Secure Wireless Smart Car Door Unlocking System

Technical Answers for Real World Problems (CSE1901)

J COMPONENT PROJECT REPORT

In

B.Tech. Computer Science and Engineering

August, 2022

(Semester 7)

By

Team Members	Reg. No.
Varun Agarwal	19BCT0070
Adarsh Singh	19BCE2284
Shreyas Khan	19BCE2265
Abhinav Gorantla	19BCE0241

Under the guidance of

Dr. Shalini L.

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

DECLARATION

I hereby declare that the thesis entitled “Secure Wireless Smart Car Door Unlocking System" submitted by me, for the award of the degree of the Bachelor of Technology in Computer Science to VIT is a record of bonafide work carried out by me under the supervision of Prof Shalini L. I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place : Vellore

Date: 25-08-2022

Signature of the Candidate

Varun Agarwal

Adarsh Singh

Shreyas Khan

Abhinav Gorantla

CERTIFICATE

This is to certify that the thesis entitled "Secure Wireless Smart Car Door Unlocking System" submitted by Varun Agarwal (19BCT0070), Adarsh Singh (19BCE2284), Shreyas Khan (19BCE2265), Abhinav Gorantla (19BCE0241), SCOPE, VIT, for the award of the degree of Bachelor of Technology in Computer Science, is a record of bonafide work carried out by him / her under my supervision during the Fall 2022 - 23 semester, as per the VIT code of academic and research ethics. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfils the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Place: Vellore

Date: 25-08-2022

Signature of the Guide

TABLE OF CONTENTS

Abstract—The most crucial aspect of software and the internet ecosystem is security. The most crucial aspect of modern asset protection for both our digital and physical assets is software and hardware security. In many instances, physical objects with some IoT base support, such as smart houses, smart cars, etc., improve oversight. In this project, we propose a secure substitute for the car unlocking system that employs cutting-edge communications methods like MAC encryption and a hashing standard to ensure futuristic security while dynamically generating disposable encryption keys to meet the needs of smart cars powered by the Internet of Things in the future. To maintain security, encryption keys are employed to make it easier to lock and unlock a car through the internet.

Keywords—connected cars, internet of vehicles, pseudorandom number, hashing, rolling code

I. INTRODUCTION

The growth of smart cars in the Internet of Vehicles (IoV) is expected to increase from 40% in 2020 to 70% in 2025. The rapid development of infrastructure, systems, and artificial intelligence learning models would cause a significant shift of the consumers from the conventional type of vehicles to a more modern type. This may also bring increased security issues, one of the major concerning issues being the car door unlocking system. IoV vehicles are equipped with a secret key transmitted over the internet to the owner's car, which is also connected to the internet. There are two types of security aspects regarding a car key, i.e., software and hardware security. Software security is the area that deals with securing the data that is being transmitted over the IoT network. Hardware security deals with the inbuilt security system of hardware to prevent any intruder from entering and making the hardware vulnerable. We will be focusing on the software security of the car unlocking system. The car is locked or unlocked when the secret key matches the one stored inside the car. This method may seem very inexpensive and easy for the manufacturers to implement into the system. However, it has a drawback; if an attacker can get inside the network, he can sense any piece of information that is being sent over the internet. If he intends to commit car theft, he can easily read the key and replicate it later to unlock the car. The current methodology of the car door unlocking system compromises its security aspect. Several approaches like symmetric and asymmetric encryption and decryption have been implemented but later discovered that they can easily be cracked with hardware-induced attacks.

II. LITERATURE REVIEW

Paper/Article Name	Author	Proposed Method	Advantages	Drawbacks
[1] REMOVING RF VULNERABILITIES FROM IOT DEVICES	Ray, P., Sultana, H. P., & Ghosh, S. (2019).	Incorporated the rolling key algorithm to overcome the flaws in its predecessor methodologies.	To prevent and overcome the relay threats caused by insecure channels, the rolling key algorithm is implemented, which enables a 2-way handshake. The rolling key algorithm provides an unused key at every instance of data transfer between the sender and receiver.	The signals that pass through these channels are essential for locking and unlocking the system, which brings about a blaring disadvantage in the security standpoint.
[2] Smart and secure	Valanarasu,	Presents a	The method	While the

IoT and AI integration framework for hospital environment.	M. R. (2019).	secure architecture for hospital environments with the help of an Internet of Things backend.	presents a major upgrade from the existing methods by using a regulation and policy layer to overlook all the trust components such as safety, privacy and dependability.	proposed method works in testing, it's not scalable to a real world large-scale model. It also has problems with interoperability.
[3] Cyber-security internals of a Škoda Octavia vRS: A hands-on approach.	Urquhart, C., Bellekens, X., Tachtatzis, C., Atkinson, R., Hindy, H., & Seeam, A. (2019).	Analysing the underlying cybersecurity of a renowned car brand.	It has been noted that as the technology of automobiles advances, many instances of cars being connected via 3G and 4G mobile networks are reported. While these services increase the ease of use and aid the consumer.	It comes with vulnerable system defects due to the underlying core technology that leads to an increase in the attacking area of the vehicle.
[4] A wireless controlled digital car lock for smart	Jamjoom, L., Alshmarani,	Focuses on developing a wireless car	The proposed methodology revolves around	This method relies on Bluetooth technology, which

transportation.	A., Qaisar, S. M., & Akbar, M. (2018, February).	lock controller built on a mobile device. The research implements the said system incorporating Internet of Things concepts.	granting requests through a server-based utility over the internet. To accommodate the authorization, a code is sent to the mobile device. The mobile device must have the companion application pre-installed to complete the communication of the code. The code is transmitted via Bluetooth. It is then sent to a front-end controller which employs recognition techniques and relays a flag back to the mobile device.	is prone to man-in-the-middle attacks, leaving the car lock easily hackable.

[5] Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study.	Auer, S., Nagler, S., Mazumdar, S., & Mukkamala, R. R. (2022).	Using the growing popularity of in-car sharing and the rising number of applications of Blockchain technology as motivation for devising a new methodology for shared mobility that involves key aspects from both its constituents.	The paper presents an architecture for encapsulating these technologies to assist car-leasing and car-sharing. The proposed method goes a step ahead by eliminating the requirement for keys to gain vehicle access	The authors identify that while sustainable, blockchain technology alone cannot expand this field in the future. Future research can aim to evaluate the authenticity of the Internet of Things devices and the scalability of the proposed model. At present, the model fares well for simulated data.
[6] Robust and low-cost solution for preventing sidejacking attacks in wireless networks using a rolling code.	Cashion, J., & Bassiouni, M. (2011, October)	Demonstrates a special method of employing rolling code technology to authenticate the client to the server.	The cost of the protocol is the same for each iteration. Retransmits communications to the user to guard against man-in-the-middle attacks.	High computational complexity is present in the solution. High power platforms are not well suited for the solution.
[7] Timestamp based	Greene, K.,	Carried out a	The algorithm	The method

defence mechanism against replay attack in remote keyless entry systems.	Rodgers, D., Dykhuizen, H., McNeil, K., Niyaz, Q., & Al Shamaileh, K. (2020, January)	series of infiltration experiments that exposed the radio frequency communicatio n flaws in remote keyless systems used in garages and cars. It was suggested to improve the current rolling code process by using timestamps.	demonstrated remarkable levels of security, simplicity, and power efficiency. The authors incorporated a timestamp-based defence mechanism with the rolling-code and assessed security to increase the security of RKE systems.	strongly depends on how quickly the signal needs to be conveyed. Difficulties might arise from a noisy channel or a signal loss.
[8] A wireless controlled digital car lock for smart transportation.	Jamjoom, L., Alshmarani, A., Qaisar, S. M., & Akbar, M. (2018, February)	Develops a wirelessly operated auto lock based on a smartphone. Allowing a large number of individuals with permission to share a lot of automobiles is	The frontend module, the server, and the smartphone all have wireless interfaces that are sent on delta-based and event driven interfaces, which increases the system's	The Bluetooth connection is not supported by the Android device emulator. This makes the suggested technique more complicated.

		the concept. Every time an authorised individual needs a car, they must first submit a request online to a server-based service.	efficiency in terms of resource use and power consumption.	
[9] Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study.	Auer, S., Nagler, S., Mazumdar, S., & Mukkamala, R. R. (2022).	Presents a high-level architecture for a blockchain-IoT-based platform for promoting shared mobility combining car-sharing and car-leasing. The proposed platform requires secure information	Traceability (including dependability), security (including privacy), and scalability are all provided with a clear trade-off.	The issue for the relevant stakeholders is to strike the right balance between maintaining and reducing the need for trust as well as determining the proper degree between holding on to and ceding control of data and processes while simultaneously assuring the system's scalability.

		sharing among multiple stakeholders (such as user, lessee, and service provider), leading to the decision to choose blockchain for its facilitation.		
[10] Pseudorandom numbers.	Lagarias, J. C. (1993).	Addresses the issue of producing pseudorandom numbers and provides a comprehensive list of known pseudorandom bit structures.	Applications where several random numbers are needed and where it is advantageous to readily repeat the same sequence are suited for Pseudo Random Number Generators.	Pseudorandom numbers' fundamental flaw is that computers can't rely on luck. To execute and finish tasks, they need a set of instructions.
[11] An Attempt to Develop an IOT based Vehicle Security System	Mukhopadhyay, D., Gupta, M., Attar, T., Chavan, P.,	Proposes a novel method which uses GSM technology.	Using GSM instead of 4G technology ensures that even in the absence of	SMS is a very old technology. IR sensors can be manipulated easily and the bluetooth

	& Patel, V.	Their solution alerts the user through an SMS message whenever a case of unauthorised access, theft, intrusion or towing is detected. They have used an IR sensor to detect any possibilities of theft through the windows, a limit switch which sends a signal whenever the car is about to be towed, a bluetooth module for the connection between microcontrolle r and dashboard	the internet, the user remains informed on their phone through SMS. This ensures that even when the user has a minimal cellular network, they can still remain updated.	networks between the different sensors and the microcontroller can be easily scrambled which can send the user some false alarms.

		module and finally a mobile application on the users' mobile through which they can remain updated.		
[13] Comparative analysis of different techniques of encryption for secure data transmission	Mota, A. V., Azam, S., Shanmugam, B., Yeo, K. C., & Kannoorpatti, K.	This paper compares some commonly used hashing algorithms like AES, DES, 3DES with comparison parameters like encryption time, decryption time, memory usage, power consumption, latency, jitter and their	This paper provides extensive research and comparison on various encryption and hashing algorithms. They have used numerous comparison criteria for this purpose. This helped us choose the best hashing algorithm to use in our project.	Does not compare these algorithms in the radio communication scenario.

		security level. After performing various tests, they have concluded that Blowfish is best in all of these parameters in general and RSA ECC is better than elgamal in almost all aspects apart from signature verification time. It was also found out that SHA256 is more secure than SHA1 and MD5 hashing algorithms.		
[14] Relay Attacks on Passive Keyless Entry and Start Systems in Modern	Francillon, A., Danev, B., & Capkun, S.	This paper demonstrates how passive keyless entry	They have performed an extensive evaluation of the	No analysis on digital PKES signals is available, hence

Cars		systems (PKES) can be easily hacked using relay attacks. In this work, the researchers designed and implemented relay attacks i n the analog domain. Their attack does not interpret or modify the signal from the car key. This relay attack methodology proposed here is very effective against PKES systems employing string cryptography like AES, RSA, etc.	relay attack on 10 car models from 8 manufacturers.	we cannot comment on the efficacy of these attacks on vehicles on using a PKES with digital signals.

[15] IoT based embedded system for vehicle security and driver surveillance	Pawar, M. R., & Rizvi, I.	In this paper, the researchers have used a microprocessor board, raspberry pi, a high resolution camera and open source software to ensure vehicle security and also check if the driver is safely driving the vehicle. In case of any violation, an alert was sent through an email message from the microprocessor board.	Use of open source software and documentation makes the device accessible to everyone and for a very low cost.	Uses very old GSM technology to send messages to the user.
[16] A review of pseudorandom number generators	James, F	In this paper, the authors show while pseudorandom number	Pre generated seed which changes every time to cause more	Old generative functions are compared and newer functions are available

		generators are calculated using a deterministic function, it is necessary for the sequence to show approximate characteristics of a true random distribution.	randomness	
[17] Wireless attacks on automotive remote keyless entry systems	Oswald, D. F	Authors show that rolling codes essentially transmit a counter that is incremented by each button press in a cryptographically authenticated way.	Protects from common keyless attacks like replay attacks.	Rolling code can be broken by intercepting the communication channel.
[18] Lock It and Still Lose It— on the ({In) Security} of	Garcia, F. D., Oswald, D., Kasper	Authors show how rolling codes have	Lightweight disposable key generation	Heavily studied technique which has been analysed

Automotive Remote Keyless Entry Systems		been incorporated into many keyless entry doors unlocking systems due to its extreme versatility and lightweight nature.	technique which is standardised throughout the world	by experts throughout the world which makes it extremely vulnerable
[19] A new remote keyless entry system resistant to power analysis attacks.	Moradi, A., & Kasper, T	Authors show that introducing a pseudorandom number generator into the rolling code can help extend the protection to prevent template attacks as well as alleviate the risks posed by brute force attacks.	Significant Improvement can be noticed when pseudorandom number generators are introduced.	Old techniques are studied which have been outclassed already.
[20] A systematic	Tang, J., &	Authors show	Generating a	Decrypting a hash

review on minwise hashing algorithms. Annals of Data Science.	Tian, Y	that it is computationally easy to calculate the hash of any given message when compared to asymmetric and symmetric key algorithms. Furthermore, two different messages cannot be associated with the same hash. Subsequently, messages cannot be altered without changing the hash.	message from a given hash is very unfeasible, thus nearly eliminating brute force attacks.	is impossible, hence making it useless as an encryption method for communication.

III. PROPOSED METHOD

We present a novel approach by combining the power of the tried and tested state-of-the-art algorithms designed to work in a simplex communication environment and ultra-modern hashing technologies.

This enables us to encrypt any data irreversibly, making communication extremely secure. Our proposed method employs a rolling filter as a key generation method for a modified MAC-and-Encrypt authenticated encryption algorithm. Instead of using a bidirectional encryption algorithm in the final stage of MAC and Encrypt, we are employing another (different from key hash) hashing algorithm, which makes the encrypted message doubly hashed and impossible to crack.

We can employ a double hashing and a unidirectional approach because the message is predefined in both systems, and we only need to authorise the source of the messages.

IV. MODULE DESCRIPTION

The proposed method is divided into two modules. The first one is the client/key side, and the second one is the car side. The client will be interchangeably used as a key since the client is the key in the proposed framework. The client will try to lock or unlock the car from their remote device connected through the internet. Connected cars are always connected to the internet. The car will be listening for a hash digest over the internet. Once it receives the digest, the car will validate and verify the authenticity to decide on the car controls.

Certain assumptions made in the following 2-way handshake system include initialising a seed before the client and car are made public. This seed will be completely random, and the same seed must be set in both the car and the client. This is essential because the entire architecture of Pseudorandom number generated rolling codes is dependent on this. Furthermore, if the client-side rolling code queue goes out of sync with the car rolling code queue, a manual reset must be performed with the initialisation of a new random seed.

a. Key Side

The key will generate a rolling code queue with the initialised seed. Upon pressing the car control button, such as locking or unlocking, the client then polls the queue and hashes the polled pseudorandom number. Depending on the car control button, the corresponding code will be appended to the newly generated hash digest. After appending the code, the entire message is now hashed again to protect the car's status from being compromised in the case of a man-in-the-middle attack. The architecture followed here is an indirect implementation of the MAC-then-Encrypt scheme where a MAC is produced based on the plaintext, and the plaintext and MAC are encrypted again to produce a ciphertext based on both. While the ciphertext is sent, the resulting hash digest is sent to the car in the proposed system.

The key side has to perform hashing twice for every button click, and given the computational prowess of modern-day machines, the given model feels viable. On the off chance that the key is not connected to the car side, the counter of the rolling code will keep getting incremented until a point where the car queue will not be able to look ahead and get back in sync. When a hacker impersonates a client and sends repeated signals to the car, a Denial-of-Service prevention mechanism depends on the number of false signals being sent in a given amount of time.

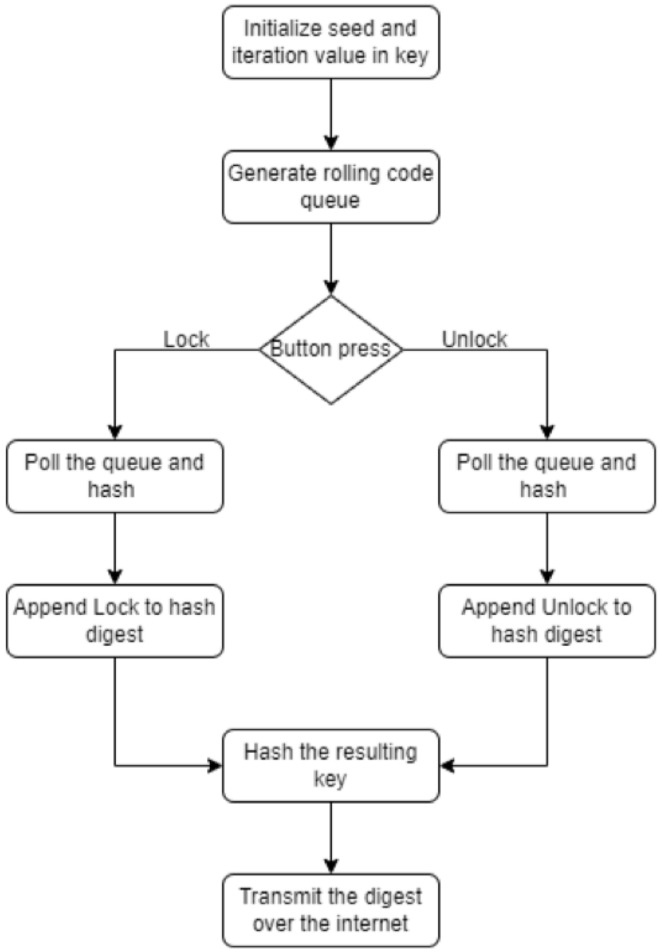

Figure 1. Flowchart for client side

From Figure 1, we can see that the double-hashed message sent over the internet is secure. It is to be noted that the client side does not perform any validation or verification of the person pressing the button. This is analogous to a traditional key, where nobody can verify if it is the key owner opening the lock. Apart from the two hashes and the appending of the car control signal, the client side does not perform any other computations. The same flowchart is given in the form of words in Pseudocode 1.

1. *Initialise queue rq.*
2. *Populate rq.*
3. *If button_press is true:*
    a. *rq.top → temp*

b. *rq.pop*
c. *hash(temp) → temp*
d. *temp + "LOCK" / "UNLOCK" → temp*
e. *hash(temp) → temp*
f. *Transmit.*

Pseudocode 1. Client-side pseudocode

b. Car Side

The car side algorithm is relatively trivial as compared to the key side. Like the key, the car will also be fitted with the same randomly generated seed. The car generates the same pseudorandom numbers and will listen for any message sent over the internet.

Upon receiving the message, the car checks whether the queue is empty. Queue being empty is an edge case for when the car and key go out of sync. If the queue is empty, the car and key must be manually reset with a brand-new seed. Until then, the internet functionalities would be restricted in the car to prevent future attacks as the car is now vulnerable. If the queue is not empty, the car then polls the queue and subjects it to the same hashing system to generate a hash digest.

As mentioned earlier, hashes cannot be decrypted, but they can only be compared with other hash digests to check their validity. Consequently, each number from the queue would have to be hashed and then appended with each control signal/code of the car (Lock or unlock) and then hashed again.

The resulting hash digest will be compared with the message sent over the internet. If they are a match, the car will execute the corresponding control, and if they are not, the car moves ahead until the entire queue is tested. The ideal rolling code queue size is 256, which would take precisely 256 out-of-sync clicks from the key side to restrict the car's internet activity and make it available only for physical locking/unlocking.

From Figure 2 below, we can see that the car actively listens for a message, and upon receiving the message, it validates the hash digest by subjecting the rolling code queue to the same hash functions in the same order. For each number, the car will have to perform one standard hash with the addition of 2 hashes after appending the respective car control signal (lock or unlock) to the intermediate hash digest. The same can be seen with the following pseudocode.

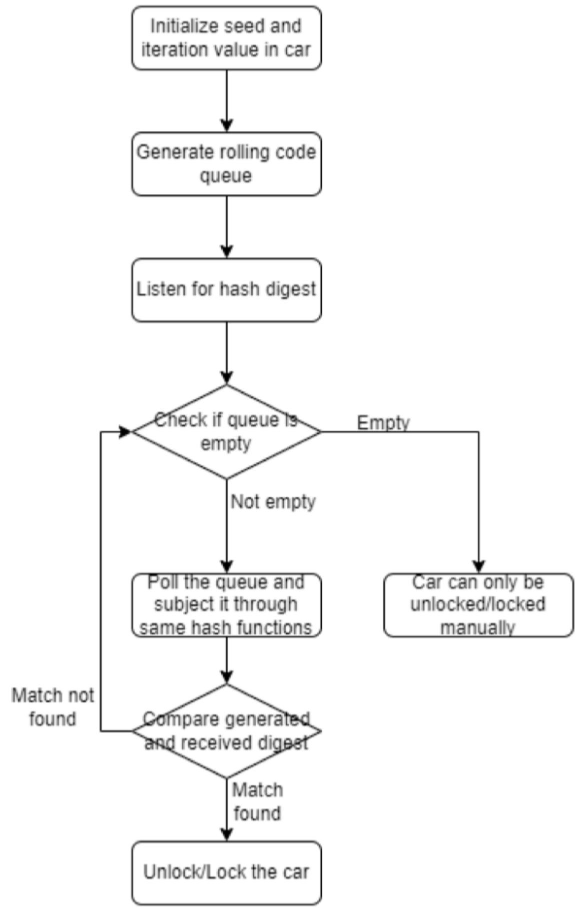

Figure 2. Flowchart for car side

1. *Initialise queue rq.*
2. *Populate rq.*
3. *Initialise TCP socket.*
4. *Receive 256 bits of data → d*
5. *for each num in rq:*
    a. *hash(num) → temp*
    b. *if temp == d:*
        i. *Lock or Unlock the car.*
6. *if no match found:*
    a. *Restrict car's activities over the internet.*

Pseudocode 2. Car-side pseudocode

V. PERFORMANCE EVALUATION

A. Type

In the proposed model, the encryption function is a hash digest, and the decryption function is a hash comparison. Hence making the program extremely secure towards brute force attacks.

B. Function Analysis

We use SHA256 for hashing, rolling code for disposable key generation and finally, a MAC and encrypt architecture for network authentication.

This sequential model involves using multiple tried and tested models, which theoretically yields a non-brute enforceable encryption standard at the cost of computational power while maintaining the integrity of the data.

C. Key Side

Our proposed model uses a random number generator which yields a key of 10^8, which can be increased depending on the computational power available. However, since the final output is hashed, the output is always a fixed size of 256 bits.

D. Rounds

The proposed model hashes in 2 rounds and ensures maximum encryption.

E. Time Complexity

The time complexity for each encryption/digest is,

$$\Sigma = T(n) = 2*({}^{29}C_1 + {}^{4}C_2)\, N_0 + 2*({}^{10140}C_1 + {}^{2}C_3 + {}^{64}C_4 + {}^{2}C_5)\, N_1 = \Theta(N) \tag{1}$$

We can clearly observe that the encryption function is linear in time and hence can provide great benefits while not compromising on quality of the hash digest. This encryption function is running a total of k times. Hence the total time complexity for the embedded system in the car is Θ (l*N). However, once the queue is generated, the time complexity reduces to Θ (N) and the time complexity to check becomes Θ (l*k*256) = Θ (l*k). Where k represents the queue length and l represents the number of functions. While the complexity of the sender / client is Θ (n).

F. Space Complexity

For the car side,

$$\sum = S(n) = l*k*(256) = l*k \tag{2}$$

Here k is the cycles, and l is the number of functions. Increasing the number of cycles will increase the space complexity. However, the space complexity is linear and hence does not have a considerable effect and can easily be scaled.

On the car side, the space complexity is a mere Θ (1) and hence does not need to be bothered.

G. Common Attacks

1. **Brute Force:** Brute force attacks are practically impossible since the hash digest is hashed again with a disposable key.
2. **Replay Attacks:** Replay attacks are impossible because the rolling code produces a new key that cannot be reused every cycle.
3. **Rolling Code Overflow:** Rolling code overflow is a common issue in systems employing rolling code. We try to minimise it with the help of a failsafe that blocks failed IP addresses; however, this is not a full-proof method to solve this issue.
4. **DoS Attacks:** DoS attacks can quickly be addressed by employing a simple software firewall / IPS, but it can lead to not being able to open the door over the internet.

H. Common Attacks

1. **Architecture:** Both DSA and our architecture employ mac and encrypt architecture for their base. However, the message is visible in the Digital Signature Algorithm and it is extremely prone to replay attacks.
2. **Key:** The key size in the rolling code is variable and the keys are disposable. Thus, they constantly change.
3. **Rounds:** Both DSA and our algorithm employ the same number of rounds.
4. **Time Complexity:** DSA wins in this comparison metric. DSA is Θ (k*l) times faster; however since the values of k and l are relatively small, it can be considered that DSA is constant time faster than our proposed work.
5. **Space Complexity:** Both the algorithms are similar in terms of space complexity.

I. Usage of SHA vs MD5 in Proposed Method

SHA	**MD5**

Highly Secure as the final output is 256 / 512 bits.	Exponentially less secure as the final output is only 128 bits.
Half as fast as MD5.	Double the speed of SHA.
No known attacks.	Many reported attacks are known.
Fixed input size.	Any input size works.

Table 1: Comparison of SHA and MD5

From Table 1, it is evident that SHA outperforms the MD5 hashing technique in the department of security. While SHA is more time consuming, it is not slow enough to overlook the security benefits it provides.

J. Proposed Method vs DSA

Proposed Method	DSA
Based on Mac and Encrypt architecture.	Based on Mac and Encrypt architecture.
Slower compared to DSA.	Faster than the proposed method.

Highly secure.	Less secure.
Replay attacks don't work.	Susceptible to common replay attacks.
New disposable key every cycle.	Fixed key.

Table 2: Proposed method vs DSA

From Table 2, we can observe that the proposed method performs better than DSA in the security aspect. On the contrary, it lacks speed in comparison to DSA.

VI. RESULTS AND EVALUATION

Regardless of the key side, the server or the car side creates a socket connection with the internet, which receives the lock and unlock signals. This indicates that it is capable of receiving all signals. The IPv4 address for the car side is 192.168.137.1.

Figure 3: Key side

The key side or client side of the connection is made to the same network. Thus, it transfers everything to the aforementioned IPv4 address as a result. Based on the user's signal to unlock or lock, the key transmits an encoded hash digest. The user can choose option 1 (lock) or option 2 (unlock), as indicated in Figure 4, depending on their requirements.

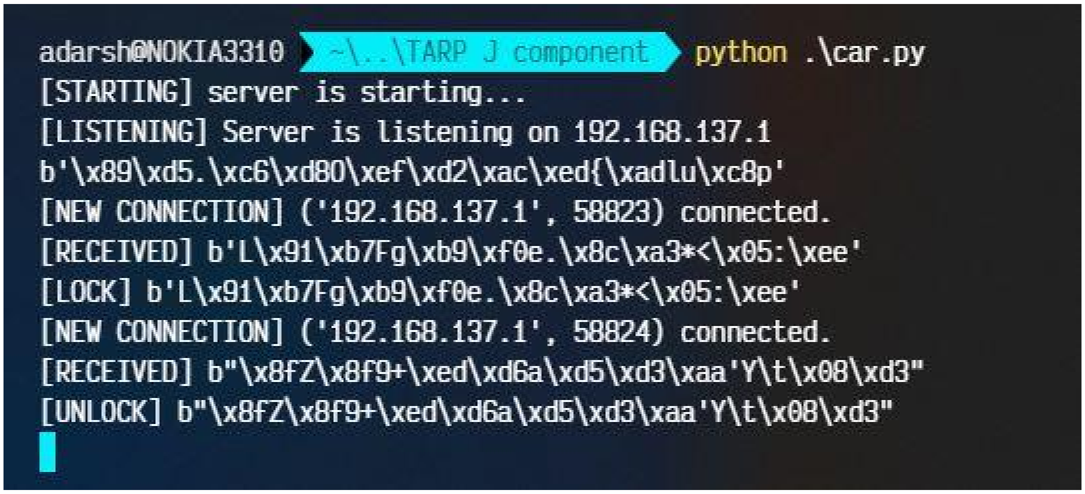

Figure 4: Car side

The car checks to see if the stream of bytes it has received is valid before proceeding. Following deduction, it either locks, unlocks, or stays in the same state. Figure 3 illustrates how it either unlocks or locks the automobile in response to a valid signal. However, when it gets an erroneous signal, it doesn't change its state; instead, it just flushes the signal out of the cache storage.

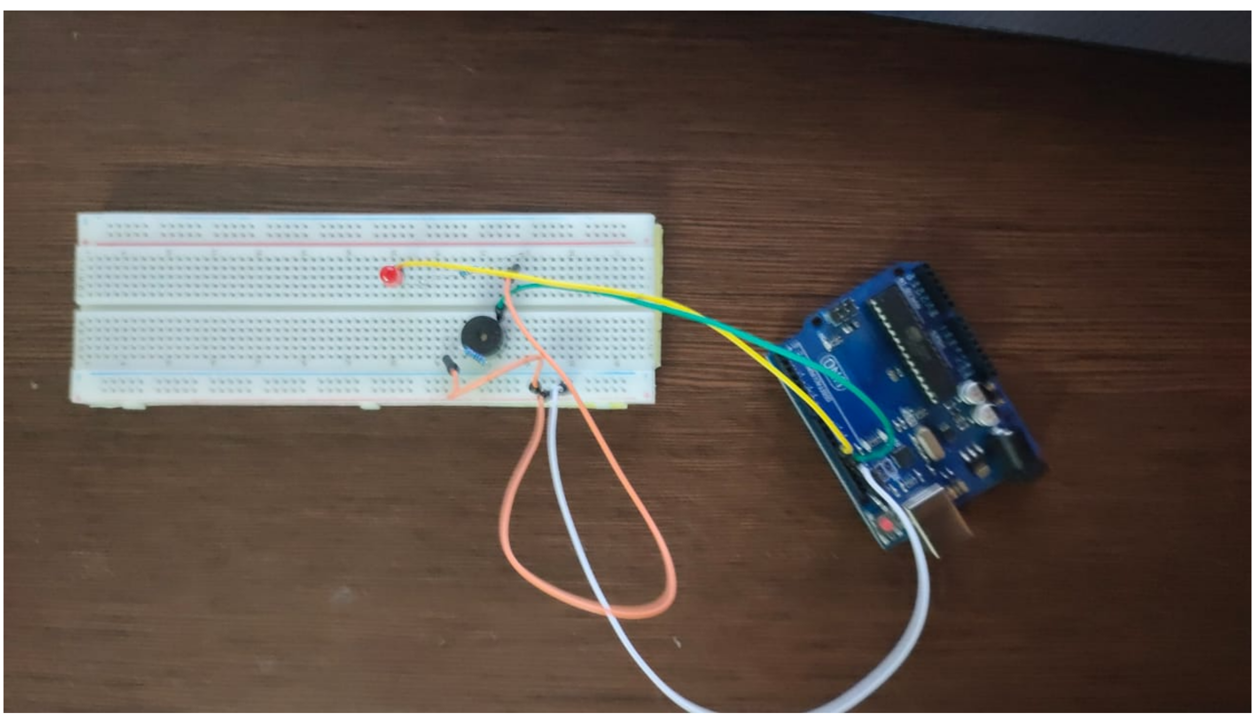

Figure 5: Simulation using Arduino board

VII. REFERENCES

[1] Ray, P., Sultana, H. P., & Ghosh, S. (2019). REMOVING RF VULNERABILITIES FROM IOT DEVICES. Procedia Computer Science, 165, 421-427.

[2] Valanarasu, M. R. (2019). Smart and secure IoT and AI integration framework for hospital environment. Journal of ISMAC, 1(03), 172-179.

[3] Urquhart, C., Bellekens, X., Tachtatzis, C., Atkinson, R., Hindy, H., & Seeam, A. (2019). Cyber-security internals of a skoda octavia vRS: A hands on approach. IEEE Access, 7, 146057-146069.

[4] Jamjoom, L., Alshmarani, A., Qaisar, S. M., & Akbar, M. (2018, February). A wireless controlled digital car lock for smart transportation. In 2018 15th Learning and Technology Conference (L&T) (pp. 46-51). IEEE.

[5] Auer, S., Nagler, S., Mazumdar, S., & Mukkamala, R. R. (2022). Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study. Journal of Network and Computer Applications, 103316.

[6] Cashion, J., & Bassiouni, M. (2011, October). Robust and low-cost solution for preventing sidejacking attacks in wireless networks using a rolling code. In Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks (pp. 21-26).

[7] Greene, K., Rodgers, D., Dykhuizen, H., McNeil, K., Niyaz, Q., & Al Shamaileh, K. (2020, January). Timestamp-based defense mechanism against replay attack in remote keyless entry systems. In 2020 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-4). IEEE.

[8] Jamjoom, L., Alshmarani, A., Qaisar, S. M., & Akbar, M. (2018, February). A wireless controlled digital car lock for smart transportation. In 2018 15th Learning and Technology Conference (L&T) (pp. 46-51). IEEE.

[9] Auer, S., Nagler, S., Mazumdar, S., & Mukkamala, R. R. (2022). Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study. Journal of Network and Computer Applications, 103316.

[10] Lagarias, J. C. (1993). Pseudorandom numbers. Statistical Science, 8(1), 31-39.

[11] Mukhopadhyay, D., Gupta, M., Attar, T., Chavan, P., & Patel, V. (2018, December). An attempt to develop an IOT based vehicle security system. In 2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS) (pp. 195-198). IEEE.

[12] Liu, Z., Zhang, A., & Li, S. (2013, July). Vehicle anti-theft tracking system based on Internet of things. In Proceedings of 2013 IEEE International Conference on Vehicular Electronics and Safety (pp. 48-52). IEEE.

[13] Mota, A. V., Azam, S., Shanmugam, B., Yeo, K. C., & Kannoorpatti, K. (2017, September). Comparative analysis of different techniques of encryption for secured data transmission. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 231-237). IEEE.

[14] Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS). Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

[15] Pawar, M. R., & Rizvi, I. (2018, April). IoT based embedded system for vehicle security and driver surveillance. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 466-470). IEEE.

[16] James, F. (1990). A review of pseudorandom number generators. Computer physics communications, 60(3), 329-344.

[17] Oswald, D. F. (2016, October). Wireless attacks on automotive remote keyless entry systems. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (pp. 43-44).s

[18] Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). Lock It and Still Lose It— on the ({In) Security} of Automotive Remote Keyless Entry Systems. In 25th USENIX Security Symposium (USENIX Security 16).

[19] Moradi, A., & Kasper, T. (2009, December). A new remote keyless entry system resistant to power analysis attacks. In 2009 7th International Conference on Information, Communications and Signal Processing (ICICS) (pp. 1-6). IEEE.

[20] Tang, J., & Tian, Y. (2016). A systematic review on minwise hashing algorithms. Annals of Data Science, 3(4), 445-468.