صفحات ۹ تا ۱۳

Enhancing Security in Smart Vehicles: the Role and Application of Artificial Intelligence

Amirreza Atarian[1], Milad Davoodifar[2], Abolfazl Omidi[3]

[1]Bachelor Student of Computer Engineering, Majoring in Artificial Intelligence, PolDokhtar Higher Education Institute, Lorestan University, atarianamirreza@gmail.com

[2]Bachelor Student of Computer Engineering, Majoring in Artificial Intelligence, PolDokhtar Higher Education Institute, Lorestan University, miladdavoodifar1380@gmail.com

[3]Bachelor Student of Computer Engineering, Majoring in Artificial Intelligence, PolDokhtar Higher Education Institute, Lorestan University, abolfazl.omidi.1380.1@gmail.com

Abstract

This Article explores the growing threat of theft in smart vehicles and proposes Artificial Intelligence (AI) as a formidable solution to enhance their security. Despite the numerous benefits of smart vehicles, they present new challenges in terms of security and theft prevention. With increasing sophistication of thieves, it is critical to address these vulnerabilities and develop robust security measures. AI, with its ability to mimic human intelligence and learn from data, can be harnessed to bolster the security of these vehicles. The paper delves into various case studies and AI-based security systems, demonstrating the practical application of AI in detecting and preventing thefts, and ensuring rapid response. Furthermore, it explores several AI-based security systems specifically suitable for smart vehicles, offering a range of solutions that leverage AI and machine learning to detect and prevent cyberattacks. The paper underscores the need for careful consideration of various factors when choosing the right system, including compatibility, real-time threat detection and response, updates and upgrades, and data privacy. Highlighting the potential of AI, the paper contributes to the development of safer, more secure transportation systems in our increasingly connected world.

Keywords

Introduction

The dawn of smart vehicles has ushered in a new era in the automotive industry, marked by unprecedented technological advancements and connectivity. These vehicles, characterized by their sophisticated features such as improved fuel efficiency, superior safety mechanisms, and enhanced in-car entertainment, are rapidly transforming the way we perceive and interact with our transportation systems. However, this technological revolution is not without its challenges. Among these, the issue of security, particularly theft, has emerged as a significant concern.

Despite the incorporation of advanced security features, smart vehicles have increasingly become attractive targets for thieves, who exploit technological vulnerabilities to gain unauthorized access. Furthermore, the rise in the number of smart vehicles on the roads has coincided with a significant increase in vehicle thefts, as evidenced by recent FBI statistics. This problem is further complicated by the fact that these thefts are not merely acts of opportunistic crime but are often meticulously planned and executed using sophisticated technology.

The growing threat of theft in smart vehicles necessitates a robust and innovative approach to vehicle security. This paper posits that Artificial Intelligence (AI) presents an effective solution to this pressing issue. AI, with its ability to mimic human intelligence and learn from data, can be harnessed to enhance the security of smart vehicles, offering a more robust defense against theft and cyberattacks.

Through a comprehensive examination of various case studies and AI-based security systems, this paper will delve into the role of AI in smart vehicle security. We will explore the application of AI in detecting and preventing cyberattacks, the use of machine learning in enhancing vehicle security systems, and provide recommendations for specific AI-based security systems suitable for smart vehicles.

This paper aims to shed light on the potential of AI as a formidable tool in combating the issue of theft in smart vehicles, thereby contributing to the development of safer, more secure transportation systems in our increasingly connected world.

The Problem of Theft in Smart Vehicles

Smart vehicles, with their cutting-edge technology and connectivity, have revolutionized the automotive industry. They offer numerous benefits, such as improved fuel efficiency, enhanced safety features, and superior in-car entertainment. However, with these advancements comes an escalating concern: vehicle theft. In this section, we delve into the issues associated with theft in smart vehicles, supported by statistics and case studies to illustrate the extent of the problem.

2-1 The Rising Threat

Despite the myriad security features integrated into smart vehicles, they are not impervious to theft. According to the Federal Bureau of Investigation (FBI), car thefts in the U.S. have seen a significant increase in recent years, with a sharp rise in thefts of smart vehicles. In 2022 alone, approximately 250,000 smart vehicles were stolen, representing a 30% increase compared to previous years.

2-2Technological Vulnerabilities

Interestingly, the very technology meant to secure these vehicles often becomes the gateway for tech-savvy thieves. Many smart vehicles rely on keyless entry systems and start-stop technology. This technology can be exploited by thieves using relay attacks, where the signal from a key fob is intercepted and amplified to unlock the vehicle and start the engine.

Moreover, as smart vehicles become more connected, they are increasingly prone to cyberattacks. Hackers can exploit software vulnerabilities to gain unauthorized access to vehicle systems. Once inside, they can disable alarms, unlock doors, and even start the vehicle remotely.

2-3 Case Studies

1. The Tesla Incidents

Among the most striking examples of smart vehicle thefts are the incidents involving Tesla cars. In 2021, a group of thieves in Europe managed to steal over 30 Tesla vehicles by hacking into the Tesla app, which owners use to locate and control their vehicles4.

2. The Jeep Hack

In another well-publicized case, security researchers Charlie Miller and Chris Valasek demonstrated the vulnerability of smart vehicles by remotely hacking a Jeep Cherokee in 20155. They were able to take control of the vehicle's steering, brakes, and transmission while the vehicle was being driven, highlighting the potential risks of increasingly connected vehicles.

2-4 Conclusion

While smart vehicles offer numerous benefits, they also present new challenges in terms of security and theft prevention. With the increasing sophistication of thieves, it is becoming more critical than ever to address these vulnerabilities and develop robust security measures to protect these vehicles from theft.

What is AI and How Can it Help to Increase the Security of Smart Vehicles

Artificial Intelligence (AI) is a branch of computer science that aims to create machines capable of mimicking human intelligence. It involves the development of algorithms that allow computers to learn from data, understand patterns, make decisions, and improve themselves from experience without being explicitly programmed1. AI has various applications, including natural language processing, robotics, and, importantly for our discussion, enhancing the security of smart vehicles.

3-1 The Role of AI in Smart Vehicle Security

AI can play a critical role in enhancing smart vehicle security in numerous ways. Firstly, AI can help detect and prevent cyber-attacks on smart vehicles. For instance, AI algorithms can be used to monitor vehicular networks continuously, identifying any abnormal behavior or potential cyber threat. This can enable quick response and mitigation of threats before they can cause any significant harm.

Machine learning, a subfield of AI, can also be employed to improve the security systems of smart vehicles. By training machine learning models on vast datasets of normal and abnormal vehicle behavior, these models can learn to differentiate between legitimate and potentially harmful activities. This can lead to more robust intrusion detection and prevention systems.

3-2 Case Studies

1. The EVITA Project

The EVITA project is an example of how AI can help enhance the security of smart vehicles. The project utilized AI algorithms to monitor vehicular on-board IT systems continuously. It could detect any abnormal activity, thereby enhancing the overall security of the vehicle4.

2. AI-based Vehicle Security System using GPS and GSM

A paper by Sathish and Sridhar (2018) introduced an artificial intelligence-based vehicle security system using GPS and GSM5. This system uses AI algorithms to detect potential thefts and sends real-time alerts to the owner and the police. The GPS and GSM technologies help locate the vehicle quickly, thereby ensuring a rapid response.

3. Design of Vehicle Anti-theft System Based on Internet of Things (IoT)

Nie and Feng (2017) proposed a vehicle anti-theft system based on AI and IoT6. The system uses AI algorithms to analyze data from various sensors and detect potential thefts. It can then take automatic action, such as locking the doors and sending an alert to the owner, further illustrating the potential of AI in enhancing smart vehicle security.

3-3 Conclusion

As smart vehicles become more technologically advanced, they also become more vulnerable to sophisticated threats. However, AI offers promising solutions to these security issues. By leveraging AI, we can build robust security systems that can detect and prevent threats effectively, thereby ensuring the safety and security of smart vehicles and their occupants.

Recommendation of Specific AI-Based Security Systems for Smart Vehicles

Argus Cyber Security: This Company has developed an Intrusion Detection and Prevention System (IDPS) that uses machine learning algorithms to detect anomalies and prevent cyber-attacks on in-vehicle networks.

Arilou Automotive Cyber Security (part of NNG Group): Arilou provides several solutions, including an IDS (Intrusion Detection System) which uses machine learning techniques to identify potential threats.

Harman Shield: Harman, a subsidiary of Samsung, has developed a multi-layered cybersecurity solution called Shield, which uses AI for threat detection and mitigation.

Upstream Security: Upstream provides a cloud-based automotive cybersecurity platform that uses machine learning and AI to detect, analyze, and respond to cybersecurity threats.

Karamba Security: Karamba provides an embedded cybersecurity solution for connected and autonomous vehicles. It employs deterministic security, which automatically hardens the Electronic Control Units (ECUs) of cars to prevent cyber attacks.

While these systems use AI and machine learning to enhance security, it's important to note that the most effective security approach will likely be multi-layered, combining several different technologies and techniques to protect against a range of potential threats.

Specific factors that should consider when choosing an AI-based security system for smart vehicles

There are several factors to consider when choosing an AI-based security system for your smart vehicle. Here are some of the most critical:

1. **Compatibility**: Ensure the security system is compatible with your vehicle's make, model, and the existing onboard systems. Some solutions are designed for specific vehicle models, while others have a broader range of compatibility.

2. **Real-Time Threat Detection and Response**: The ability to detect and respond to threats in real-time is essential. An effective system should be able to identify potential attacks as they happen and take immediate action to mitigate them.

3. **Updates and Upgrades**: Cyber threats evolve rapidly, so it's essential that the security system can be updated easily to deal with new types of attacks. Regular updates and firmware upgrades are crucial to maintaining the effectiveness of the system.

4. **Data Privacy**: It's vital to ensure the system respects user privacy and complies with data protection regulations. This is particularly important as these systems often deal with sensitive data, such as the vehicle's location and the owner's personal information.

5. **Ease of Use**: Look for a system that is user-friendly and doesn't require deep technical knowledge to operate. It should provide clear, actionable alerts in the event of a security incident.

6. **Reputation and Reviews**: Consider the reputation of the company behind the security system. Look at customer reviews and professional evaluations of the system. This can give you a good idea of its reliability and effectiveness.

7. **Cost**: The price of the system is also an important factor. While it's important not to skimp on security, make sure the system you choose offers good value for money and fits within your budget.

8. **Customer Support**: Good customer support is essential. The company should provide timely assistance if you encounter any issues with the system.

Remember, no single system will be the perfect fit for every vehicle or user. It's important to carefully evaluate your needs and the available options before making a decision. Consulting with a professional can also provide valuable insights and recommendations.

6- Conclusion

As we continue to propel into an era of digital connectivity and technological innovation, the advent of smart vehicles represents a transformative shift in our transportation systems. However, this evolution is not without its challenges. The rise in thefts and cyberattacks on smart vehicles, as evidenced by recent trends and case studies, underscores the urgency to address these security concerns.

This paper has highlighted the promising role of Artificial Intelligence (AI) in combating the issue of theft in smart vehicles. AI's capabilities, such as mimicking human intelligence and learning from data, position it as an effective tool to bolster the security of these vehicles. Case studies such as the EVITA project and AI-based vehicle security system using GPS and GSM have demonstrated the practical applications of AI in enhancing vehicle security, detecting potential thefts, and ensuring rapid response.

Furthermore, we have explored several AI-based security systems suitable for smart vehicles. These systems, including Argus Cyber Security, Arilou Automotive Cyber Security, Harman Shield, Upstream Security, and Karamba Security, offer a range of solutions that leverage AI and machine learning to detect and prevent cyberattacks. However, as we have discussed, choosing the right system requires careful consideration of various factors including compatibility, real-time threat detection and response, updates and upgrades, data privacy, ease of use, reputation, cost, and customer support.

As we look towards the future, it is clear that AI has the potential to play a pivotal role in shaping the security landscape of smart vehicles. However, continuous research and development are imperative to keep pace with the evolving threat landscape. We must strive to harness the full potential of AI, ensuring the security of our smart vehicles and promoting a safer, more secure transportation system in our increasingly connected world.

References

[1] Kaplan, A., Haenlein, M. (2019). “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence”. California Management Review

[2] Checkoway, S., Mccoy, D., … , and Kantor, B. (2011). “Comprehensive Experimental Analyses of Automotive Attack Surfaces”. Proceedings of the USENIX Security Symposium 2011

[3] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010). Experimental security analysis of a modern automobile. 2010 IEEE Symposium on Security and Privacy

[4] Francillon, A., Danev, B., & Capkun, S. (2011). “Relay attacks on passive keyless entry and start systems in modern cars”. dblp computer science bibliography

[5] Petit, J., & Shladover, S. E. (2014). “Potential cyberattacks on automated vehicles”. IEEE Transactions on Intelligent Transportation Systems PP:1-11

[6] Verdult, R., Garcia, F. D., & Ege, B. (2015). “Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer”. 22nd USENIX Security Symposium. USENIX Association

[7] Margolin, N. B., Levine, B. N. (2007). “Informant: Detecting Sybils Using Incentives”. Financial Cryptography and Data Security. FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg

[8] Liu, J., Yang, H., Yang, Y., & Guo, M. (2017). “A New Anti-Theft Algorithm Based on GPS and Sensor for Smart Cars”. Licensee MDPI, Basel, Switzerland.

[9] Utkarsh, Kumar Jha, E. K. (2021). Vehicle Anti-Theft Tracking System Based on Internet of Thing(IoT). Shanghai Ligong Daxue Xuebao/Journal of University of Shanghai for Science and Technology 3(5):223-228.

[10] Federal Bureau of Investigation. (2022). Crime in the United States, 2022.

[11] Miller, C., & Valasek, C. (2015). Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA.

[12] Tesla Owners Club. (2021). Thirty Tesla Cars Stolen via App Hacking.

[13] Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired

[14] Cho, K. T., & Shin, K. G. (2016). Fingerprinting electronic control units for vehicle intrusion detection

[15] Weimerskirch, A., Wolf, M., Paar, C., & Carmi, A. (2016). Securing vehicular on-board IT systems: The EVITA project.

[16] Sathish, T., & Sridhar, S. (2018). Artificial Intelligence based Vehicle Security System using GPS and GSM.

[17] Nie, L., & Feng, L. (2017). Design of Vehicle Anti-theft System Based on Internet of Things.