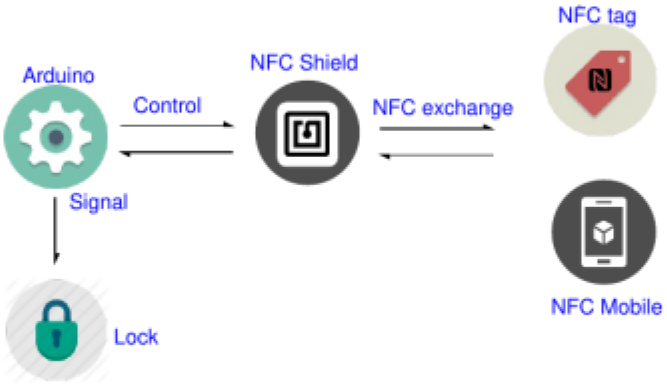
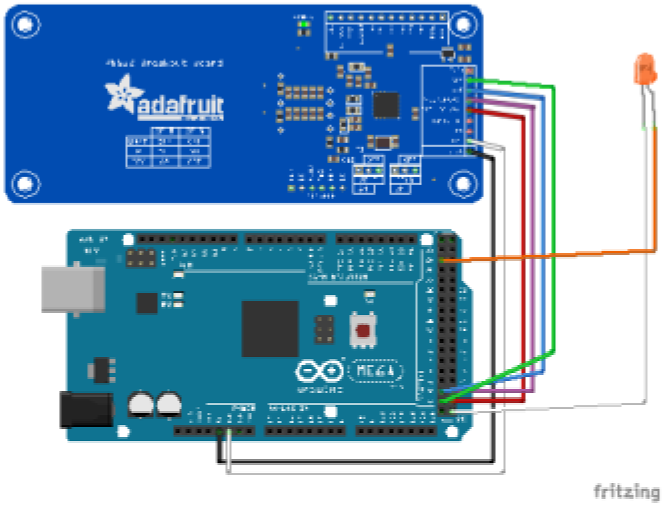


TABLE II
NFC SHIELD SPECIFICATIONS [14]

Size	40.5×43mm
IC	NXP PN532
Operating Voltage	3.3V
Power Supply Voltage	3.3 5.5V
Max Supply Current	150mA
Working Current(Standby Mode)	100mA
Working Current(Write Mode)	120mA
Working Current(Read Mode)	120mA
Indicator	PWR
Interface	SPI Interface, Std Raspberry Pi 20pins Interface

Details about the NFC tag reader used in the project

	 Arduino Control NFC Shield NFC exchange NFC tag Signal Lock NFC Mobile Fig. 2. Components interaction **Graphical abstract of how the system works**  Fig. 3. Prototype diagram **Prototype design of how the Arduino is connected to the NFC shield**
VOCAB: (w/definition)	NFC - Near field communication Modules/Shields - pre-built circuits (can be different kinds of sensors, Bluetooth, Wi-fi, Joysticks, Ethernet, etc.) SPI - Serial Peripheral Interface - an interface used to send data across microcontrollers MISO and MOSI- unidirectional method for communicating where one piece (controller) controls the other MOSI - the output from SPI master to slave MISO - output from slave to master
Cited references to follow up on	H. Chaouchi, “Chapter 1. Introduction to the Internet of Things,” in The Internet of Things: Connecting Objects to the Web. Wiley and Sons, 2010, pp. 1–32.

N. Mitton and D. Simplot-Ryl, “From the Internet of things to the Internet of the physical world,” Comptes Rendus Physique, vol. 12, no. 7, pp. 669–674, 2011, Nanoscience and nanotechnologies: hopes and concerns.

History of Keys, “History of Locks,” accessed on July 2020. [Online]. Available: http://www.historyofkeys.com/locks-history/history-of-locks/

The History of Keys, “History of Locksmithing,” accessed on July 2020. [Online]. Available: http://www.historyofkeys.com/lockshistory/history-of-locksmithing

P. R. Nehete, J. P. Chaudhari, S. Pachpande, and K. P. Rane, “Literature Survey on Door Lock Security Systems,” International Journal of Computer Applications, vol. 153, pp. 13–18, 2016.

Y. T. Park, P. Sthapit, and J. Pyun, “Smart digital door lock for the home automation,” in TENCON 2009 - 2009 IEEE Region 10 Conference, 2009, pp. 1–6.

M. S. Hadis, E. Palantei, A. A. Ilham, and A. Hendra, “Design of smart lock system for doors with special features using bluetooth technology,” in Procedings of the International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, Mar. 2018, pp. 396–400.

A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, “Development of web-based smart security door using qr code system,” in 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 2020, pp. 13–17.

G. K. Verma and P. Tripathi, “A Digital Security System with Door Lock System Using RFID Technology,” International Journal of Computer Applications, vol. 5, pp. 6–8, 2010.

K. Tshomo, K. Tshering, D. Gyeltshen, J. Yeshi, and K. Muramatsu, “Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition,” in 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 2019, pp. 1–5.

T. Igoe, D. Coleman, and B. Jepson, “Chapter 2. NFC and RFID,” in Beginning NFC. O’Reilly Media, Inc., 2014, pp. 11–24.

V. Coskun, K. Ok, and B. Ozdenizci, “Chapter 2. NFC and RFID,” in Professional NFC Application Development for Android. Wrox, 2013, pp. 11–24.

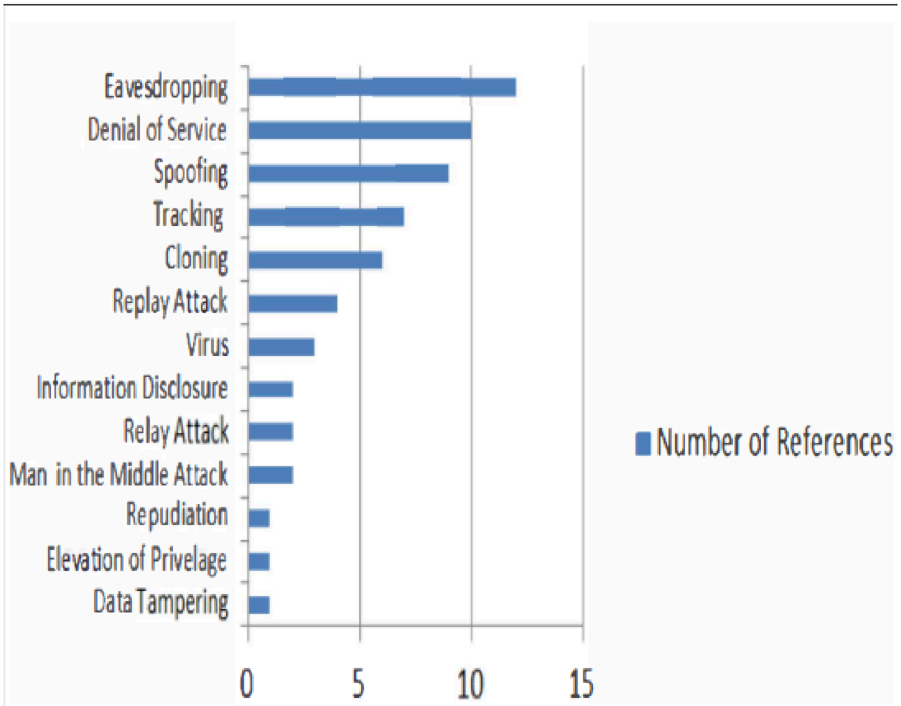
S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, “Arduino based door unlocking system with real time control,” in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 358–362.

	Iteadstudio, “ITEAD PN532 NFC Module,” accessed on July 2020. [Online]. Available: https://www.itead.cc/wiki/ITEAD PN532 NFC MODULE Unity, “Unity 3D,” accessed on July 2020. [Online]. Available: http://unity3d.com
Follow up Questions	Why wasn’t any unlocking method and mechanism tested and used? (The results show only the response from the screen). What would happen in case of a power outage? It is mentioned that the lock could only be unlocked through NFC, but that the power for the Arduino came from a power outlet, or AC/DC. Would that mean that during a power outage, a person would not be able to enter their home? How many NFC tags can be registered (entered in the Arduino database) and recognised by the Arduino as authorized?

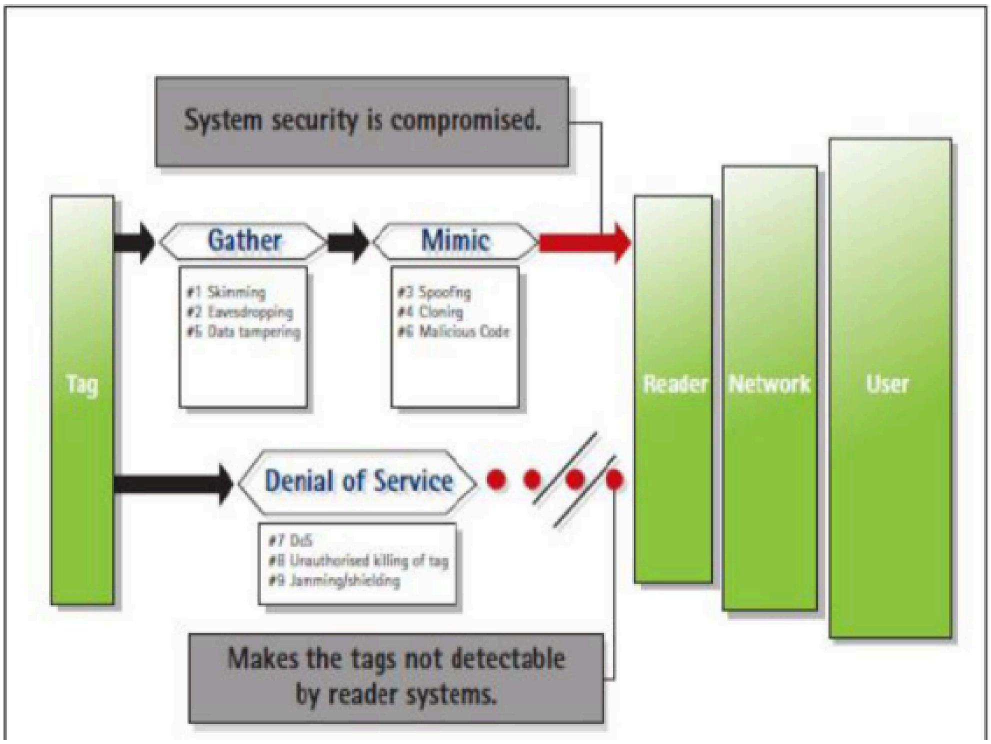
Article #15 Notes: RFID Security Issues & Challenges

Source Title	RFID security Issues
Source citation (APA Format)	Kulkarni, G., Shelke, R., Sutar, R., & Mohite, S. (2014). RFID Security Issues & Challenges. *IEEE 2014 International Conference on Electronics and Communication Systems (ICECS)*, 1–4. https://doi.org/10.1109/ECS.2014.6892730
Original URL	https://ieeexplore.ieee.org/document/6892730
Source type	Conference Paper
Keywords	RFID, Security, Privacy, Eavesdropping
#Tags	RFID, RFID lock, RFID security
Summary of key points + notes (include methodology)	The most significant issues that come with RFID are privacy and authentication security. RFID is a kind of technology that aids computers and computing systems to identify different things. Humans can naturally do so, but computers execute those tasks poorly. RFID is projected to completely replace the bar code in a couple of years. Unfortunately, the security part is minimized and may cause risks to organizations and individuals because of the want to reduce tag prices, so there are plenty of security requirements that need to be addressed in order for RFIDs to achieve their full potential. It is important to understand that perfect security and privacy cannot exist, so it is not a question of making RFID technology completely flawless, but rather, minimizing entry points for a thief Vulnerable aspects: ● Jamming: ○ Thieves can achieve this through powerful transmitters (large distance) or shielding (more passive) ● Eavesdropping ○ RFID technology emits data, so it is possible that the data be eavesdropped ○ Thieves do this by intercepting data with a compliant reader ○ Simple for thieves to do because of RFID tags using clear text communication (due to memory, capacity, or cost) ○ Eavesdropping is dangerous because the data from the RFID tag could allow the thief to collect sensitive information, or formulate a replay attack

	● Replay Attack ○ May be executed through a clone of the RFID tag, or resending a signal from an Eavesdropping attack ○ To effectuate this kind of attack, information from the tag must first be collected while it is used (aka if eavesdropping and unauthorized card reading is secure, then it would be near impossible to execute a replay attack) ● Deactivation ○ Renders the RFID tag useless (the reader can no longer identify the tag) ● Detaching the tag ○ (In the case of supermarkets as an example) the tag is physically removed from an item (or switched with another) so the RFID reader doesn't identify the item correctly ● Spoofing ○ This method allows thieves to write blank RFID tags ● Man-in-the-middle ○ Possible in real-time, while the data is in transit ○ Unrecognizable by the system, which will think a network error occurred ○ RFID is vulnerable to this type of attack due to their small size and low price (aka lack of sophistication circuitry security-wise) ● Cloning ○ Gives access to the attacker the same rights as if he had the original RFID tag RFID tags may revolutionize society but first, many security aspects need to be analyzed and improved to protect consumers' and organizations' privacy and personal information. Protecting data and valuable information is extremely important in communication. It is obvious that RFID is the answer to a lot of people's lives, but their small size and low cost mean they have to be improved and analyzed much more for security threats to be the optimal tool.
Research Question/Problem/ Need	RFID is rapidly growing, with its uses being expanded, so security issues that come with RFID have to be investigated.

<table>
<tr>
<td><b>Important Figures</b></td>
<td>


<b>Major attacks and how the number of times they happened (period not defined)</b>



<b>Threat categories, what they do, and how they affect data transmission between the tag and reader</b>
</td>
</tr>
<tr>
<td><b>VOCAB: (w/definition)</b></td>
<td>Jamming - attempt to disturb (RFI) the air interface between the RFID reader and</td>
</tr>
</table>

	RFID tag Shielding - blocking radio frequency electromagnetic signals and cause RFI RFI - radio frequency interference Eavesdropping - secretly listening to a conversation Replay attack - attacker abusing another’s identity by repeating the same authentication sequence Spoofing - the duplication of tag data and transmitting it to a reader Man-in-the-middle-attack - attacker interrupts the communication path between the tag and reader, and manipulates the information back and forth Cloning - capture data from one tag and creates a copy of it on new tag
Cited references to follow up on	"Specification of RFID Air Interface", http://www.epcglobaline.org. Bereford and F. Stajano, (2003), "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, Vol. 2, No. I, pp 46-55. Q. Z. Sheng , X. Li and S. Zeadally "Enabling next-generation RFlD applications: Solutions and challenges", Computer, vo1.41, no. 9, pp.21 -28 2008 Adriana Alxandru, Eleonora Tudora, Ovidiu Bica "Use of RFlD Technology for Identification, Traceability, Monitoring and Checking of Product Authenticity" World Academy of Sciences, Engineering and Technology, Issue 7 1, November 20 10, pp. 765-769. Tieyan Li "Employing Lightweight Primitives on Low-cost RFID Tags for Authentication", IEEE VTC 2008 Fall. Mitrokotsa, M.R. Rieback and A.S. Tanenbaum. ClassifYing RFlD Attacks and Defences. Information Systems Frontiers, Springer, July 2009. Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp381-394, February 2006. Divyan M. Konidala, Daeyoung Kim, Chan Yeob Yeun, Byoungcheon Lee "Security Framework for RFID-based Applications in Smart Home Environment" Journal of Information Processing Systems, Volume 7, March 201 1, pp. 1 1 1- 120 Garfinkel, S. & Rosenberg, B. (2005). RFID: Applications, Security, and Privacy, Addison-Wesley Professional, ISBN:0321290968, Boston,MA.
Follow up Questions	Are there other alternatives to RFID? How can these deficiencies in RFID be

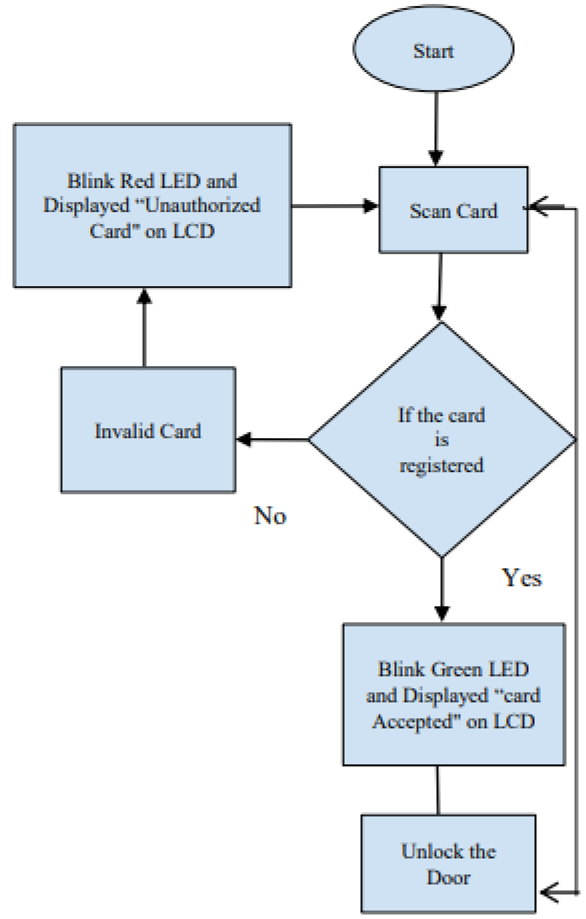
	resolved? Are there other aspects in which RFID could be used, but without the possibility for negative intentions?

Article #16 Notes: Door Lock using RFID and Arduino

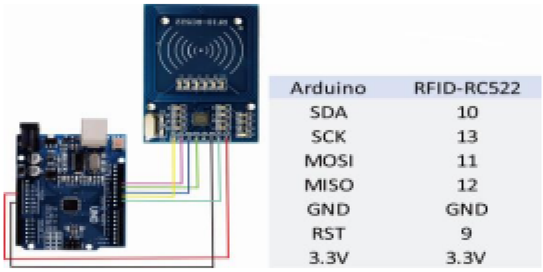
Source Title	Door Lock using RFID and Arduino
Source citation (APA Format)	Dharmale, G. J., Katti, J., Waghere, S., Patankar, T., & Ati, K. (2022). Door Lock using RFID and Arduino. *IEEE 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–5. https://doi.org/10.1109/ICCCNT54827.2022.9984396
Original URL	https://ieeexplore.ieee.org/document/9984396
Source type	Conference Paper
Keywords	Crystals, Programming, Light emitting diodes, Liquid crystal displays, RFID, Arduino, Internet of Things, Door lock system
#Tags	Lock, Smart home door lock, Arduino door lock
Summary of key points + notes (include methodology)	RFID is a wireless and contactless system that is available in a variety of industries. It allows the performance of several operations such as access control, management systems, etc. RFID Arduino door lock systems are secure and effective, and can be done rapidly, especially because of the ease-of-use of Arduino. Also, each RFID tag is different and has its own code, which makes it secure to lock and unlock with this system. A device like this would allow users to quickly lock and unlock doors without having to put too much effort. Methodology: 1. The RFID card was registered first 2. The coding of the Arduino with its different conditions fo whether to let access to or deny access to cards was then coded around the RFID that was registered a. Check the card ID i. If registered, unlock the lock ii. If not, stay locked with a display message 3. Parts of the RFID system a. RFID tag - Antenna - Electronic chip unit - Has battery power to output a message to the reader by using the loading trick: opening and closing the load on

	the tag antenna to affect the measurable unit. The voltage change are considered zero, which transmits the information from mark to reader b. RFID reader - Frequency module - Control unit - Antenna coil (generate magnetic field) The tag has battery power 4. Arduino pseudocode a. Scan card b. Check card’s hexadecimal code in memory i. Code is in memory - Authorized card - LED blink green ii. Code is not in memory - Unauthorized card - LED blink red Parts of the system: - Arduino UNO - Open-source board - Based on easy-to-use hardware and software - Able to read input and transform into output - RC522 RFID Reader - Radio Frequency module to receive and transmit electromagnetic signals - Breadboard - For building and testing the circuit - Green and red LED - Green to show a valid card, red to show an unregistered/invalid RFID tag - LCD 16*2 - Display module - To display messages on screen - Jump Wires - To connect the different parts - Resistor (220Ω) - Control the flow of electricity in the circuit The researcher successfully developed an Arduino and RFID-based door lock. The system works as expected: when a user with the right RFID card tries unlocking the system, the green LED and the screen show the door unlocking, and when the wrong tag is used, the red LED and screen show accordingly.
Research Question/Problem/ Need	How could a simpler and faster way to unlock doors be developed?

Important Figures

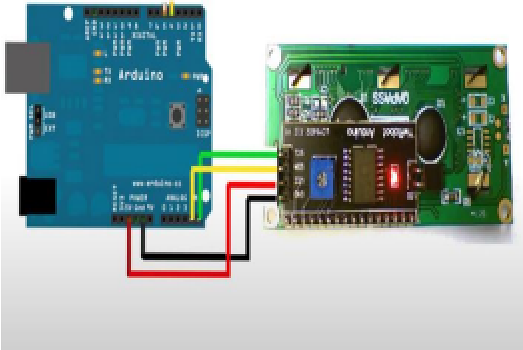
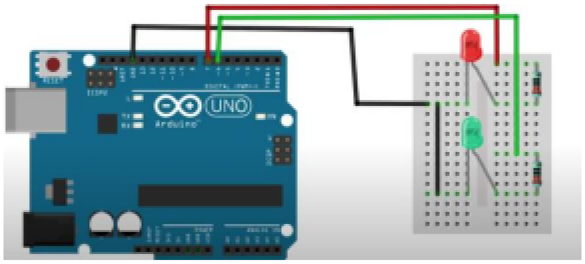
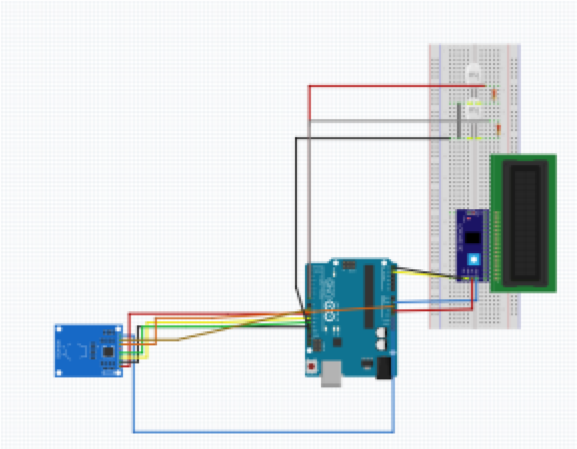

Start
Scan Card
Blink Red LED and Displayed "Unauthorized Card" on LCD
If the card is registered
Invalid Card
No
Yes
Blink Green LED and Displayed "card Accepted" on LCD
Unlock the Door

Flowchart of the pseudocode of the Arduino



Arduino	RFID-RC522
SDA	10
SCK	13
MOSI	11
MISO	12
GND	GND
RST	9
3.3V	3.3V

RFID connection with Arduino with what ports they connected each element to

	 **LCD and Aruino connection**  **LEDs and Arduino connection (resistors to protects the LEDs)**  **Complete circuit with all the parts**
VOCAB: (w/definition)	LED - light emitting diode LCD - liquid crystal display
Cited references to follow up on	Gyanendra Kumar Verma, (2010), A Digital Security System with Door Lock System Using RFID Technology. International Journal of Computer Applications (0975 – 8887) Volume 5– Issue No.11. RFID-Based Digital Door Locking System, Shubham Soni, Rajni Soni, Akhilesh A.

	Waoo. ISSN: 2582-8835 (Online), Volume-1 Issue-2, September 2021. R. Weinstein, “RFID: A technical overview and its application to the enterprise,” IT Professional, vol. 7, no. 3, May-June 2005, pp. 27-33. Website Reference - RFID Card Reader with Arduino RFID RC522 and LCD 16, https://www.instructables.com/RFID-CARDREADER-WITH-ARDUINORFID-RC522-andLCD-16/. Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, and Muhammad Usman Asad, "RFID Based Security and Access Control System" IACSIT International Journal of Engineering and Technology, Vol. 6, No. 4, August 2014. Zhang, L., "An Improved Approach to Security and Privacy of RFID Application System," Wireless Communications, Networking, and Mobile Computing. International Conference. pp 1195- 1198, 2005. Orji EZ*, Oleka CV, Nduanya UI, Automatic Access Control System using Arduino and RFID, Journal of Scientific and Engineering Research, 2018, 5(4):333-340. https://www.hackster.io/babariyasmit/rfiddoor-lock-system-c177a3. https://howtomechatronics.com/tutorials/arduino/rfid-works-make-arduino-based-rfiddoor-lock/ Arduino - https://www.arduino.cc.
Follow up Questions	How did the testing take place? What exactly is the loading trick? Could it be explained better/into more detail?

Article #17 Notes: Door Security System for Home Monitoring Based on ESP32

Source Title	Door Security System for Home Monitoring Based on ESP32
Source citation (APA Format)	Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door Security System for Home Monitoring Based on ESP32. *Procedia Computer Science*, *157*, 673–682. https://doi.org/10.1016/j.procs.2019.08.218
Original URL	https://www.sciencedirect.com/science/article/pii/S1877050919311378
Source type	Journal Article
Keywords	Home Security, Internet of Things, Lock Door, IoT, Encrypted, MQTT, Cloud
#Tags	Smart home door lock, door lock,
Summary of key points + notes (include methodology)	Doors are important in home security. This project proposes an application based on Arduino and using IoT technology to monitor and control a door, which in turn would increase house security. For this system, MQTT cloud was used as the communication unit between the door lock system and the smartphone. A PIR sensor will be place in front of the door to detect movement, and a touch sensor is placed on the door handle to sense when someone tries to open the door by force. If this happens, an alarm will ring and notifications will be sent to the house owner of the existence of an intruder. MQTT enables a publish/subscribe mechanism. A receiver can connect to the server to subscribe for a specific topic. After that, if a message is generated, the message will be sent to the receiver. In contrast, if one is using HTTP a device that would receive the message needs to request periodically to a server whether is a message or not. The security of a house can be improved by improving the security of its door. IoT has been used in previous works about smart home technology for a variety of uses. Research has also been conducted on efficiency to lower energy consumption. Furthermore, there has been research on smart home security systems, which could monitor both external activity using motion sensors and cameras as well as autonomous locking through a mobile smartphone app, but there are not many systems that incorporate IoT, home security systems and remote controlled doors. The purpose of this study is to monitor and control a

door remotely, receive alerts when someone is near the door, grant access to trusted people who are near the door, and view the access history (when the lock was opened and for how much time). The major differences between this project and past ones is that this lock also allows the owner to view access history and to grant access from afar to the people they trust.

Methodology:

- ESP32:
  - Microcontroller
  - Used to integrate the device in one environment
  - Used because it has two cores
    1. Run Wifi functions
    2. Execute uploaded programs
  - Has a Bluetooth and Wifi module and 36GPIO
  - Relatively large memory
  - Low power consumption
  - Integrated touch sensor
- PIR sensor
  - Detect motion
- Magnetic sensor
  - Detect whether the door is opened or closed

Communication between the system and the phone is through the MQTT protocol system, which uses SSL encryption.

- MQTT provides MQTT broker service (over the internet)
- MQTT broker is responsible for receiving all signals sent and delivering them to the subscriber.
- A publisher/subscriber (device) like a mobile phone uses an app to send commands to the MQTT
- This device also receives signals from the MQTT in the form of notifications for different reasons
- Another publisher/subscriber is the microcontroller/IoT device (aka a mini computer that executes program)
- In this case, the microcontroller sends messages to the MQTT
- The messages are results from things sent by the sensors
- The microcontroller also acts as a subscriber in the way that it receives a message/command to execute
- The lock itself is only a subscriber - it only receives commands on what to do and does it

Components

- Adaptor - to supply electricity to the system fro, the outlet
- Step Down - to reduce voltage received from 12V to 5V
- PCB - connect all electrical components
- ESP32 - microcontroller
- Reset Button - Button to reset the ESP32

- PIR sensor - for movement detection
- LED - red for power & green for wifi indicator
- Magnetic sensor - sense door status (locked/unlocked)
- Internal touch sensor - sense where the door is opened from (inside vs outside)
- Mosfet - for automatic switches
- Alarm Buzzer - alarm to ring when the door is opened by force
- Electric strike - to lock/unlock the door.

Software

- Divided into 2 parts:
    - Mobile app
    - Door lock software

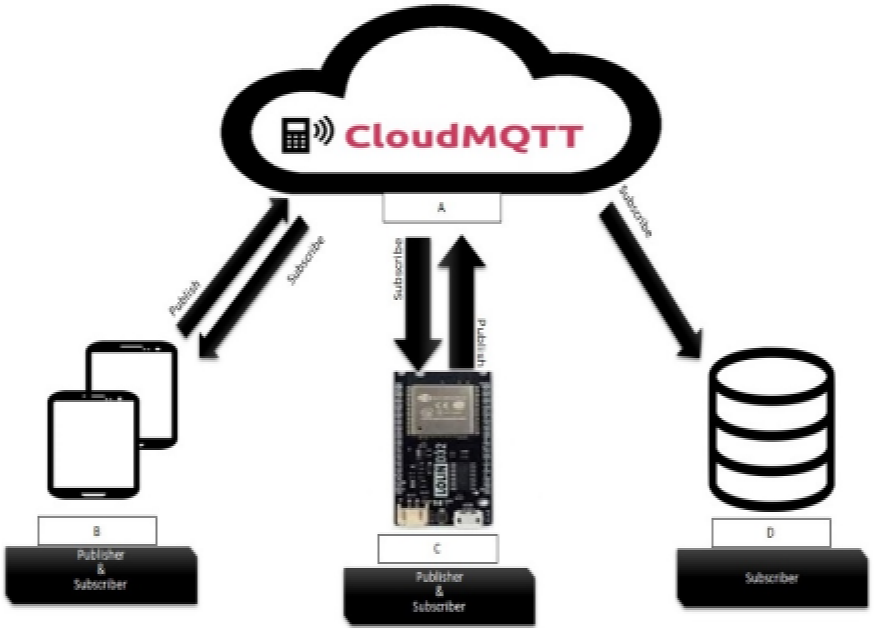
The MQTT receives a message and transmits it to the door lock. It then analyzes the order that has been given; if it is to unlock the door, then the door would unlock, a notification would be sent to the phone, and a timer would start. After 10 seconds, if the door had not been opened, it would lock again. If the command tis to lock the door, the system would check if the door is opened or closed using the magnet sensor. If the door is not closed, it will send a message saying the door is not closed, and if the door is closed, it will lock the door. If the command is to turn the buzzer off, it will check whether the buzzer is ringing. If the buzzer is ringing, it will turn it off, if it is not, it will send a notification to the user that the alarm is off. If the command is to reset, the system will erase its memory and restart. If no message is received, the touch sensor will sense whether there has been any contact and execute a bunch of sensing. If the PIR sensor detects movement, a message will be sent to the owners about motion being detected in front of their door.
The 3 main door statuses are: door opened/closed, door locked/unlocked, alarm is ringing/not ringing

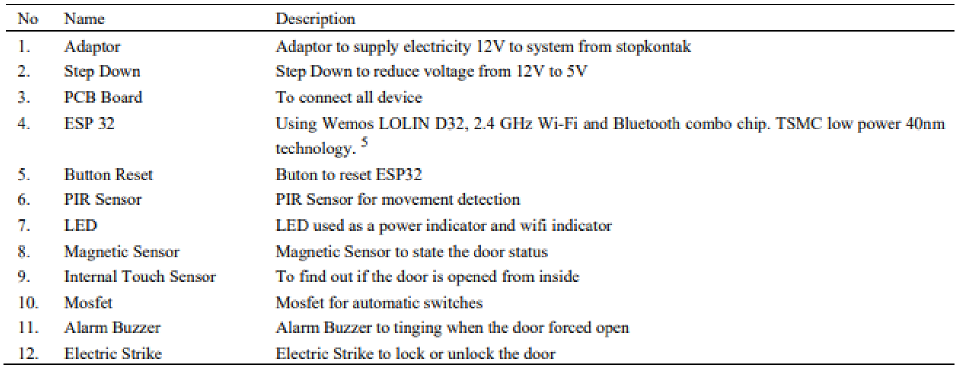
Analysis

Motion detection was done through a PIR sensor. It was placed 48.5 cm facing down on the prototype door. It was able to detect up to 1.6 m accurately.

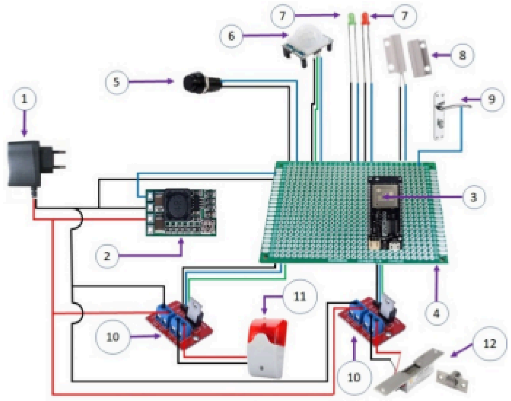
For the testing of the MQTT sending and receiving messages accurately, WireShark (a tool for analyzing network traffic) was used.
4 tests conducted

1. Testing on sending messages from MQTT without SSL encryption
    a. Message was able to be seen clearly by MQTT but also others (aka insecure)
2. Testing on receiving messages by MQTT without SSL encryption
    a. Message was received successfully, but could be seen by others (insecure)
3. Testing on sending messages from MQTT with SSL encryption
    a. Message was sent but could not be read by the public
4. Testing on receiving messages by MQTT with SSL encryption

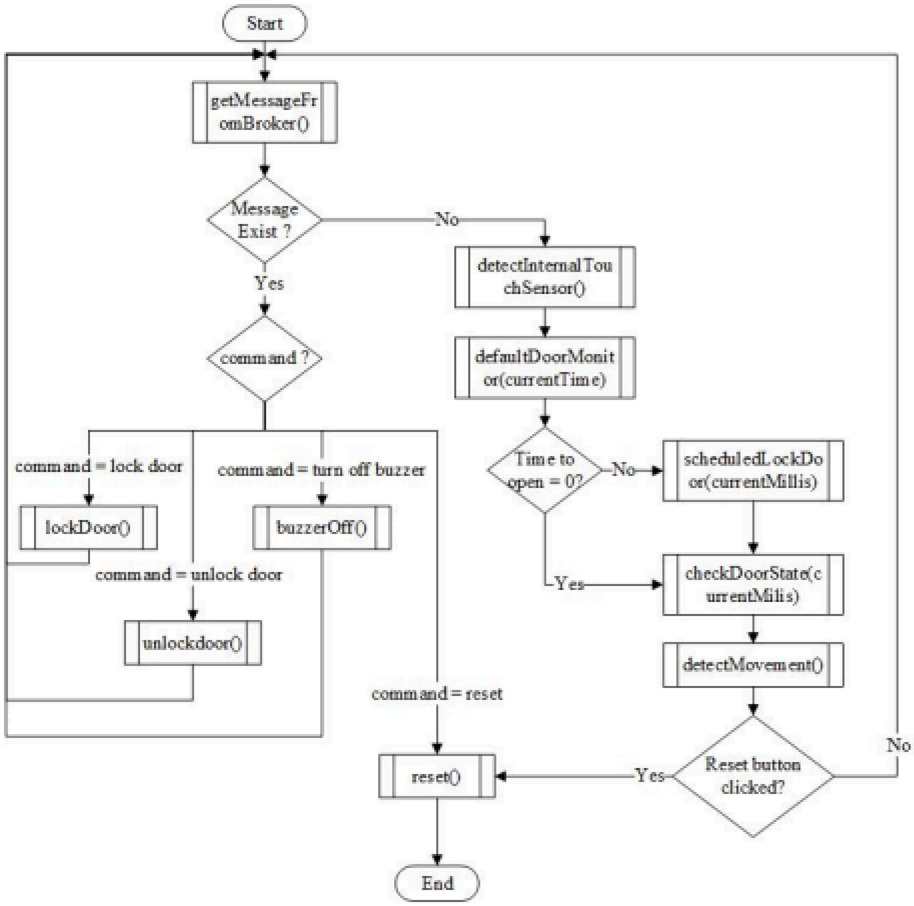
	a. Message was received, but could not be read by others Conclusion This article presents a smart home security system based on IoT comprised of an ESP32, PCB, Step down (12V to 5V), 12V adaptor, reset button, PIR sensor, green and red LEDs, Magnetic Sensor, Internal touch sensor, 2 Mosfet, alarm buzzer, and electric strike door lock. This system can control and monitor a door remotely, by also allowing access to other people and tracking the door history. Test have shown that the optimal place ot put the PIR sensor was 48.5cm high, and it could only accurately detect motion closer or equal to 1.6 m. They also show that it was possible to send and receive encrypted messages to make the system safe from hackers. Possible future improvements include implementing a camera for the owners to see who or what was detected by the PIR sensor, an emergency call property to call the police, a feature for easier communication between visitors and owners, and a feature to filter the door's history log.
Research Question/Problem/ Need	Doors are the primary defense system in a house so it is important for them to be as advanced as they can. Also, people often forget to close the door behind them after they leave the house or want to check if they did or not.
Important Figures	 CloudMQTT A Publish Subscribe Subscribe Publish Subscribe B Publisher & Subscriber C Publisher & Subscriber D Subscriber Fig. 1. System Architecture Design **Diagram of how the system interacts with each part: the phone, door lock, listener, and cloud (MQTT protocol)**



No	Name	Description
1.	Adaptor	Adaptor to supply electricity 12V to system from stopkontak
2.	Step Down	Step Down to reduce voltage from 12V to 5V
3.	PCB Board	To connect all device
4.	ESP 32	Using Wemos LOLIN D32, 2.4 GHz Wi-Fi and Bluetooth combo chip. TSMC low power 40nm technology. [5]
5.	Button Reset	Buton to reset ESP32
6.	PIR Sensor	PIR Sensor for movement detection
7.	LED	LED used as a power indicator and wifi indicator
8.	Magnetic Sensor	Magnetic Sensor to state the door status
9.	Internal Touch Sensor	To find out if the door is opened from inside
10.	Mosfet	Mosfet for automatic switches
11.	Alarm Buzzer	Alarm Buzzer to tinging when the door forced open
12.	Electric Strike	Electric Strike to lock or unlock the door



Parts of the system and their connection

	 Start
	getMessageFromBroker()
	Message Exist ?
	No
	Yes
	command ?
	command = lock door
	command = turn off buzzer
	lockDoor()
	buzzerOff()
	command = unlock door
	unlockdoor()
	command = reset
	reset()
	End
	detectInternalTouchSensor()
	defaultDoorMonitor(currentTime)
	Time to open = 0?
	No
	scheduledLockDoor(currentMillis)
	Yes
	checkDoorState(currentMilis)
	detectMovement()
	Reset button clicked?
	Yes
	No
	Software pseudocode

VOCAB: (w/definition)	MQTT - Message Queue Telemetry Transport - a protocol used for network communication 36GPIO - General purpose input/output - a signal pin on the circuit SSL - Secure sockets layers encryption creates a unique communication between devices that provides privacy, authentication and integrity to the communication over the internet Publisher & subscriber - a device in the system - publishers can send information, subscribers can only receive information PCB - printed circuit board - used to connect electrical components together in a circuit
Cited references to follow up on	Burange AW, Misalkar HD. Review of Internet of Things in development of smart cities with data management & privacy. IEEE International Conference on Advances in Computer Engineering and Applications. 2015 July 23;: p. 1. Wukkadada B, Wankhede K, Nambiar R, Nair A. Comparison with HTTP and MQTT In Internet of Things (IoT). In Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA

2018); 2018; Coimbatore. p. 249-253.

Vikram N, Harish KS, Nihaal MS, Umesh R, Kumar SAA. A Low Cost Home Automation System Using Wi-Fi Based Wireless Sensor Network Incorporating Internet of Things(IoT). In 2017 IEEE 7th International Advance Computing Conference; 2017; Hyderabad. p. 174-179.

Alaa M, Zaidan AA, Zaidan BB, Talal , Kiah MLM. A Review of Smart Home Applications based on Internet of Things. Journal of Network and Computer Applications. 2017; 97.

Agarwal A, Hada N, Virmani D, Gupta T. A Novel Design Approach for Smart Door Locking and Home Security using IoT. A High Impact Factor & UGC Approved Journal. 2017 August; 6(8): p. 1-5.

M. N, Kamat , Shinde D. Smart Door Security Control System Using Raspberry Pi. International Journal of Innovations & Advancement in Computer Science. 2017 November; 6(11): p. 1-4.

Gupta RK, Balamurugan S, Aroul K, Marimuthu R. IoT Based Door Entry System. Indian Journal of Science and Technology. 2016 October; 9: p. 1-5.

Kodali RK, Jain V, Bose S, Boppana L. IoT Based Smart Security and Home Automation System. In 2016 International Conference on Computing, Communication and Automation (ICCCA); 2016; Noida. p. 1286-1289.

Sahoo KC, Pati U. IoT Based Intrusion Detection System Using PIR Sensor. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT); 2017; Bangalore.

Tanwar S, Patel P, Tyagi S, Kumar N, Obaidat MS. An Advanced Internet of Thing based Security Alert System for Smart Home. In 2017 International Conference on Computer, Information and Telecommunication Systems (CITS); Dalian.

Kumar S, Swetha S, Kiran VT, Johri P. IoT based Smart Home Surveillance and Automation. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON); 2018. p. 786-790.

Prabaharan J, Swamy A, Sharma A, Bharath KN, Mundra PR, Mohammed KJ. Wireless Home Automation and Security System using MQTT Protocol. In 2017 2nd IEEE International Conference On Recent Trends In Electronics Information & Communication Technology; 2017; Bangalore. p. 2043-2045.

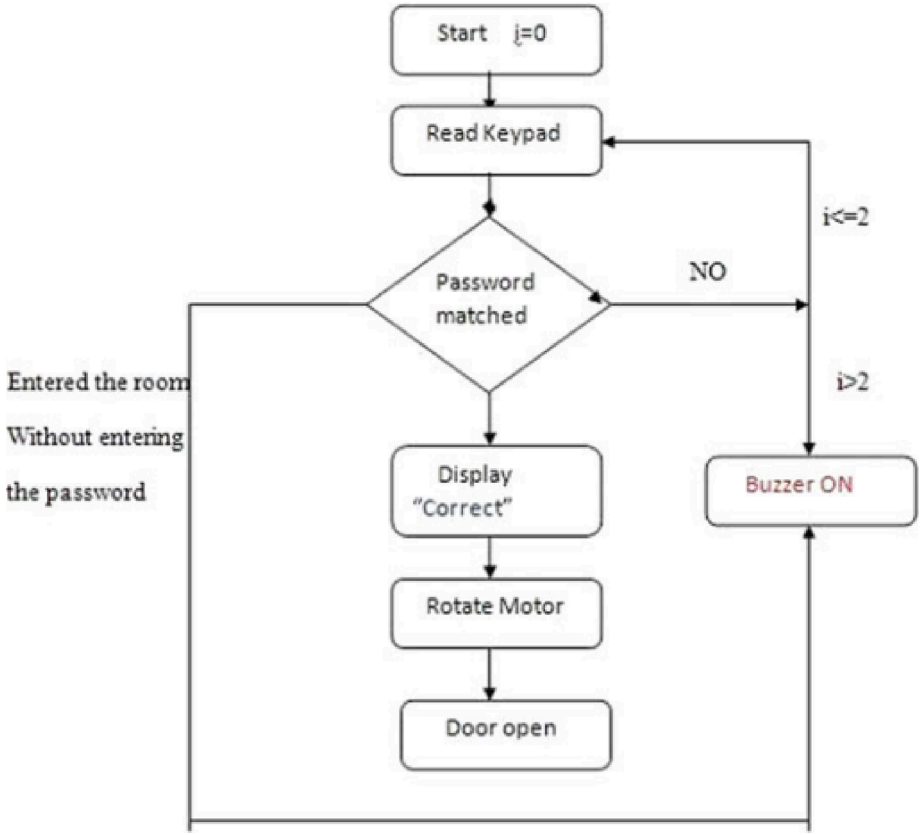
	Pandit V, Majgaonkar P, Meher P, Sapaliga S, Bojewar S. Intelligent Security Lock. In International Conference on Trends in Electronics and Informatics; 2017; Tirunelveli. p. 713-716. Dutta J, Wang Y, Maitra T, Islam SH, Rawal BS, Giri D. ES3B: Enhanced Security System for Smart Building using IoT. In 2018 IEEE International Conference on Smart Cloud (SmartCloud); 2018; New York. p. 158-165. Home - WEMOS.CC. [Online].; 2018 [cited 2019 June 2. Available from: https://www.wemos.cc/
Follow up Questions	How would this system receive its electrical energy? Would it be directly connected to a power outlet? Does incorporating this system mean that one has to replace their entire door?

Article #18 Notes: IoT-Based Smart Security System on a Door Lock Application

Source Title	IoT-Based Smart Security System on a Door Lock Application
Source citation (APA Format)	Dansana, D., Mishra, B. K., Sindhuja, K., & Sahoo, S. (2021). IoT-Based Smart Security System on a Door Lock Application. In: Kumar, R., Mishra, B. K., & Pattnaik P. K. (Eds.), Next Generation of Internet of Things (Vol. 201, pp. 695–703). Springer Singapore. https://doi.org/10.1007/978-981-16-0666-3_57
Original URL	https://link.springer.com/chapter/10.1007/978-981-16-0666-3_57
Source type	Conference Paper
Keywords	Smart door, Arduino, Password, Home automation, Arduino, Infrared ray, (IR) sensors
#Tags	Smart door lock, Arduino, Automated door
Summary of key points + notes (include methodology)	Innovation is at the center of our lives. Having home automation using IoT enables people to control their homes from a distance and helps them save time and energy, while also keeping the home safe. Previous works have researched and proposed home security systems, but they lack the use of a buzzer system. This article will make a similar system, but will incorporate a buzzer system. The project will revolve around an Arduino and several sensors. The proposed system involves a digital code lock with 4 digits. The Arduino will have a passcode in its memory, and if the user enters in the same passcode, then access will be granted and the Infrared (IR) Sensor will be deactivated. The passcode entered by the user does not match the one in the Arduino, access will be denied and the user can try again. After three denials, the buzzer will ring. Also, if a person enters the house without entering any passcode (force the door open), the IR sensor will sense that and the buzzer will ring. **Parts/Components:** ● Arduino Uno:Microcontroller for hardware ● LCD Display: Liquid crystal display (LCD) works based on light modulating properties with polarizers for light beams ● Keypad: For people to enter the passcode ● IR Sensor: Motion detector ● Bread Board: allow to model the circuit and connect electrical parts ● Buzzer: sound gadget for an alarm ● Servo Motor: specific angle-controlled motor, for locking/unlocking door ● Potentiometer: three-terminal resistor with a customizable voltage divider

	- 220- Resistor: to limit the flow of electricity in the circuit - Connecting Wires: connect all electrical components - USB Cable: used to connect Arduino and the system. **System Pseudocode** 1. Person enters passcode a. Correct Passcode i. Display correct ii. Turn servo motor and unlock door b. Incorrect Passcode i. Not third try 1. Try again ii. Third try 1. Buzzer turns on 2. Person forcefully opens the door (without passcode) a. Buzzer turns on **Results:** Testing was conducted for both when the passcode was correct and when it was incorrect. The system worked well.
Research Question/Problem/ Need	IoT is constantly getting more popular and widely used. A method for better home management with a buzzer system is needed.

Important Figures



Flow chart of proposed work

Pseudocode flowchart of how the system would operate and what actions would be triggered for each condition

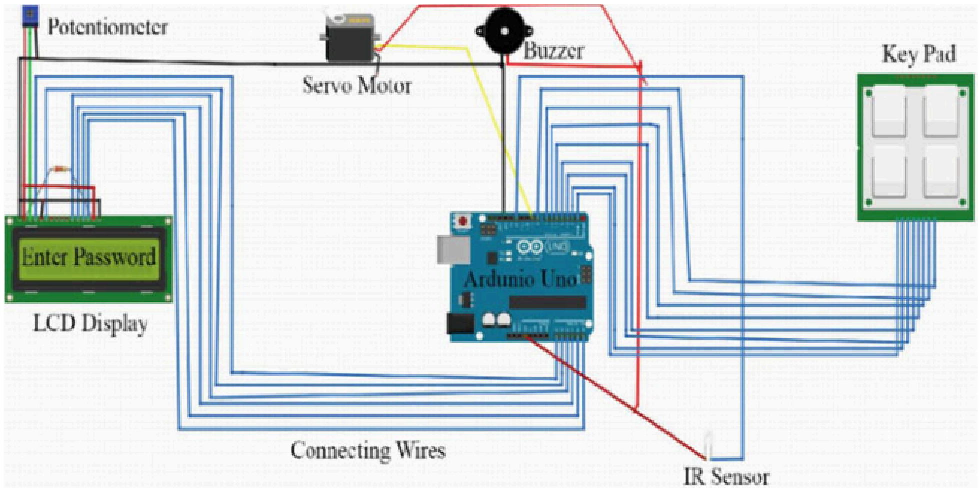
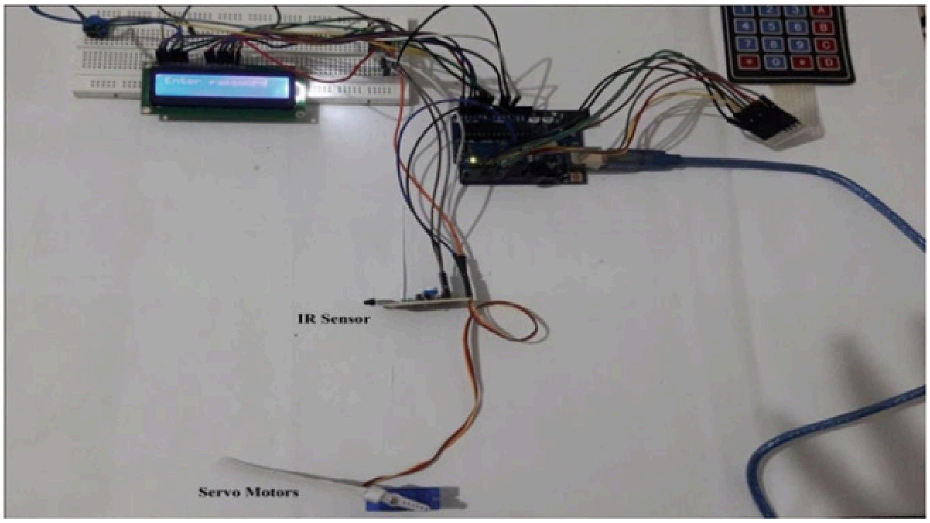


Fig. 2 Block diagram of smart security system

Model of the system with all the parts connected

	 **Fig. 3** Digital code lock venture **Actual model built**
VOCAB: (w/definition)	IR - Infrared - having a wavelength greater than red but less than microwaves (emitted by heated objects) Infrared sensor - sensor that detects motion by receiving Infrared radiation Potentiometer - a variable resistor with a third adjustable terminal. The potential at the third terminal can be adjusted to give any fraction of the potential across the ends of the resistor.
Cited references to follow up on	Aldawira CR et al (2019) Door security system for home monitoring based on ESP32. Procedia Comput Sci 157: 673–682 KumAri, VA, ArAin A, JiSKAni AA (2018) Keyless smart home: an application of home security and automation Park YT, Sthapit P, Pyun J-Y (2009) Smart digital door lock for the home automation. In: TENCON 2009–2009 IEEE region 10 conference. IEEE Hussein NA, Al Mansoori I (2017) Smart door system for home security using raspberry pi3. In: 2017 ınternational conference on computer and applications (ICCA). IEEEs Khan SR, Al Mansur A, Kabir A, Jaman S, Chowdhury N (2012) Design and ımplementation of low cost home security system using GSM network. Int J Sci Eng Res 3:1 Kale MPV, Sharma SD (2014) Intelligent home security system using illumination sensitive background model. Int J Adv Eng Res Dev (IJAERD) 1

	ElShafee A, Hamed KA (2012) Design and implementation of a WIFI based home automation system. World Acad Sci Eng Technol 68: 2177–2180 Park YT, Sthapit P, Pyun J-Y (2009) Smart digital door lock for the home automation. In: TENCON 2009- 2009 IEEE region 10 conference, pp 1–6 Hung C-H, Bai Y-W, Ren J-H (2015) Design and implementation of a door lock control based on a near field communication of a smartphone. In: 2015 IEEE ınternational conference on consumer electronics-Taiwan (ICCE-TW), pp 45–46 Gupta RK, Balamurugan S, Aroul K, Marimuthu R (2016) IoT based door entry system. Indian J Sci Technol 9:1–5 Prabaharan J, Swamy A, Sharma A, Bharath KN, Mundra PR, Mohammed KJ (2017) Wireless home automation and security system using MQTT protocol. In: 2017 2nd IEEE ınternational conference on recent trends ın electronics ınformation & communication technology; 2017; Bangalore, pp 2043–2045 Pandit V, Majgaonkar P, Meher P, Sapaliga S, Bojewar S (2017) Intelligent security lock. In: International conference on trends in electronics and ınformatics; 2017; Tirunelveli, pp 713–716 Dutta J, Wang Y, Maitra T, Islam SH, Rawal BS, Giri D (2018) ES3B: enhanced security system for smart building using IoT. In: 2018 IEEE ınternational conference on smart cloud (SmartCloud); New York, pp 158–165 Balas VE, Solanki VK, Kumar R, Khari M (eds) (2019) Internet of things and bigdata analytics for smart generation, vol 154. Springer, p 309 Khari M, Kumar M, Vij S, Pandey P (2016) Smart cities: a secure datatransmission model. In: Proceedings of the second ınternational conference on ınformation andcommunication technology for competitive strategies, pp 1–5 Khari M, Garg AK, Gandomi AH, Gupta R, Patan R, Balusamy B (2019) Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Trans Syst Man Cybern Syst 50(1):73–80 Vimal S, Khari M, Dey N, Crespo RG, Robinson YH (2020) Enhanced resource allocation in mobile edge computing using reinforcement learning based MOACO algorithm for IIOT. Comput Commun 151:355–364 Vimal S, Khari M, Crespo RG, Kalaivani L, Dey N, Kaliappan M (2020) Energyenhancement using multiobjective ant colony optimization with double Q learning algorithmfor IoT based cognitive radio networks. Comput Commun 154:481–490
Follow up Questions	Was enough testing done? How would you ensure that the system works all the

	time? Is a servo motor the best way to unlock a smart-door? Isn't having the locking part mechanical less safe? Also, don't solenoids consume less energy (they only need energy to either lock or unlock)? Where would the power come from/

Article #19 Notes: Smart Digital Door Lock for the Home Automation

Source Title	Smart Digital Door Lock for the Home Automation
Source citation (APA Format)	Park, Y. T., Sthapit, P., & Pyun, J.-Y. (2009). Smart digital door lock for the home automation. *TENCON 2009 - 2009 IEEE Region 10 Conference*, 1–6. https://doi.org/10.1109/TENCON.2009.5396038
Original URL	https://ieeexplore.ieee.org/document/5396038
Source type	Conference Paper
Keywords	Digital door lock system, home automation, ZigBee, Sensor node
#Tags	Door Lock, Smart Door lock, Control system, Smart Home door lock
Summary of key points + notes (include methodology)	ZigBee module will be used. It consists of an RFID reader for authentication, an LCD, motors for opening and closing the door, sensor nodes to detect conditions in the house, communication nodes, and a controller module to control the whole system. The biggest advantage of this system over others is that it can be easily installed and used without the need for specific equipment or mount. Although there has been previous research about ZigBee home automation systems, they all provided limited security if at all. This project proposes a digital door lock for a home automation system that uses ZigBee sensors at their optimal level. In this system, the ZigBee module is in the lock and the lock acts as the main controller for the whole system. The whole system can be surveyed through the digital door lock because it is the first and last thing people come across when entering or leaving the house. This system can be installed anywhere with ease. ZigBee Module ● Includes RF communication node ● Main components: ○ Transceiver - uses RF chip with a modern implementing of the medium access control ○ MCU - controller to control the transceiver and execute programs ● Contains program memory for implementing medium access control, a network layer, and an application layer Door Lock ● Contains control module

    - Brains of the system. Controls door lock & controls and monitors the network
    - Controls motor drive circuit
- Contains Input/Output module
- Contains Motor module
- Composed of:
    - main processor
    - ZigBee module
        - Interface between sensor nodes and control module
    - Door lock controller
        - Open/close buttons activate digital door lock for opening and closing actions
    - CDMA module
        - Notify users about emergencies through SMS and MMS
    - camera module
        - Interaction between visitor and home-owner before opening the door
    - card reader
        - Used for authentication through RFID tags
    - Microphone
        - Interaction between visitor and home-owner before opening the door
    - Speaker
        - Interaction between visitor and home-owner before opening the door
    - LCD
        - Entering and changing password
        - Changing sensor node settings
        - Displaying information on the screen

Sensor Node

1. Monitor the conditions in and around the house (ie. temperature, gas leakage, burglary, etc.)
2. Switch power status of device in the house

- Constantly upload the data and send messages to results from commands sent.

Communication

1. Centralized mode
    - Door lock takes control of communication in the network
    - Sensor nodes act as instructed by the door lock
    - This type of communication is done when everything is all right
    - Reduces unnecessary communication between sensor nodes and central controller as well as save energy consumption
2. Emergency mode
    - This type of communication is done during emergency situations (fires, burglary, etc.)

- After sensor node detects the emergency mode, the respective action is turned on (ie. water would start falling to stop a fire, or a buzzer would start ringing in case of a burglary
- The event is directly reported to the door lock
- Door lock reports the even to the user (SMS or MMS)

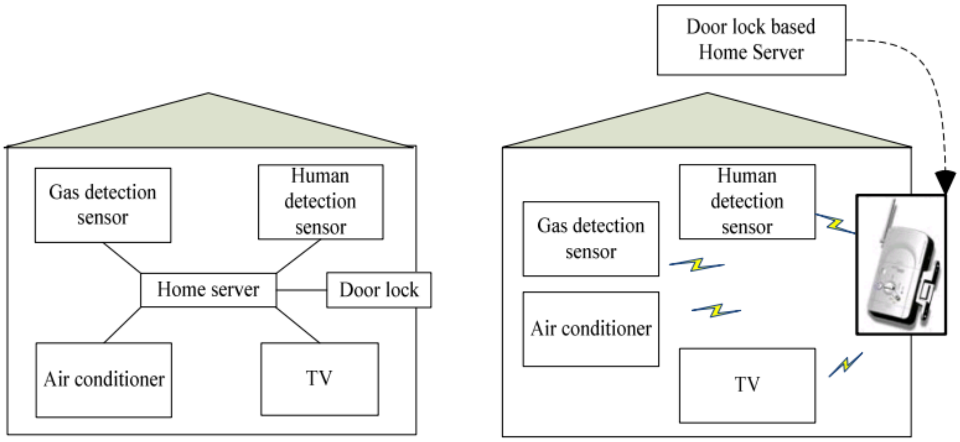
Door Lock System

- Person is authenticated through RFID tag
- Door unlocks and LCD displays all the information about the house status
- The user can change the status of the home or leave them

1. Manual mode
2. Automatic mode

Three possible events;

1. Person entering
    a. The lock is the first thing the person sees when trying to enter
    b. They authenticate
    c. The system door unlocks
    d. The lock then gets fresh information on the status of the house, checks for emergency and displays it on the LCD
    e. Lock enters manual mode and user can set things on and off through the LCD
    f. If the LCD is not touched, system enters automatic mode
        i. For the mode to work, prior settings have to be determined (what devices should be on/off when the user is at home)
        ii. The system will then turn on or off all the devices for which the settings were determined
2. Person Leaving
    a. The lock is the last thing the person sees when leaving the house
    b. Once the lock button is pressed, the door lock receives all the house status and displays them on the screen
    c. Systems enters manual mode
        i. User can choose what to turn on and off manually
    d. If user doesn't touch the LCD screen after leaving, system enters automatic mode
        i. For the mode to work, prior settings have to be determined (what devices should be on/off)
        ii. The system will then turn on or off all the devices for which the settings were determined
3. Emergency
    a. System detects an emergency situation
    b. The information si notified by the door lock
    c. Sensor node handles the emergency through actuators
    d. Door lock sends SMS or MMS to user about the emergency
    e. Triggers an alarm (for example if it is a gas leakage, everything that could impact the situation to make it worse is turned off)

	Final design Implemented a prototype for home automation based on a door lock with ZigBee network protocol. The final design remodeled a commercial door lock. All the circuits for locking/unlocking were rebuilt into the AVR controller for ZigBee. The UI is the touch LCD. An adaptor is connected to the ZigBee relay module which is on the sensor node. The switch module is used to power the system on/off Conclusion This paper presents a new, working method for home automation based on the principle of a door lock. It makes sense because it is the first and last thing a user would see when entering or leaving their home. This system uses ZigBee's capacities at a maximum for controlling and surveying a house. This device is also cheap thanks to the wireless communications, flexibility and ease of installation.
Research Question/Problem/ Need	Wireless technologies are replacing wired ones because they provide more flexibility and extensibility.
Important Figures	 Door lock based Home Server Gas detection sensor Human detection sensor Home server Door lock Air conditioner TV Gas detection sensor Human detection sensor Air conditioner TV Figure 1. Typical wired home server system VS. proposed smart door lock based server system. **Comparison between the usual smart home system and this device. The digital door lock is at the center of the whole system.**

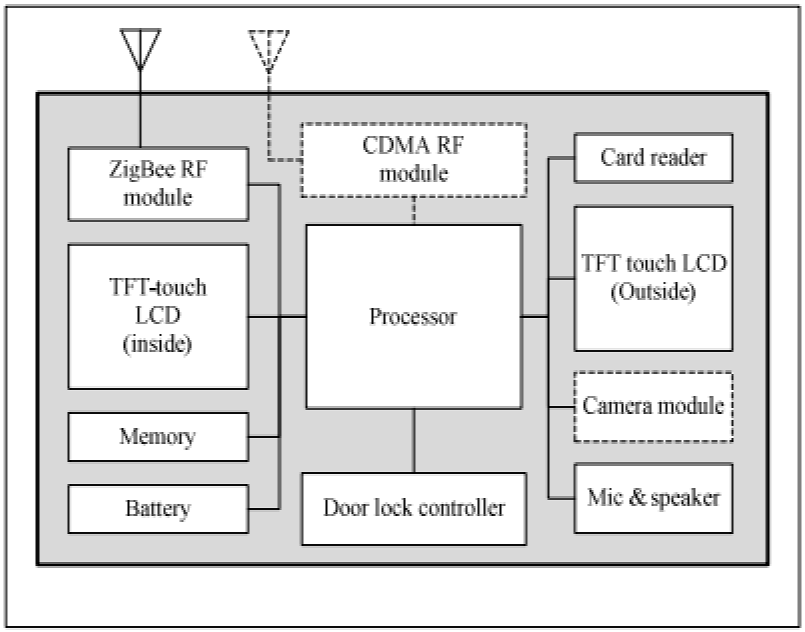
<table>
<tr>
<td></td>
<td>


Figure 3. Structure of digital door lock.

Figure of the door lock and all f what it contains with their simplified connections
</td>
</tr>
</table>

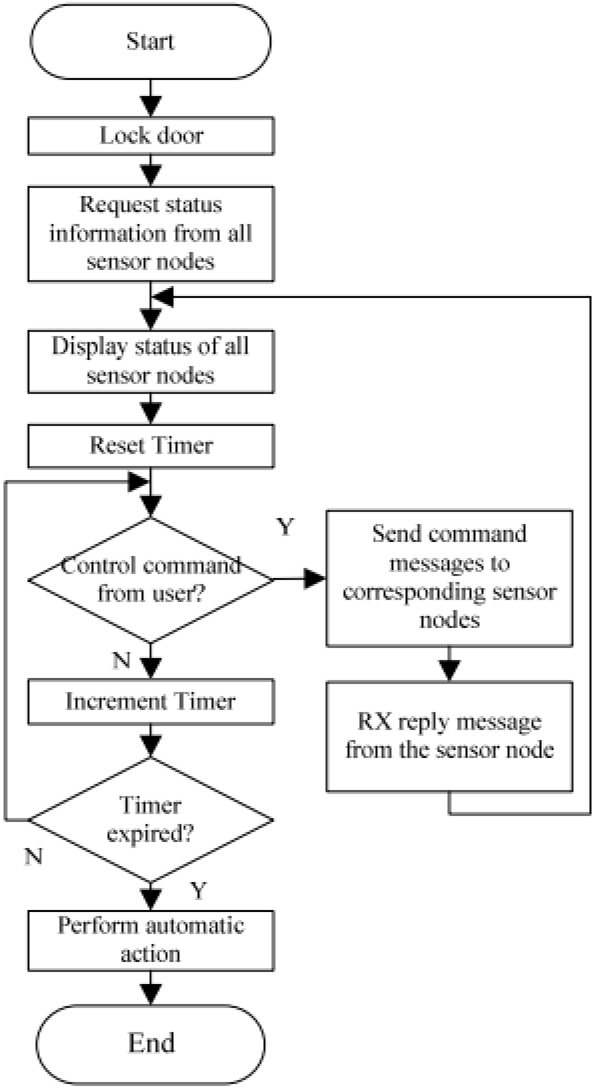

Start
Lock door
Request status information from all sensor nodes
Display status of all sensor nodes
Reset Timer
Control command from user?
Y
Send command messages to corresponding sensor nodes
RX reply message from the sensor node
N
Increment Timer
Timer expired?
N
Y
Perform automatic action
End

Figure 5. Flow chart for outgoing event.

Pseudocode of what happens when a person leaves the house

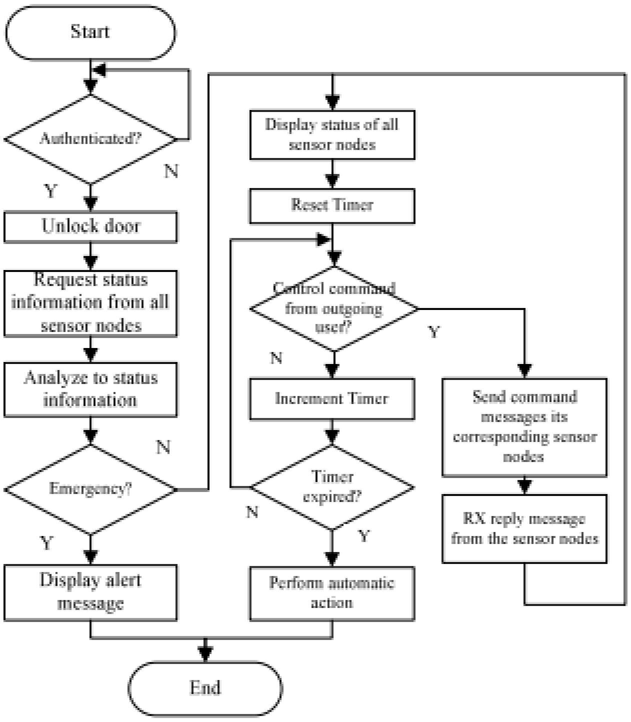
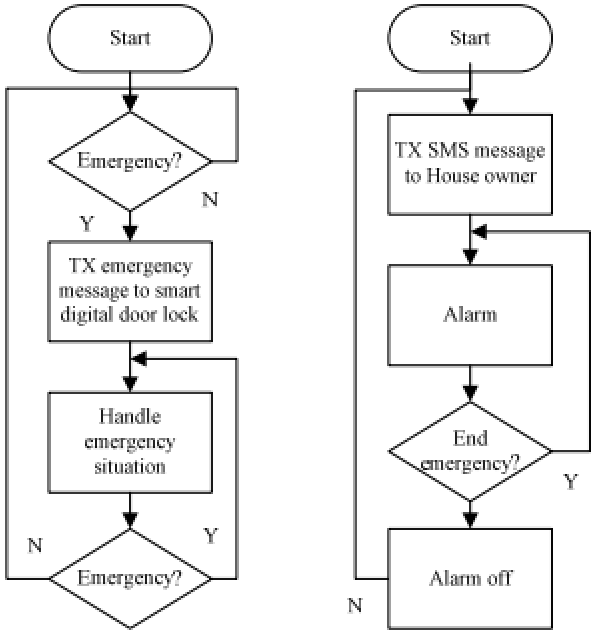

Start
Authenticated?
N
Y
Unlock door
Request status information from all sensor nodes
Analyze to status information
N
Emergency?
Y
Display alert message
Display status of all sensor nodes
Reset Timer
Control command from outgoing user?
Y
N
Increment Timer
Send command messages its corresponding sensor nodes
Timer expired?
N
Y
RX reply message from the sensor nodes
Perform automatic action
End

Figure 6. Flow chart incoming event.

Pseudocode for when a person enters the house


Start
Emergency?
N
Y
TX emergency message to smart digital door lock
Handle emergency situation
N
Y
Emergency?
Start
TX SMS message to House owner
Alarm
End emergency?
Y
Alarm off
N

(a) Sensor node (b) Digital door lock

Figure 7. Flow chart for emergency event.

	Pseudocode for emergency situations and what would happen in the sensor node (a) and digital lock (b)
VOCAB: (w/definition)	CDMA - code division multiple access - channel access method for communication methods SMS - Short messaging service - allows to send and receive text messages (usually through a cell phone) MMS - multimedia messaging service - allows to send and receive media (pictures, audio recordings, videos) between mobile devices ZigBee - protocol that provides an easy to use architecture for wireless networks
Cited references to follow up on	ZigBee Alliance Document 053474r06, ZigBee Specification, v. 1.0, Dec 2004. F. L. Zucatto, C.A. Biscassi, F. Monsignore, F. Fidelix, S. Coutinho, and M. L. Rocha, "ZigBee for Building Control Wireless Sensor Networks," in proceeding of Microwave and Optoelectronics Conference, pp. 511- 515, Oct. 2007. Il-Kyu Hwang and Jin-Wook Baek, "Wireless Access Monitoring and Control System based on Digital Door Lock," IEEE Trans. On Consumer Electronics, Vol. 53, No. 4, Nov. 2007. pp 1724-1730. A. Wheeler, “Commercial Applications of Wireless Sensor Network Using ZigBee”, IEEE Communications Magazine, V. 45, N. 4, pp.:70 – 77, April 2007. Eaton Corp., “Eaton Home Heartbeat,” http://www.homeheartbeat.com/HomeHeartBeat/index.htm. http://www.ZigBee.org
Follow up Questions	Was enough testing conducted? If so, how was the system tested? What would happen during a power outage? Would a person be locked inside or outside their house?

Article #20 Notes: A Smart Lock System using Wi-Fi Security

Source Title	A Smart Lock System using Wi-Fi Security
Source citation (APA Format)	Kassem, A., Murr, S. E., Jamous, G., Saad, E., & Geagea, M. (2016). A smart lock system using Wi-Fi security. *IEEE 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, 222–225. https://doi.org/10.1109/ACTEA.2016.7560143
Original URL	https://ieeexplore.ieee.org/document/7560143
Source type	Conference Paper
Keywords	Local Area Network, Central Control, SmartLock-System
#Tags	Smart Lock, Lock Control,
Summary of key points + notes (include methodology)	This paper presents a locking system using more modern and innovative technology. The world is constantly evolving and finding new innovations to advance the future and make the world "smarter". Unfortunately, locks have been around for around 4000 years and their way of working has not changed that much. The question is why not make a lock and key innovate as the world is changing around them. Nowadays, smartphones and the number of mobile devices people have is rapidly increasing worldwide. Furthermore, a variety of useful apps have been developed. Phones are no longer used to only call people, they are also used to control several devices in human's everyday lives. Through phones, people are able to control so many devices from a distance. Locks are normally used using a key or passcode. However, these locks can cause issues, for example if a key is lost or a passcode forgotten. Using a phone to unlock a lock would resolve those issues and present more accessibility to the user. **Smart Lock Systems** Phones have become an integral part of human's lives, so it is deduced that it would be less likely to lose them than to lose a key. Also they are much bigger and harder to lose. Furthermore, phones are very secure and protect valuable personal information. A Smart lock system would replace a keychain with a digital keychain and all the keys with digital ones. Those digital keys could be managed through the phone and updated/renewed anytime through any device, which would save time and effort

for users.

Major Parts of the system

1. Door lock controller - implements all functions necessary for the lock
2. Central control - heart of the system - combination of smaller systems that read, command, lock/unlock, and execute other operations of the lock
3. Mobile application - where the digital keychain is stored and where all the digital keys can be found. The SLS app is the only software able to control the system. Provides other useful tools for users

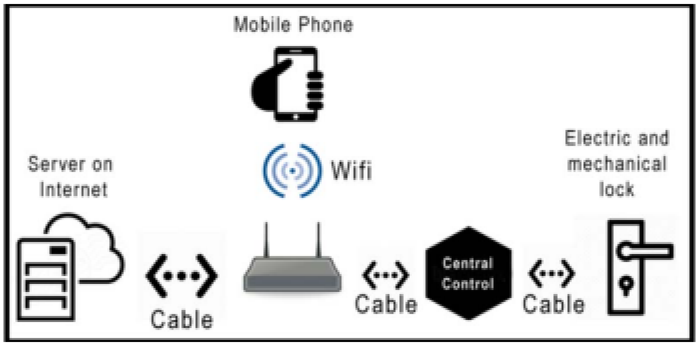
How the system works
The user should be connected to the same LAN as the system.
When the user is connected to the same network as the system, they can send commands to the lock using the app. Commands are sent through Wi-fi and received by the Central control
Central control receives the packets and assembles them with an Ethernet Module, then it decides to follow the command or not.
The commands sent to the central control will be sent to the smart lock server, where the notifications are forwarded to user through email, or text message

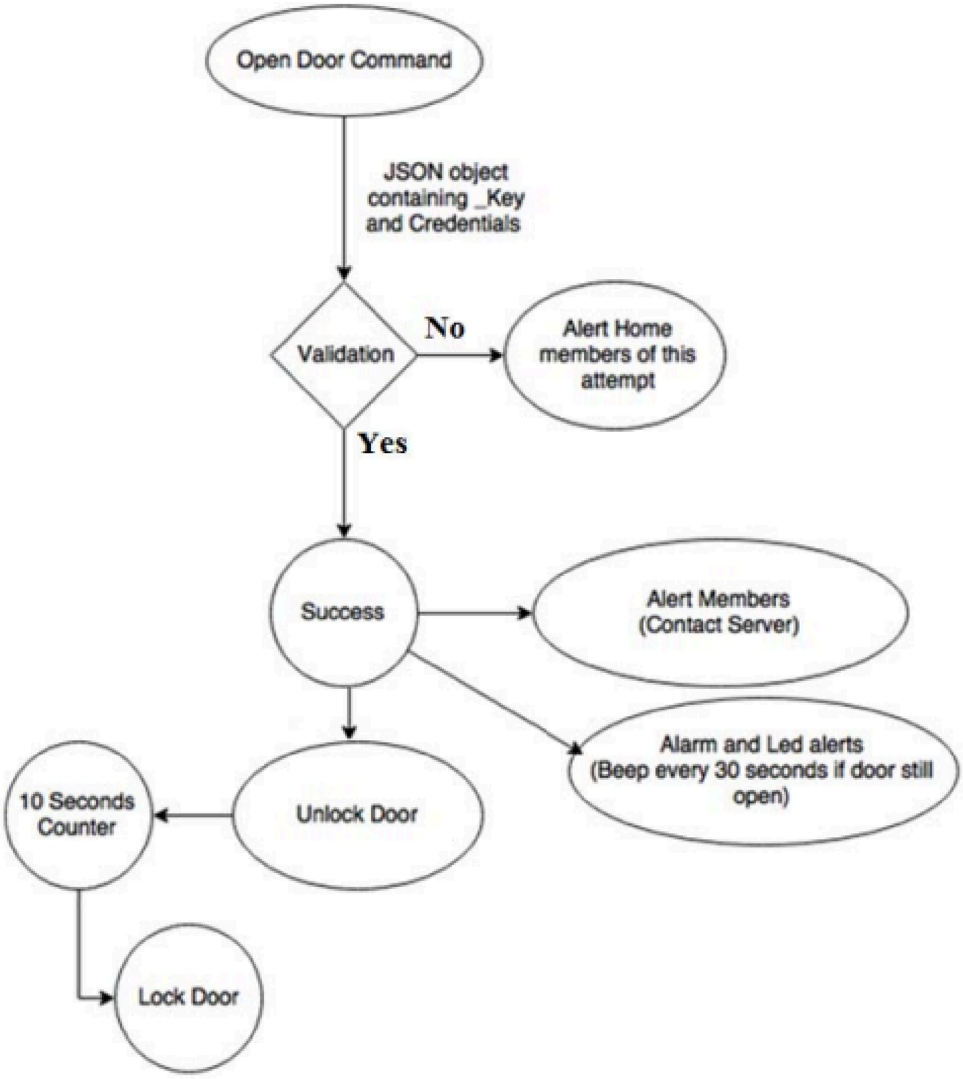
Operation requirements:

- LAN - offered through a router
- Power - offered through ethernet connection (PoE)

System operation

1. Startup
    a. Initialize system - full format cycle to clear memory
    b. Configure ports - full re-initialization of all I/O ports, thus resetting the LED and Buzzer states
    c. Check system - system is checked for security (prevent tampering)
    d. Connect to LAN - attempt to connect to LAN
    e. configure keys - each central control has its own UDID. With this, the generation of a set of accepted keys is done
    f. Main loop - system goes into main loop
2. Main Loop
    a. System waits for user commands and keeps the connection to the router
3. Open door command
    a. User connects to LAN
    b. Command is sent to central control through the app
    c. Central control checks the key validity
    d. If the key is correct, system unlocks the door for 8 seconds
4. Leaving the door open
    If the lock is left open for more than 30s
    a. Beep will sound every 30s
    b. Every 2 minutes, all the people who have the key will be notified through email or text message

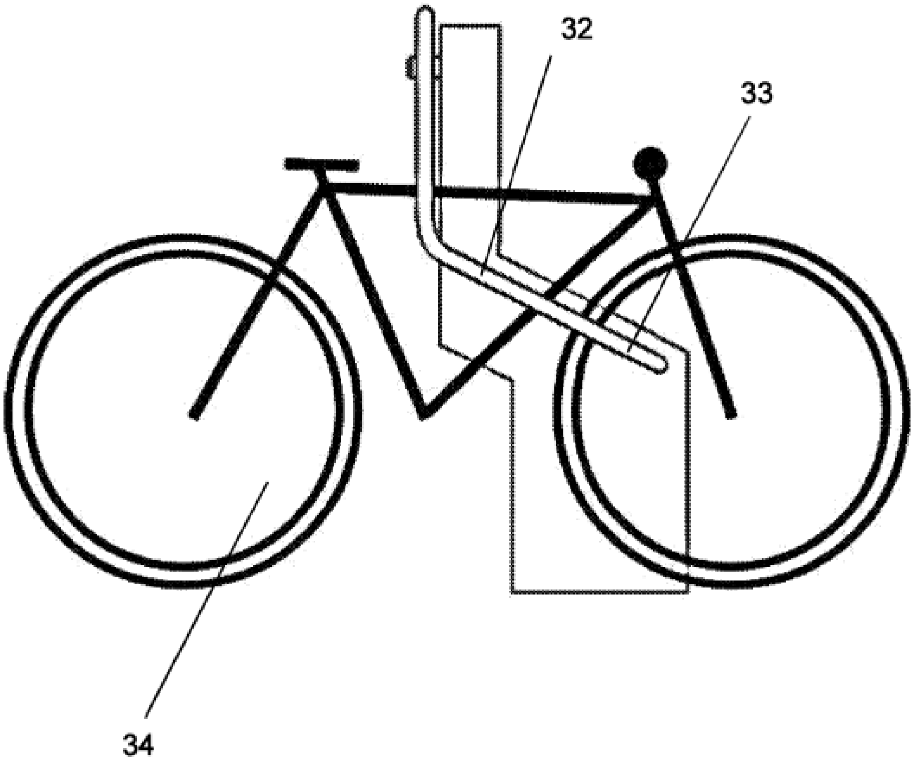
	Offline operation If there is no internet connection, only the people who have the master key (a predefined key in the system and app that cannot be shared) will be able to open the door. **Prevent hacking** The system is completely controlled through the phone, so security is left to the user's phone. The LAN is the next layer of security, but the system's router security will be set to WPA2/PSK with a key of at least 15 characters. This will create an immensely large number of possible keys, which makes it incredibly hard to penetrate the system. Furthermore, the mechanical system is connected to the router through cable, so physical access is needed to tamper with the system. Finally, every key and master key are different with unique UDID patterns, which are generated randomly with timestamps to prevent duplicates. **Conclusion** This system could be used for a variety of different reasons and applications. A system like this really innovates the lock and makes it much easier to use. The system is also easy to install and set up, to make it applicable to so many fields and purposes.
Research Question/Problem/ Need	People use keys all the time, ranging from lockers, to cars, to houses, to dorms. The problem is that there are costs that come with the manufacturing, duplication and distribution of keys, as well as security problems when keys are lost
Important Figures	 Mobile Phone Server on Internet Wifi Electric and mechanical lock Cable Cable Central Control Cable Figure 1. SLS System Architecture **Rough system architecture and what each device would be communicating with**

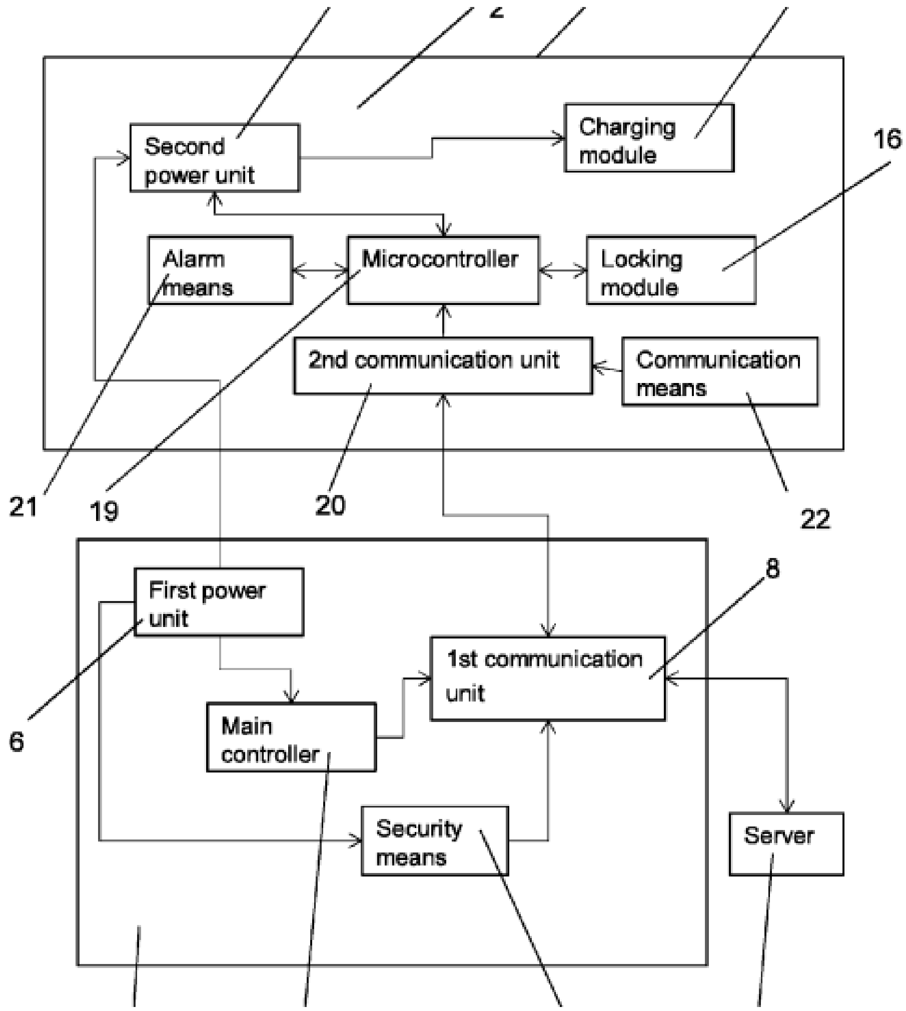
	 Open Door Command JSON object containing _Key and Credentials Validation No Alert Home members of this attempt Yes Success Alert Members (Contact Server) Alarm and Led alerts (Beep every 30 seconds if door still open) Unlock Door 10 Seconds Counter Lock Door **Unlock command pseudocode**
VOCAB: (w/definition)	SLS - smart lock system LAN - local area network - group of devices that share a same internet connection PoE - power over ethernet I/O - input/output UDID - Universal Device identifier WPA2/PSK - Wi-fi protected access 2/pre-shared key - security protocol for wireless networks
Cited references to follow up on	"History". Locks.ru. Retrieved 2016-03-14, website : www.locks.ru/germ/informat/schlagehistory.htm A. Kassem; M. Hamad, C. El Moucary, “A Smart Spirometry Device for Asthma Diagnosis”, 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS), pp. 1629-1632, 2015

	X. Lv and L. Xu, "AES encryption algorithm keyless entry system," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, Yichang, pp. 3090-3093, 2012. Chih-Chung Lu and Shau-Yin Tseng, "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter," ApplicationSpecific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on, pp. 277-285, 2002. Cao Wanpeng and Bi Wei, "Adaptive and dynamic mobile phone data encryption method," in China Communications, vol. 11, no. 1, pp. 103- 109, 2014. C. M. Chen and T. H. Chang, "The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method," Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on, Kaohsiung, pp. 37-41, 2015. S. Goswami, S. Misra and M. Mukesh, "A PKI based timestamped secure signing tool for e-documents," High Performance Computing and Applications (ICHPCA), 2014 International Conference on, Bhubaneswar, pp. 1-6, 2014.
Follow up Questions	Why aren’t the notifications forwarded to the user through the app? Although the system would work during internet shortages, what would happen during power outages? Would it be possible to design a similar system but smaller like school lockers for example?

Patent #1 Notes: System and method for bike locking

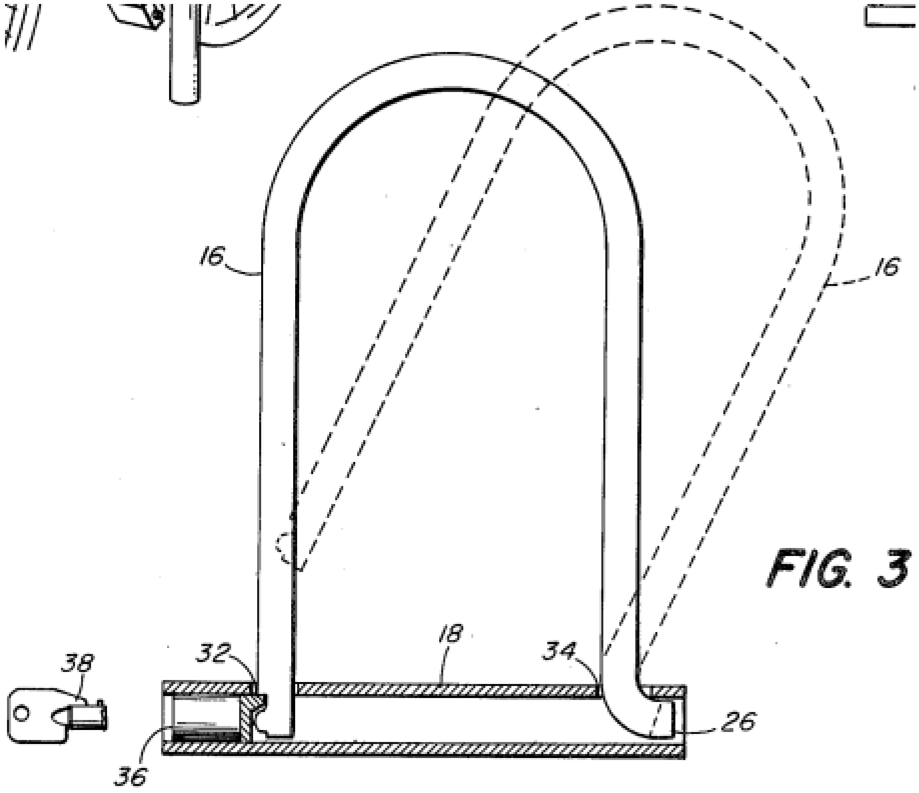
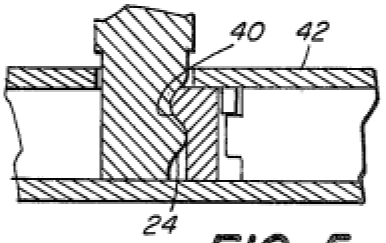
Source Title	System and method for bike locking
Source citation (APA Format)	HAIDAK, M., KÕIV, K., & REINHOLD, O. (2015). System and method for bike locking. United States Patent Application Publication (Patent US20150096335A1). https://patents.google.com/patent/US20150096335A1/en
Original URL	https://patents.google.com/patent/US20150096335A1/en
Source type	Patent
Keywords	Secure locking, bike lock
#Tags	Bicycle lock, Locking
Summary of key points + notes (include methodology)	This project presents an innovation to give a safe and easy to use lock for bicycle riders, in order to secure any type of bicycle by locking the frame and back wheel without the rider needing to carry their own bike lock. Features: - alarm system - sound and light to indicate a free spot for a bicycle - Video recording - Locked bicycles are safe for 24 hours, with 24/7 call support and a network map - Steel bar locked by cell, mobile device, or other contact free - Minimal design allows for optimal space usage ⟶ being able to put it near any building - Charging module (solar panel) ⟶ charge e-bike, scooter, or other electronic device + includes an information and entertainment screen A system to lock bicycles consisting of a main unit; a docking unit, which contains housing, a locking node, a second power unit, a charger node, a microcontroller, a second communication ; a server; a local station server; a way for user identification with the local station server connected to the server, a security system, a docking unit, a locking node, another power unit, a charger node, a microcontroller, another communication node, an alarm system. The microcontroller is connected to the alarm system and locking module. The locking module has a locker, a locker door, a lever, a bearing, and a lock. The first communication node is connected to the main controller, the security system, second communication node, and a wired or wireless network with the server. The second communication node is connected to the microcontroller, the first

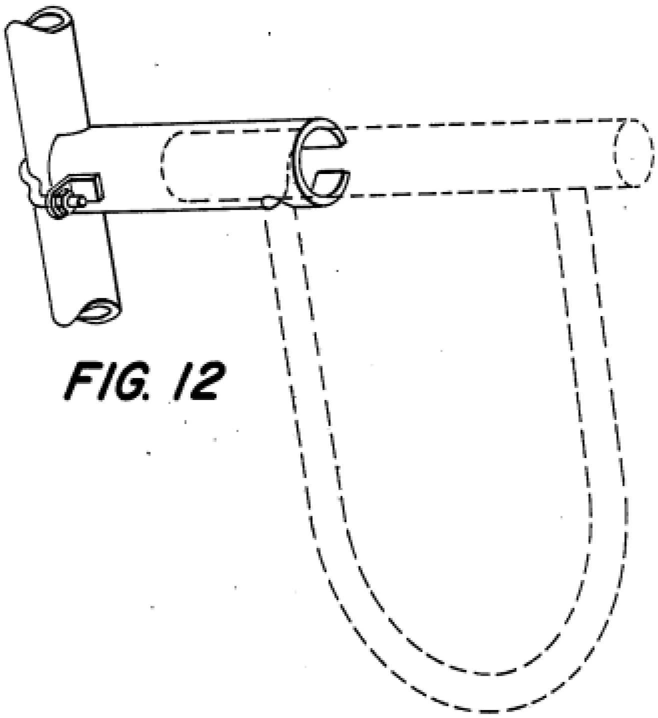
	communication unit, alarm system. The first power unit is connected to the main controller, security system, and the second power unit. The second power unit is connected to the first, the microcontroller, and chagrin system.
Research Question/Problem/ Need	Bicycle locks are small and easily breakable. An alternative to those is using rental bikes systems (city bike locking systems), but these are not suited for personal bicycles
Important Figures	 **Drawing of the design and how it would attach to the bike**

	 2 Second power unit Charging module 16 Alarm means Microcontroller Locking module 2nd communication unit Communication means 21 19 20 22 First power unit 8 1st communication unit 6 Main controller Security means Server **Overview of each part of the system and how they would collaborate**
VOCAB: (w/definition)	Module - part/system
Cited references to follow up on	No references
Follow up Questions	How exactly would this system help with not having enough bike racks? What if the place someone is going does not have this system, but they did not know, so they didn't break their personal bike lock? Is this system really better than personal bike locks?

Patent #2 Notes: Bicycle lock and bracket

Source Title	Bicycle lock and bracket
Source citation (APA Format)	Zane, M. S., & Zane, P. L. (1979). *Bicycle lock and bracket* (Patent US4155231A). https://patents.google.com/patent/US4155231A/en
Original URL	https://patents.google.com/patent/US4155231A/en
Source type	Patent
Keywords	U-lock, bicycle lock, bicycle lock bracket
#Tags	Bicycle lock, locking mechanism,
Summary of key points + notes (include methodology)	This patent provides a U-lock and its mount to secure a bike and be able to travel with the lock. The U lock resembles a U with both lines being parallel, but with one that has a “shoulder” at the end for opening motion. The crossbar has one end adapted to the “shoulder”, and the other with a keyhole to unlock the other side of the lock. The mount for the U-lock which is hollow to put around the bike frame and has an L-shape to hold the lock Because of the increasingly expensive bicycles, there has been an increase in bike thefts. Bicycle thieves often use bolt cutters to cut bike locks. U-locks are the locks that are the most resistant to bolt cutters and hack saws, but they are inconvenient during riding because of their size, weight, and are expensive. This device is a bolt cutter and hacksaw resistant lock, which can be transported more easily. There are 2 main components to the lock: the shackle and the cross piece. Both the shackle and cross piece should be built from thick and treated high-grade steel for optimal security. The bracket to store the lock is made in an L-shape for one side of the L to attach to the bicycle, while the other holds the lock. The lock can be modified (made smaller, larger, or change the unlocking method) for several different uses.
Research Question/Problem/ Need	Bicycle thefts are increasing, and the locks (U-locks) that are most resistant to thieves’ tools are hard to transport and expensive

Important Figures	 FIG. 3 **View of all the parts of the lock and how they would interact.**  FIG. 5 **Detailed view of the locking mechanism**

	 FIG. 12 **View of the mounting bracket and where the lock would go**
VOCAB: (w/definition)	N/A
Cited references to follow up on	63,212 8/1882 Pettibone .... 70/18 410,027 8/1889 Rueckert .... 70/18 1,542,016 6/1925 Stull .... 70/18 X 2,889,451 6/1959 Longo ... 248/314 X 3,739,607 6/1973 Smedley .... 70/18 3,754,418 8/1973 Miller .... 70/18 3,924,426 9/1975 Zane et al. .... 70/18 3,964,706 6/1976 Adams .... , 248/538 X 3,967,475 7/1976 Zane 70/18
Follow up Questions	How did you test this device? Is this actually better than a regular U-lock without a mount? Why is the locking mechanism designed this way?

Patent #3 Notes: Indoor intelligent bluetooth door lock control system based on arduino

Source Title	Indoor intelligent bluetooth door lock control system based on arduino
Source citation (APA Format)	孙亚琼, 汪晨, 武诗博, 魏玲燕, 金磊, & 周华亮. (Yaqiong Sun, Chen Wang, Shibo Wu, Lingyan Wei, Lei Jin, & Hualiang Zhou) (2016). *Indoor intelligent bluetooth door lock control system based on arduino* (Patent CN205476932U). https://patents.google.com/patent/CN205476932U/en
Original URL	https://patents.google.com/patent/CN205476932U/en
Source type	Patent
Keywords	Door lock, Control System, Arduino, Bluetooth template
#Tags	Arduino, Bluetooth, Door Lock
Summary of key points + notes (include methodology)	This paper presents an indoor intelligent Bluetooth door lock based on Arduino. It consists of a cell-phone customer terminal, an Arduino, a bluetooth module, lock body with the motor rotating device, and an electrical power system. Smartphones are continuously evolving and the number of people who have one increases with them. Also, people are more and more protective of their assets but the performance of today's locks and usability do not achieve the title of "modern". IoT is becoming increasingly popular, which can expand to door locks. Smart door locks should be the center of household technology. From an interview conducted, 80% more than 70% think that in the following 35 years, door locks will be unlocked using more modern methods, such as a mobile app, keycard, etc. This proves the demand and need for intelligent door locks. Having a Bluetooth door lock aids in many ways. For example, it prevents people from forgetting their keys and being locked from their house. The purpose of this project was to develop a working and reliable smart door lock system with Bluetooth based on Arduino. Components: ● Arduino - as a microcontroller ● Bluetooth module - for communication ● Motor rotating device - for locking/unlocking ● Power supply - to provide power to the system ● Alarm system - to send emergency messages to local police stations The Arduino and the motors are connected to the power supply. The Bluetooth

	module is connected to the Arduino. The Bluetooth module receives information and verifies it. If it is correct, then the Arduino controls the motors and opens the lock. Further improvements for this system are a multifunctional intellectual customer side, a passcode extension, and a communication system (to get in touch with other users) The benefits of this system are that it can control a door lock using Bluetooth. Also, there is a bell and the system contains a police-contacting system to call the police in a timely manner. Furthermore, using Bluetooth means there are no additional expenses or subscriptions to pay to use this device, it has low-power consumption, and has a variety of prospective applications.
Research Question/Problem/ Need	People need more and more privacy and personal protection of their assets. Current locks do not provide the necessary protection and are not modern enough.
Important Figures	N/A the only figure I could find was in Chinese and there was no way to translate it
VOCAB: (w/definition)	Bluetooth - standard to connect wirelessly computers, phones, tablets, etc. on a short range
Cited references to follow up on	N/A
Follow up Questions	How did you design this system? Did you build the design? If so, what does it look like? Although smartphone usage is increasing, is Bluetooth really the best way to unlock locks? What kind of Arduino, motors, bluetooth module were used? How does the alarm system get engaged?