IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133101

Using ML Models and IOT to Secure Smart Vehicles from Relay Attacks

Kumar Madar [1], Sweedal Flora Dmello[2], Yashwanth S[3], Anusha [4],

Mr. Vijayananda V Madlur[5]

Student, Dept. Of Computer Science and Engineering, Mangalore Institute of Technology & Engineering, Moodabidri, India[1-4]

Associate Professor, Dept. of Computer Science and Engineering, Mangalore Institute of Technology & Engineering, Moodabidri, India[5]

Abstract: This introduces an innovative approach to enhancing the security of smart vehicles by combining Machine Learning (ML) and the Internet of Things (IoT). The system utilizes IoT sensors to collect real-time data from the vehicle's environment and keyless entry system, which is then analyzed using ML algorithms to detect anomalies and potential relay attacks. To strengthen security, the system incorporates multi-factor authentication with biometric recognition such as fingerprint and facial recognition. Continuous learning and adaptation mechanisms ensure the system remains resilient to evolving threats, offering a robust defense against cyberattacks in smart vehicle environments. Through experimentation and validation, the system demonstrates its efficacy in accurately identifying and mitigating security threats, making it suitable for integration into existing automotive security frameworks.

Keywords: Keywords for securing smart vehicles from Relay attacks include IoT sensors, machine learning models, real-time monitoring, response mechanisms, Relay attacks, smart vehicles, security, detection, adaptability, resilience, continuous improvement, cyber threats, transportation, and digital age.

I. INTRODUCTION

The advancement of smart transportation has significantly increased efficiency through the integration of smart technology, computer systems, networks, and global communication enhancements. However, this progress has also brought about a higher risk of cyberattacks targeting modern vehicles. Cybercriminals now require specialized tools, skills, resources, and financial backing to carry out sophisticated attacks, often operating clandestinely and honing their abilities in secret. Smart cars are particularly vulnerable due to potential weaknesses in their hardware, software, and data infrastructure. To mitigate this risk, our study focuses on leveraging smart computer programs to detect cyberattacks, with a specific emphasis on relay attacks that can cause substantial harm. By combining IoT, cybersecurity, and AI principles, our detection system learns from extensive datasets comprising various attack scenarios and distances, effectively identifying threats such as the Man in the Middle (MITM) and replay attacks. The culmination of these efforts will result in a hardware model that showcases our project's capabilities in enhancing the safety and security of smart cars, thus contributing to a more resilient and protected transportation ecosystem.

II. LITERATURE SURVEY

[1] A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays. Khaw, YM, Jahromi, AA, Arani, MFM et al, A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays, IEEE Transactions on Smart 2020 This paper presented a deep-learning-based cyberattack detection system for transmission line protective relays and different possible attack scenarios. This paper used a Novel Deep learningbased cyberattack detection system that includes an autoencoder method.

[2] Securing smart vehicles from relay attacks using machine learning. Usman Ahmad, Hong Song, Awais Bilal1, Mamoun Alazab2, Alireza Jolfaei Securing smart vehicles from relay attacks using machine learning: April 2020. This paper proposed a relay attack detection method by making use of a CART algorithm that uses seven security features for profiling normal key fob messages. The proposed algorithm can identify the legitimate drivers using three driving features and an LSTM recurrent neural network and comparison of CART algorithm with SVM and KNN learning algorithms is done.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133101

III. SCOPE AND METHODOLOGY

Scope

The aim of this project is to make smart cars safer from a sneaky kind of attack called a relay attack. We want to stop bad guys from tricking the car into unlocking without the owner knowing. To do this, we're using smart technology like Machine Learning and IoT sensors. These will help us spot when something suspicious is happening and stop it before any harm is done. We'll test our solution to make sure it works well, and we'll make sure it can work with different kinds of smart cars. We also want to teach people about this threat and how to protect themselves. Overall, our goal is to make smart cars more secure and give people peace of mind knowing their vehicles are better protected from these kinds of attacks.

Methodology

The methodology for safeguarding smart vehicles from Relay attacks entails initial data gathering from IoT sensors, followed by the training of ML models to recognize attack patterns. Real-time monitoring systems are then implemented, coupled with alerting mechanisms to notify users of suspicious activities. Additionally, response mechanisms such as disabling vehicle ignition are integrated to thwart potential attacks swiftly. Rigorous testing is conducted across diverse scenarios to validate the system's efficacy and resilience. Continuous improvement strategies are employed based on feedback and evolving cyber threats to maintain a high level of security for smart vehicles.

IV. SYSTEM ARCHITECTURE

The system architecture for securing smart vehicles from relay attacks using ML models and IoT with a face recognition model in Python comprises several key components. Firstly, IoT devices such as cameras and sensors are deployed in the vehicle to capture real-time data. This data is then fed into the ML model, specifically the face recognition algorithm, which analyzes and verifies the identity of individuals attempting to access the vehicle. The ML model's output is integrated with the vehicle's security system, allowing authorized users to unlock the vehicle only after successful face recognition authentication. Additionally, the system includes secure communication protocols between the IoT devices, ML model, and vehicle security system to prevent unauthorized access and ensure data privacy. Overall, this architecture provides a robust and intelligent solution for safeguarding smart vehicles against relay attacks using advanced ML and IoT technologies.

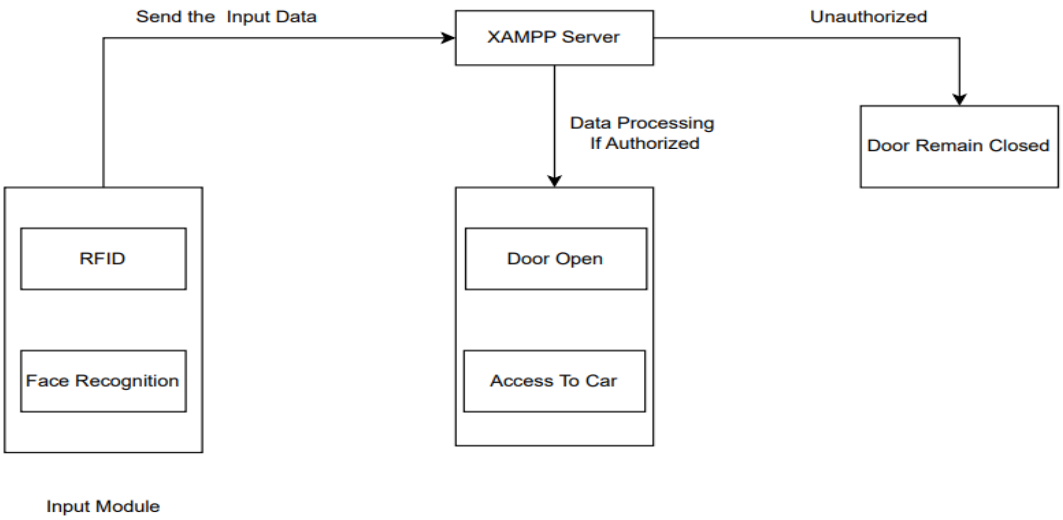

Fig.1 System architecture

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133101

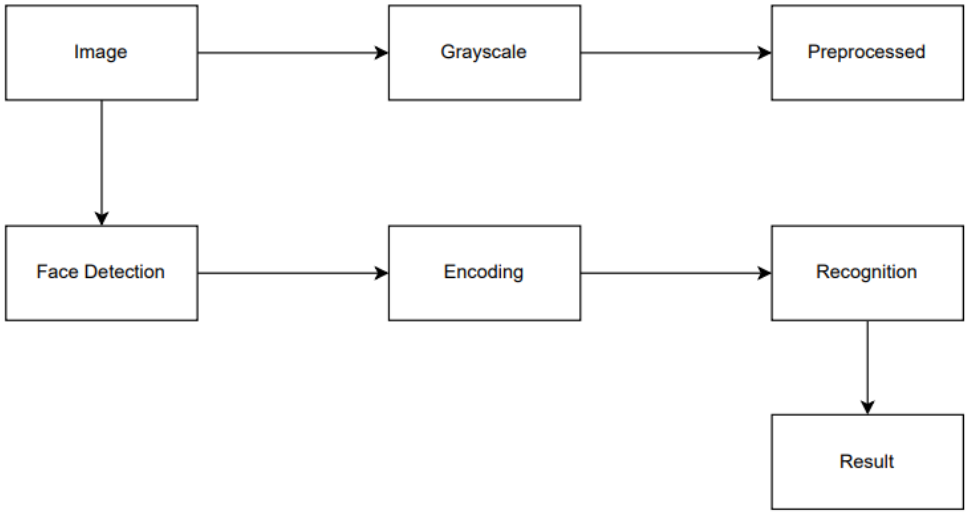

Fig.2 Activity diagram

V. CONCLUSION

In conclusion, the proposed system architecture leveraging IoT sensors, machine learning models, real-time monitoring systems, and response mechanisms represents a robust and proactive approach to mitigating Relay attacks on smart vehicles. By combining these elements, the system can detect and respond to suspicious activities swiftly, enhancing the overall security posture of smart vehicle ecosystems. The integration of continuous improvement strategies based on feedback and evolving threats ensures that the system remains adaptable and resilient over time. Ultimately, this comprehensive approach aims to safeguard smart vehicles and their users from potential cyber threats, contributing to a safer and more reliable transportation environment in the digital age.

REFERENCES

[1]. Qinyi Xu; Beibei Wang; Feng Zhang; Deepika Sai Regani; Fengyu Wang; K. J. Ray Liu, Wireless AI in Smart Car: How Smart a Car Can Be? USA, 05 March 2020, IEEE.

[2]. Syed Rizvi, Jarrett Imler, Luke Ritchey and Michael Tokar, Securing PKES against Relay Attacks using Coordinate Tracing and Multi-Factor Authentication, Department of Information Sciences and Technology Pennsylvania State University Altoona PA USA, 18 April 2019

[3]. Khaw, YM, Jahromi, AA, Arani, MFM et al, A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays, IEEE Transactions on Smart Grid:2020.

[4]. Usman Ahmad, Hong Song, Awais Bilal1, Mamoun Alazab2, Alireza Jolfaei Securing smart vehicles from relay attacks using machine learning: April 2020.

[5]. A. Wang, “Internet of Things Computer Network Security and Remote-Control Technology Application,” 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICM CCE),2020, pp.1814-1817, doi:10.1109/ICMCCE51767.2020.00398.