**IT4010 – Research Project - 2024**

**Topic Assessment Form**

**Project ID:** **24-25J-140**

1. Topic (12 words max)

**Enhancing Autonomous Vehicle Security through Advanced Cryptographic Methods and GPS Spoofing Mitigation.**

2. Research group the project belongs to

**Information Assurance & Security (IAS)**

3. Research area the project belongs to

**Cyber Security (CS)**

4. If a continuation of a previous project:

| | |
|---|---|
| Project ID | **N/A** |
| Year | **N/A** |

5. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

The rapid advancement of autonomous vehicle technology has introduced new security challenges, necessitating robust and adaptive security solutions. Traditional vehicle key entry systems, which use simple RF chips and have limited encryption due to their small battery capacity, are susceptible to attacks such as replay, rolling code, roll jam, and rollback. To address these vulnerabilities, we are developing a smart key system through an Android application to replace conventional keys. Additionally, our research focuses on enhancing security for autonomous vehicles by implementing a lightweight and secure Elliptic Curve Cryptography (ECC) authentication mechanism for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. We are also incorporating a challenge-response mechanism using Physical Unclonable Functions (PUFs) to strengthen authentication and protect against side-channel attacks, cloning, and tampering. Furthermore, we are creating an anomaly-based detection system to effectively identify and counter GPS spoofing attacks, thereby improving the reliability and security of autonomous vehicle navigation.

1. Developing a smart key for vehicle entry system using an Android application to replace traditional key fobs, leveraging the computational power of smartphones to generate longer, more secure encryption keys, encrypting signals before transmission, and incorporating Role-Based Access Control (RBAC) with time-based permissions, along with multi-factor authentication (MFA) for vehicle access and EV charging stations.

2. Implementing a lightweight and secure Elliptic Curve Cryptography (ECC) authentication mechanism for V2V and V2I communications.

3. Implementing a challenge-response mechanism using Physical Unclonable Functions (PUFs) to enhance the authentication process for autonomous vehicles, safeguarding sensing devices against side-channel attacks, cloning attempts, and tampering threats.

4. Develop an effective anomaly-based detection system to identify GPS spoofing attacks on autonomous vehicles.

This research aims to enhance the security of autonomous vehicles by addressing the specific vulnerabilities in vehicle access, V2V and V2I communications, and GPS navigation, providing a comprehensive solution to the evolving threats in the cybersecurity domain.

- Smartwatch Vulnerability Analysis Focusing on BLE Protocol - Hannah Fawle & Danielle LeBlanc - https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?article=2305&context=acadfest - Published by DigitalCommons@SHU, 2024

- Key Fob Replay Attacks on Personal Vehicles: Vulnerabilities and Mitigation Strategies - Ana Kapulica; Vedran Dakić; Zlatan Morić; Robert Petrunić- Date of Conference: 23-25 May 2024- Date Added to IEEE Xplore: 12 June 2024 - DOI: 10.1109/HORA61326.2024.10550523 - Publisher: IEEE - Conference Location: Istanbul,Turkiyehttps://www.researchgate.net/publication/381393133_Key_Fob_Replay_Attacks_on_Personal_Vehicles_Vulnerabilities_and_Mitigation_Strategies

- Keys- Types of Keys-Link
- PHONE AS A KEY™- https://www.lincoln.com/support/category/lincoln-way-app/keyless-remote-with-phone-as-a-key/
- A Comparative Analysis of Hybrid Deep Learning Models for Human Activity Recognition - https://www.mdpi.com/1424-8220/20/19/5707
- Integrated GPS Tracking and Automated Sorting: A Technological Leap for Enhanced Logistics Efficiency - https://ijrpr.com/uploads/V4ISSUE10/IJRPR18537.pdf
- An Android-Based Multifactor Authentication for Securing Passive Keyless Access System - https://ieeexplore.ieee.org/document/9824254/
- k. gulebian, "THE HISTORY OF THE CAR KEY," 21 January 2022. [Online]. Available: https://www.lexusofnorthborough.com/the-history-of-the-car-key-2/.
- T. Marin Aranitasi, "Increasing the vehicle security by improving the Remote," April 2022. [Online]. Available: https://www.ijera.com/papers/vol12no4/Ser-3/B1204030915.pdf
- M. [. Cosentino, "secjuice," secjuice, [online]. Available: https://www.secjuice.com/attacking rke-how-to-hack-a-car-open/
- lessonsec, "lessonsec," lessonsec, [online]. Available: https://lessonsec.com/posts/analysis-of-a-remote-control/?ref=secjuice.com
- "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures," Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication, no. 2021, 2021.Available:https://www.researchgate.net/publication/359925015_Security_Hardened_and_Privacy_Preserved_Vehicle-to-Everything_V2X_Communication/link/6256d7964173a21a0d0f7b6d/download
- rfwireless, "MANET Vs VANET Vs FANET-Difference Between MANET,VANET,FANET," rfwireless, [Online]. Available: https://www.rfwireless-world.com/Terminology/MANET vsVANET-vs FANET.html
- K. S. a. A. Marańda, "Security methods against Black Hole attacks in Vehicular Ad-Hoc Network," 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), 2020. Available: https://ieeexplore.ieee.org/document/9306724
- Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems Using Blockchain and PUF- https://ieeexplore.ieee.org/abstract/document/10151864
- A simulated approach to evaluate side-channel attack countermeasures for the Advanced Encryption Standard-https://www.sciencedirect.com/science/article/abs/pii/S0167926018305170
- Supervised Machine Learning Tools and PUF Based Internet of Vehicles Authentication Framework- https://www.mdpi.com/2079-9292/11/23/3845
- Yang, Q.; Zhang, Y.; Tang, C.; Lian, J. A Combined Antijamming and Antispoofing Algorithm for GPS Arrays. Int. J. Antennas Propag. 2019, 2019, 8012569. https://www.researchgate.net/publication/332446023_A_Combined_Antijamming_and_Antispoofing_Algorithm_for_GPS_Arrays

6. Brief description of the nature of the solution including a conceptual diagram (250 words max)

The proposed solution involves a multi-faceted approach to enhance the security of autonomous vehicles.

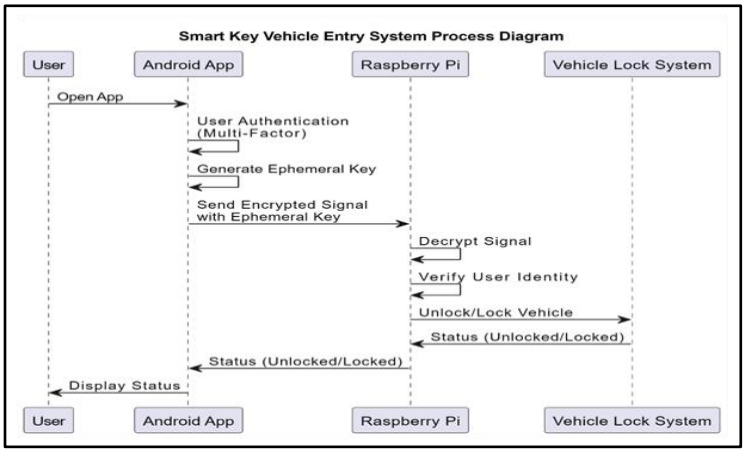
**Smart Key:** Develop a fully digital vehicle entry using an Android application to replace traditional key fobs. This app will enhance the computational power of smartphones to generate longer, more secure encryption keys and encrypt signals before transmission, thereby mitigating potential man-in-the-middle attacks. Before accessing the application, the user needs to authenticate himself to the application then. The application will also incorporate Role-Based Access Control (RBAC) with time-based permissions, allowing vehicle owners to grant temporary access to mechanics, or other legitimate parties. Additionally, it will integrate multi-factor authentication (MFA) for both vehicle access and user authentication at EV charging stations, enhancing security beyond RFID and credit card swipes. To improve efficiency of the encryption and decryption we are intent to use GPU based encryption method instead of traditional CPU based encryption method.

**Lightweight ECC Authentication:** Implement a secure and lightweight ECC-based authentication mechanism for V2V and V2I communications. This will mitigate attacks such as black hole ensuring the integrity and reliability of vehicular networks.

**PUF-based Challenge-Response:** Develop a secure challenge-response mechanism leveraging PUFs for autonomous vehicles. This will ensure robust authentication and protect against side-channel attacks, cloning, and tampering.

**Mitigating GPS Spoofing:** Using existing datasets developing a machine learning model to implement anomaly-based detection framework to mitigate GPS spoofing attacks on autonomous vehicles. This solution is built on the integration of advanced machine learning models that analyze GPS data in real-time to detect irregularities indicative of spoofing attempts.

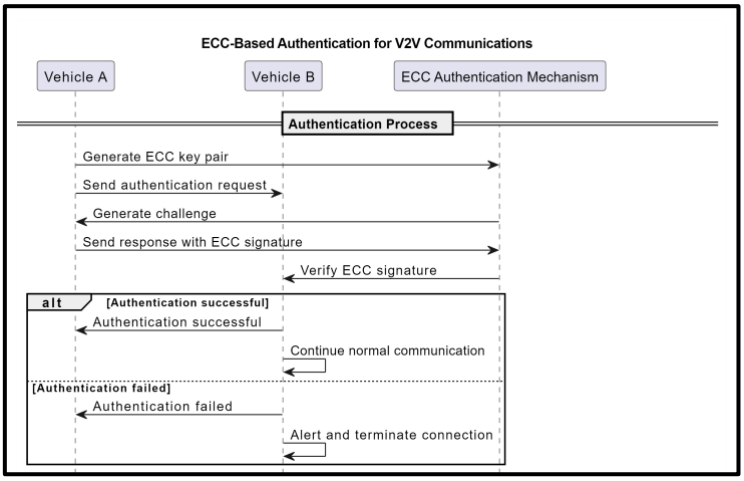
The conceptual diagram will illustrate the interaction between these components, highlighting the flow of authentication and encryption processes.

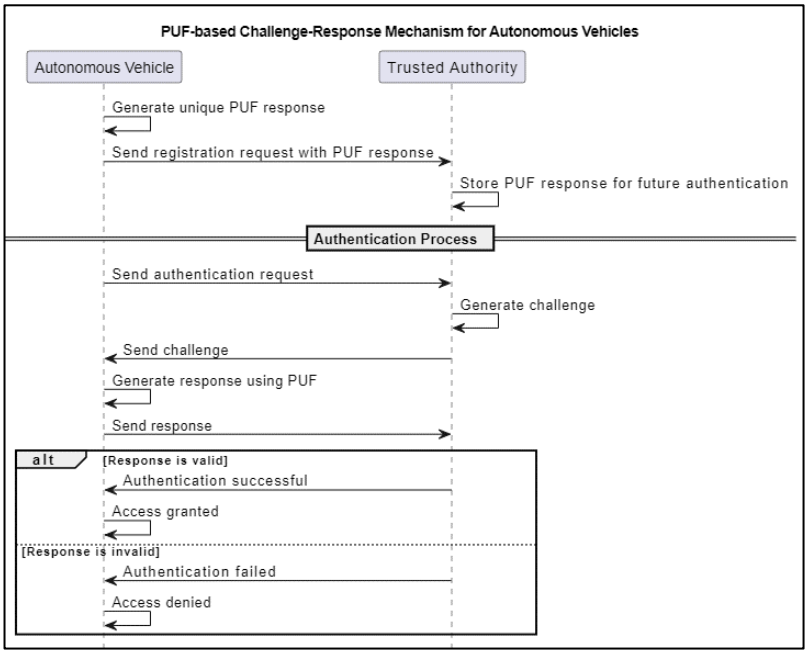


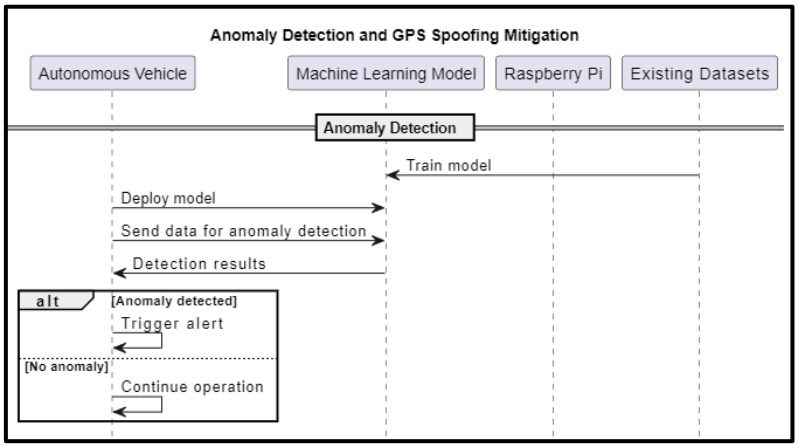
SLIIT UNI
THE KNOWLEDGE UNIVERSITY

# IT4010 – Research Project - 2024

## Topic Assessment Form



7. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

This research requires expertise in several specialized domains:

**Cryptography:** Knowledge in lightweight and advanced cryptographic techniques, particularly ECC, is essential. The implementation of secure encryption methods for both the Android key fob and V2V/V2I communications requires in-depth understanding of cryptographic principles and practices.

**Network Security:** Expertise in network security is crucial for developing and implementing authentication mechanisms to protect V2V and V2I communications. Understanding the threats and vulnerabilities in vehicular networks, such as black hole attack will guide the development of robust security protocols.

**Physical Unclonable Functions (PUFs):** Comprehensive knowledge of how PUFs work, including their unique physical properties that make them resistant to cloning and tampering, is essential. Expertise in the design and implementation of PUF-based systems is also required, particularly in integrating PUFs into security systems to generate unique challenge-response pairs that enhance authentication processes.

**Implement Raspberry and Arduino:** Utilize Raspberry Pi for complex data processing and network communication, serving as the central control unit for security operations. Employ Arduino for real-time sensor interaction and direct hardware management, crucial for responsive and efficient vehicle security systems. Together, these platforms enable robust, flexible, and scalable security solutions for modern vehicular environments.

**GPS Technology:** solution requires specialized expertise in machine learning. particularly in training and optimizing models for anomaly detection. Additionally, cybersecurity knowledge is crucial to understand GPS spoofing attacks and design effective mitigation strategies. Expertise in autonomous vehicle technology is needed to integrate the detection framework seamlessly. Comprehensive data on GPS signals, both normal and spoofed, is essential for model training and validation, ensuring the framework's reliability and effectiveness in real-world scenarios.

**Mobile Application Development:** Proficiency in Android application development is required to create the secure key fob application. This includes integrating advanced encryption methods and MFA into the app, ensuring compatibility with vehicle systems and EV charging stations.

**Data Analysis and Machine Learning:** The implementation of anomaly detection algorithms for signal strength monitoring and the development of machine learning models for threat detection will benefit from expertise in data analysis and machine learning.

**Data Requirements:**

**Cryptographic keys and certificates:** For ECC and other encryption methods.

**GPS signal data:** For analyzing signal strength and detecting anomalies.

8. Objectives and Novelty

Main Objective

The primary goal of this research is to enhance vehicular security through several innovative components. The Smart Key initiative aims to replace traditional key fobs with a digital vehicle entry system using an Android app, utilizing enhanced computational capabilities for secure encryption and incorporating advanced features such as Role-Based Access Control and multi-factor authentication. Lightweight ECC Authentication focuses on securing V2V and V2I communications with ECC-based mechanisms to protect against network vulnerabilities. The PUF-based Challenge-Response component is designed to ensure robust vehicle authentication using Physical Unclonable Functions, guarding against cloning and tampering. Lastly, the Mitigating GPS Spoofing effort involves developing a machine learning model to detect and counteract GPS spoofing, ensuring the reliability and safety of autonomous vehicle navigation. Together, these components aim to enhance the vehicle security.

| Member Name | Sub Objective | Tasks | Novelty |
|---|---|---|---|
| Wickramaarachchi J.C | Developing a Smart Key Vehicle Entry System | • Study existing vehicle entry systems and security mechanisms.<br>• Design and implement a fully physical keyless system using an Android app.<br>• Implement strong authentication mechanism in the Android app.<br>• Develop Role-Based Access Control (RBAC) for granting temporary access to third parties.<br>• Develop secure Bluetooth communication protocols between the Android app and the vehicle unit. | Eliminating physical key fobs and relying solely on a secure Android application, enhancing convenience and security. By leveraging the computational power of smartphones, it employs longer encryption keys for increased security. The system is designed to be universally compatible with any vehicle brand, unlike current brand-specific solutions. It enhances security further by encrypting signals before transmission, preventing man- |

| | | | |
|---|---|---|---|
| | | • Develop a mechanism for generating and using time-sensitive ephemeral encryption keys.<br>• Implement GPU based encryption before transmitting to the vehicle unit to prevent man-in-the-middle attacks.<br>• Integrate the app with EV charging stations for authentication.<br>• Test and validate the security and functionality of the system. | in-the-middle attacks. The implementation of Role-Based Access Control (RBAC) allows vehicle owners to grant temporary access to others with defined roles and time limits. Additionally, the app integrates as an authentication method for EV charging stations, adding a layer of convenience and security. |
| Albalushi O.T.M.G | Implement ECC-based authentication for V2V/V2I communications | **Research and Analysis:**<br>• Study existing authentication mechanisms for V2V/V2I communications.<br>• Analyze the benefits of ECC (Elliptic Curve Cryptography) over other methods.<br>**Design Phase:**<br>• Design an ECC-based authentication protocol.<br>• Ensure the protocol is lightweight and efficient for real-time communications.<br>**Development Phase:**<br>• Develop the ECC-based authentication mechanism.<br>• Implement the mechanism in a controlled environment. | Introducing a lightweight and efficient ECC-based authentication mechanism that enhances the security of V2V and V2I communications, effectively mitigating attacks such as black hole attack. |

| | | | |
|---|---|---|---|
| | | **Testing Phase:**<br>• Test the authentication mechanism in various scenarios to ensure robustness.<br>• Perform security tests to mitigate potential attacks like black hole attacks.<br>**Deployment and Monitoring:**<br>• Deploy the authentication mechanism in a real-world V2V/V2I network.<br>• Monitor performance and security and make necessary adjustments. | |
| Jayasinghe K.A.C. T | Implement a PUF-based challenge-response mechanism for autonomous vehicles. | **Research and Analysis:**<br>• Study existing authentication mechanisms for autonomous vehicles.<br>• Analyze the benefits of PUF technology over other methods.<br>**Design Phase:**<br>• Design a PUF-based challenge-response protocol.<br>• Ensure the protocol is secure and efficient for real-time communications.<br>**Development Phase:**<br>• Develop the PUF-based challenge-response mechanism.<br>• Implement the mechanism in a controlled environment. | Introducing a PUF-based challenge-response mechanism that enhances the security of autonomous vehicles by effectively protecting against side-channel attacks, cloning attempts, and tampering threats. This approach leverages the inherent uniqueness of PUFs to ensure robust and dynamic authentication. |

| | | | |
|---|---|---|---|
| | | **Testing Phase:**<br>• Test the authentication mechanism in various scenarios to ensure robustness.<br>• Perform security tests to mitigate potential attacks such as side-channel attacks, cloning, and tampering.<br>**Deployment and Monitoring:**<br>• Deploy the authentication mechanism in a real-world autonomous vehicle network.<br>• Monitor performance and security and make necessary adjustments. | |
| Wanigasekara W.M.I.W | Develop comprehensive anomaly-based GPS spoofing detection framework. | **Research and Selection of Machine Learning Models:**<br>• Review existing literature on machine learning models used for anomaly detection.<br>• Select appropriate models (e.g., neural networks, support vector machines, decision trees) for initial implementation.<br>**Data Collection and Preprocessing:**<br>• Gather GPS data from autonomous vehicles under normal and spoofed conditions. | Using existing datasets developing a machine learning model to implement anomaly- based detection system Using Raspberry Pi to simulate and mitigate GPS spoofing attack on autonomous vehicles. |

| | | | |
|---|---|---|---|
| | | • Preprocess the collected data to remove noise and ensure it is suitable for training.<br><br>**Model Training and Optimization:**<br><br>• Train selected machine learning models using the preprocessed data.<br>• Optimize model parameters to improve detection accuracy and reduce false positives.<br><br>**Framework Design and Development:**<br><br>• Design a comprehensive framework that integrates the trained models for real-time anomaly detection.<br>• Implement the framework in a suitable programming environment (e.g., Python, TensorFlow, or PyTorch).<br><br>**Testing and Validation:** | |

| | | | |
|---|---|---|---|
| | | • Conduct extensive testing of the framework under various scenarios to ensure reliability.<br>• Validate the effectiveness of the framework in detecting GPS spoofing attacks through controlled experiments.<br><br>**Performance Analysis and Improvement:**<br><br>• Analyze the performance of the framework using metrics such as detection accuracy, response time, and false positive rate.<br>• Identify areas for improvement and refine the models and framework accordingly.<br><br>**Attack Scenario Demonstration:**<br><br>• Conduct an attack scenario using a Raspberry Pi to simulate GPS spoofing.<br>• Demonstrate the research output by showing how the anomaly detection framework mitigates the attack. | |

9. Supervisor checklist

a) Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

| Yes | ✓ | No | |
|---|---|---|---|

b) Does the proposed topic exhibit novelty?

| Yes | ✓ | No | |
|---|---|---|---|

c) Do you believe they have the capability to successfully execute the proposed project?

| Yes | ✓ | No | |
|---|---|---|---|

d) Do the proposed sub-objectives reflect the students' areas of specialization?

| Yes | ✓ | No | |
|---|---|---|---|

e) Supervisor's Evaluation and Recommendation for the Research topic:

10. Supervisor details

| | Title | First Name | Last Name | Signature |
|---|---|---|---|---|
| Supervisor | | Kavinga | Yapa | |
| Co-Supervisor | for | Hansika | M. | for |
| External Supervisor | | | | |
| Summary of external supervisor's (if any) experience and expertise | | | | |

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

**IT4010 – Research Project - 2024**

**Topic Assessment Form**

**This part is to be filled by the Topic Screening Panel members.**

Acceptable: Mark/Select as necessary

| | |
|---|---|
| Topic Assessment Accepted | ✓ |
| Topic Assessment Accepted with minor changes (should be followed up by the supervisor)* | |
| Topic Assessment to be Resubmitted with major changes* | |
| Topic Assessment Rejected. Topic must be changed | |

* Detailed comments given below

Comments

| |
|---|
| Accepted. |

The Review Panel Details

| Member's Name | Signature |
|---|---|
| Mr. Amila Senaratne | |
| Mr. Kavishka Yapa | |
| | |
| | |
| | |
| | |

*__Important__:

1. According to the comments given by the panel, make the necessary modifications and get the approval by the **Supervisor** or the **Same Panel**.
2. If the project topic is rejected, identify a new topic, and follow the same procedure until the topic is approved by the assessment panel.