ENHANCING AUTONOMOUS VEHICLE SECURITY

24-25J-140

SLIIT
FACULTY OF COMPUTING

OUR TEAM

Mr. Kavinga Abeywardena

Supervisor

Ms. Hansika Mahaadikara

Co-Supervisor

Wickramaarachchi J.C.

IT21369810

Albalushi O.T.M.G

IT21099472

Jayasinghe K.A.C.T

IT21146442

Wanigasekara W.M.I.W

IT21249648

INTRODUCTION

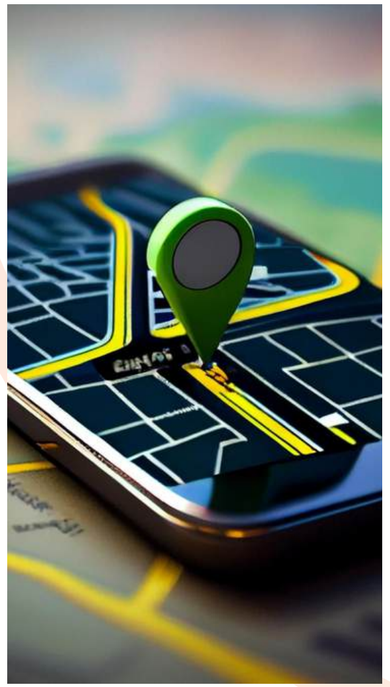
- **Smart Key System:** We are developing a smart key system using an Android app to replace traditional vehicle key fobs, enhancing security and convenience.

- **Lightweight mechanism to mitigate Black-Hole Attack:** Our research includes implementing lightweight ECC for secure Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, protecting against network attacks.

- **Physical Unclonable Functions (PUFs):** We are utilizing PUFs to create a robust challenge-response mechanism, enhancing authentication and guarding against side-channel attacks.

- **Mitigate GPS Spoofing:** A machine learning-based anomaly detection system is being developed to identify and counter GPS spoofing, ensuring reliable navigation for autonomous vehicles.





OBJECTIVES

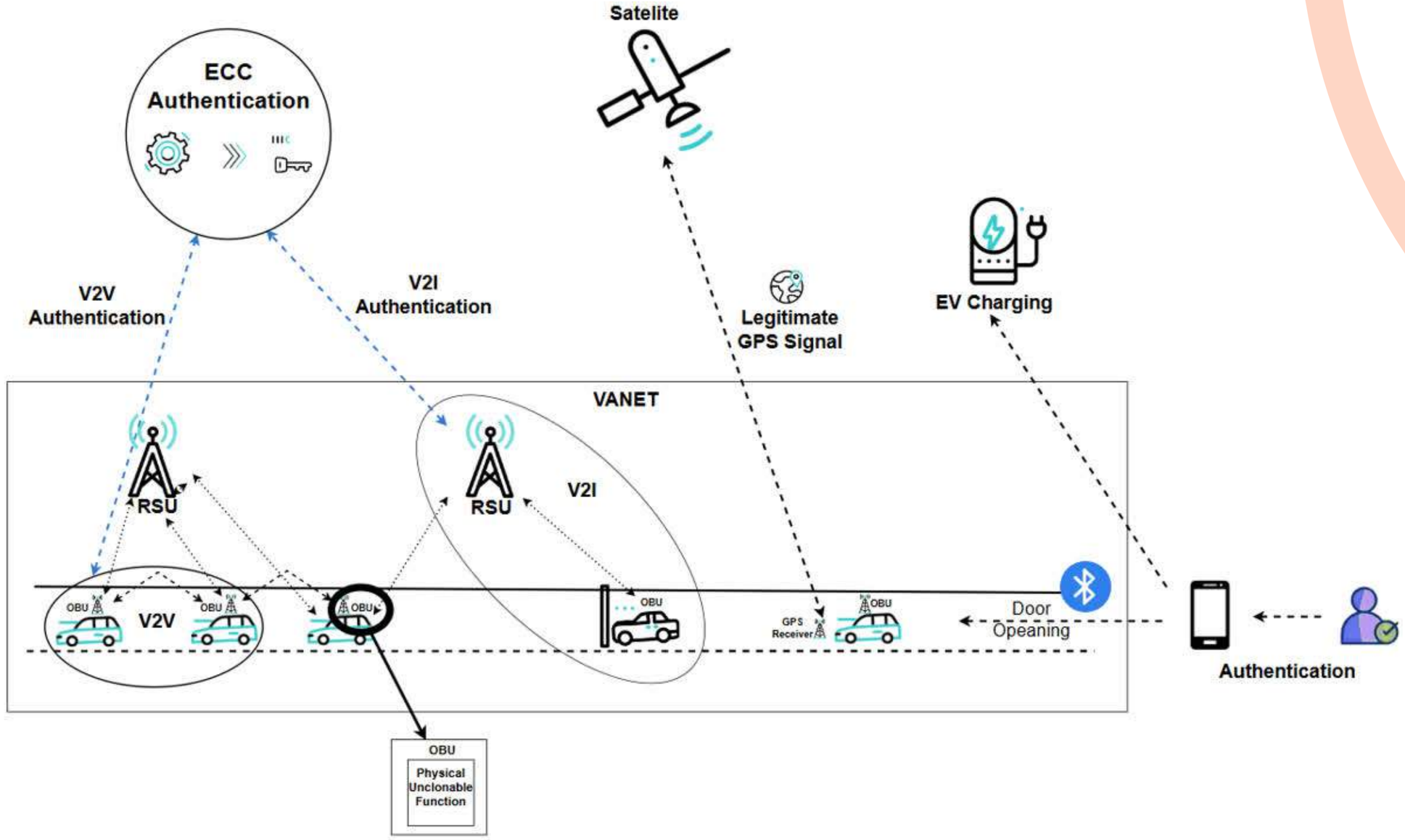
To enhance the overall security of autonomous vehicles by developing the following components:

- Developing a Smart Key Vehicle Entry System
- Implement ECC-based authentication for V2V/V2I communications
- Implement a PUF based challenge response mechanism for autonomous vehicles.
- Develop comprehensive anomaly-based GPS spoofing detection framework.

Research Questions

- How to enhance security by introducing a android application instead of traditional key fobs?
- How to introduce a proper authentication mechanism to EV charging stations by the smart key.
- How can lighweight ECC improve V2V and V2I security and efficiency?
- How effective is ECC-based authentication in mitigating black hole attacks compared to PKI?
- How can PUFs provide secure challenge-response mechanisms for autonomous vehicles?
- How can machine learning detect and mitigate GPS spoofing in autonomous vehicles?

SYSTEM DIAGRAM



IT21369810

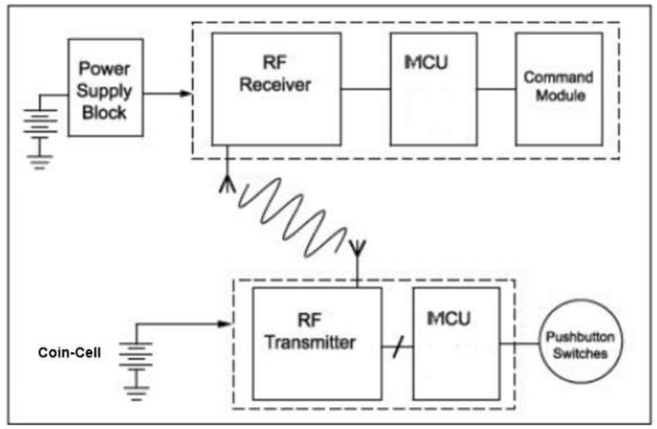
Wickramaarachchi J.C.

Cyber Security

SLIIT
FACULTY OF COMPUTING

BACKGROUND & RESEARCH PROBLEM

- Traditional vehicle entry systems with basic RF chip key fobs are vulnerable to attacks like replay, roll jam, and rollback due to limited encryption and power constraints, making them easy targets for attackers.
- Current EV charging stations typically rely on RFID and credit card swipes for authentication, which may not provide sufficient security against unauthorized access or fraud.
- Current Android key fobs are often designed specifically for each manufacturer, limiting interoperability and flexibility across different vehicle brands.



EXISTING RESEARCH

Title	Authors	Published Year
[1] An Android-Based Multifactor Authentication for Securing Passive Keyless Access System	• Aditya D Naik • Ritvik Vibhu • Udbhav P Saboji • Vanisha R.M • Nagasundari S • Prasad B Honnavalli	2022
[2] Enhancing Connected Vehicle Security: Innovations in Two-Factor Authentication	• Huseyin Karacali • Efecan Cebel • Nevzat Donum	2024
[3] PRESTvO: PRivacy Enabled Smartphone Based Access to Vehicle On-Board Units	• B. Groza • T. Andreica • A. Berdich • P. S. Murvay • E. H. Gurban	2024

RESEARCH GAP

Research / Review Paper / Article	Mobile Application	Access control for the USERS	Encrypting before sending to the BLE	MFA authentication for the EV charging
Research [1]	✓	✓	✗	✗
Research [2]	✓	✗	✓	✗
Research [3]	✓	✓	✓	✗
Proposed Solution	✓	✓	✓	✓

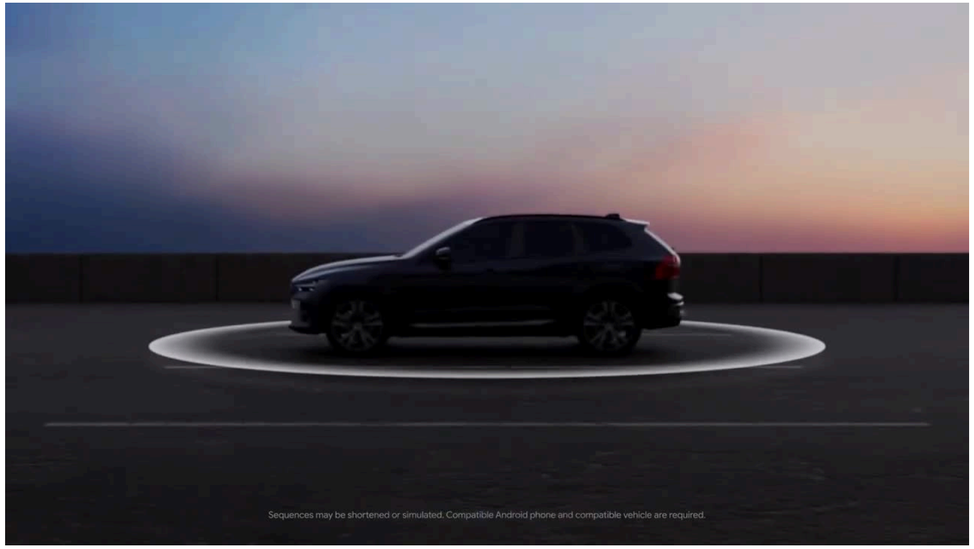
OBJECTIVES

Main Objectives

- To develop an Android application that replaces traditional key fobs by leveraging smartphones' computational power to generate longer and more secure encryption keys, encrypt signals to prevent man-in-the-middle attacks, and incorporate user authentication with Role-Based Access Control (RBAC) and time-based permissions for granting temporary access to authorized individuals.

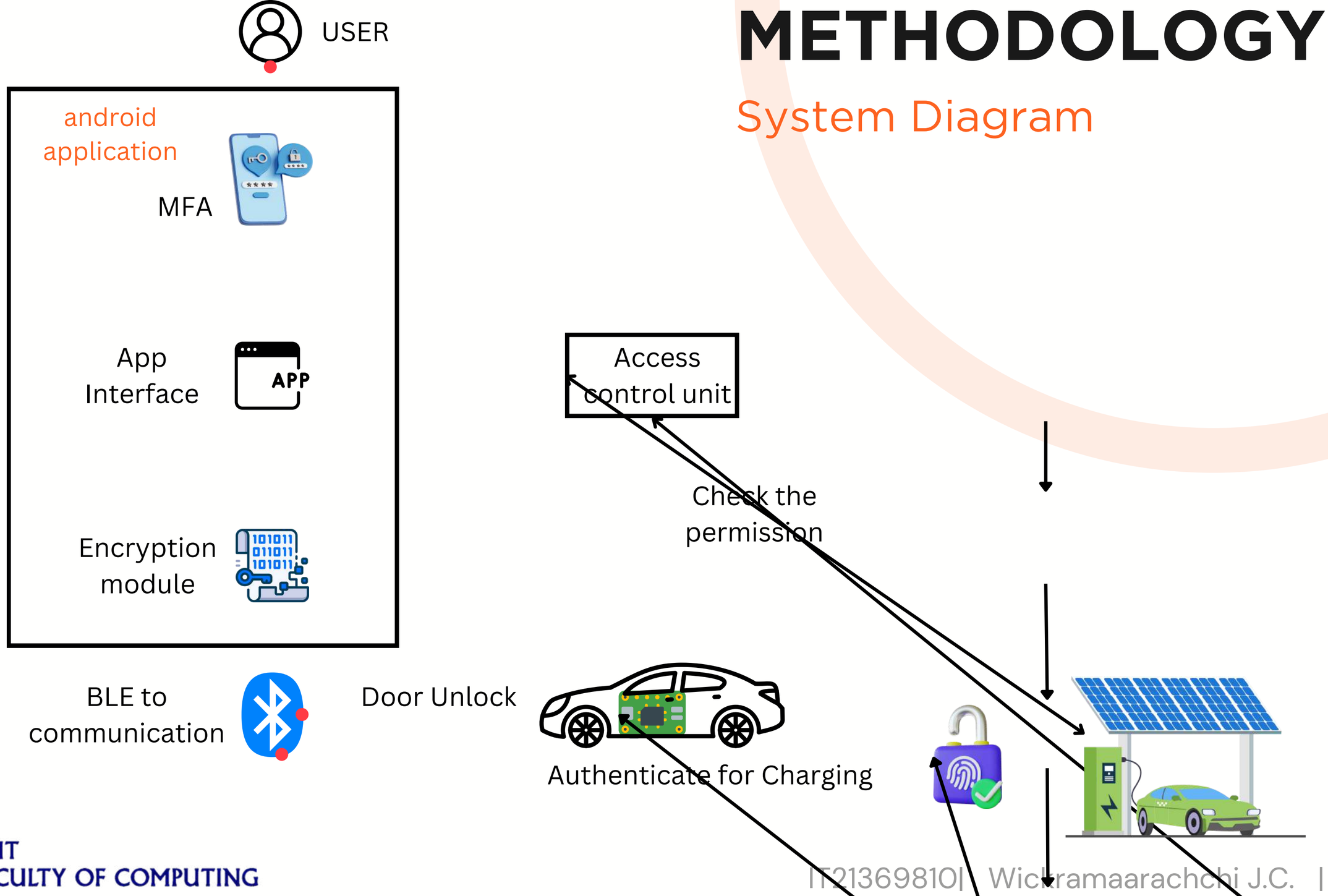
Sub Objectives

- Design and Development of the Android Application
- Implement Enhanced Encryption Method
- Incorporate User Authentication and Access Control
- Establish Secure Communication Protocols



METHODOLOGY

System Diagram



REQUIREMENTS

Functional Requirements:

- Authenticate users using passwords, biometrics, or multi-factor authentication (MFA).
- Implement Role-Based Access Control (RBAC) for temporary access permissions.
- Generate secure encryption keys and encrypt communications to prevent interception.
- Allow users to unlock, lock, and start the vehicle through the app.

Non- Functional Requirements:

- Security
- Performance
- Reliability
- Usability
- Scalability

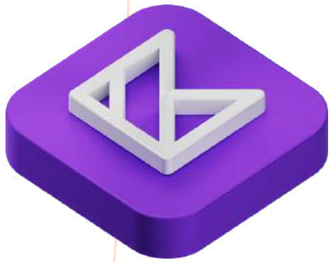
Technical Requirements:

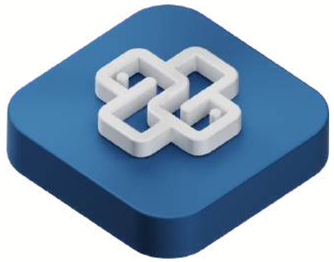
- Develop for Android, compatible with various smartphone models.
- Operate both online and offline, using secure network protocols.
- Use Kotlin and encryption libraries for development.

TOOLS & TECHNOLOGIES

Technologies

- Kotlin(Android App Development)
- Firebase
- Bluetooth (BLE)
- Python
- AWS
- Raspberry Pi





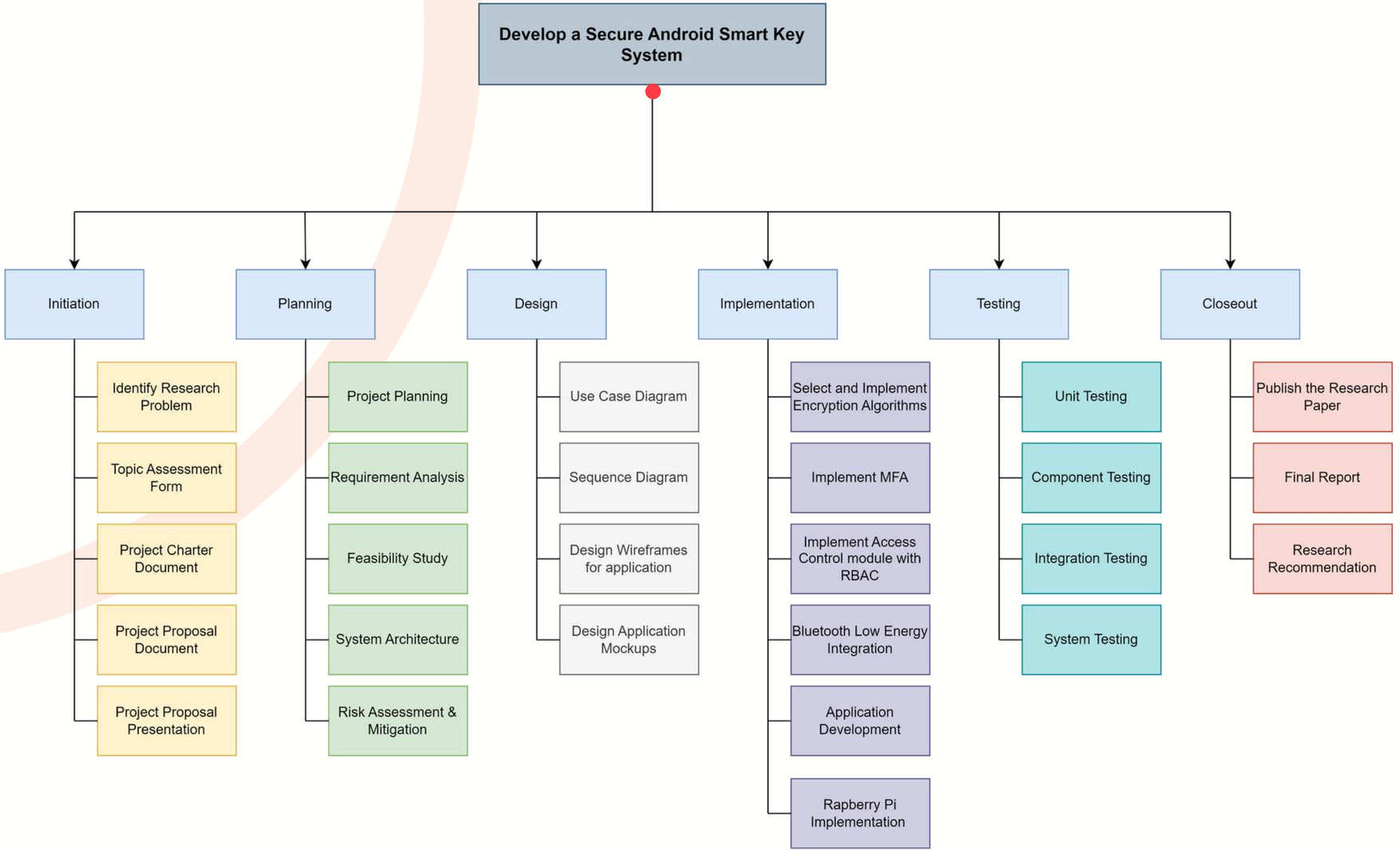
Algorithms & Architectures

- AES (Advanced Encryption Standard)
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- Elliptic Curve Cryptography (ECC)

Techniques

- End-to-End Encryption
- Time Stamped Ephemeral keys

Work Breakdown Structure



References

[1] A. D. Naik, R. Vibhu, U. P. Saboji, V. R. M, N. S and P. B. Honnavalli, "An Android-Based Multifactor Authentication for Securing Passive Keyless Access System," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-8, doi: 10.1109/I2CT54291.2022.9824254.

[2] H. Karacali, E. Cebel and N.Donum, "Enhancing Connected Vehicle Security: Innovations in Two-Factor Authentication," International Conference on Technology (IConTech), May 02-05, 2024, Alanya/Turkey, pp. 108-121

[3] B. Groza, T. Andreica, A. Berdich, P. -S. Murvay and E. H. Gurban, "PRESTvO: PRivacy Enabled Smartphone Based Access to Vehicle On-Board Units," in IEEE Access, vol. 8, pp. 119105-119122, 2020, doi: 10.1109/ACCESS.2020.3003574.

[4] S.Hamdare, O.Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown and J. Lloret "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations". Sensors 2023, 23, 6716. https://doi.org/10.3390/s23156716

IT21099472

Al balushi O.T.M.G.

Cyber Security

SLIIT
FACULTY OF COMPUTING

BACKGROUND & RESEARCH PROBLEM

Current Authentication Mechanisms: Existing V2V and V2I communication systems primarily use traditional cryptographic methods, which can be inefficient and resource-intensive.

Black Hole Attacks: V2V and V2I communications are vulnerable to black hole attacks, where malicious nodes drop packets, disrupting network reliability and safety.

Need for lightweight Solutions: Real-time communications in vehicular networks require lightweight and efficient authentication protocols to ensure quick and secure data exchanges.

Advantages of ECC: Elliptic Curve Cryptography (ECC) offers stronger security with smaller key sizes, making it suitable for resource-constrained environments like vehicular networks.

EXISTING RESEARCH

Title	Published Year
[1] An ECC-Based Conditional Privacy-Preserving Authentication Scheme for V2V Communication in VANETs.	2022
[2] An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs	2022
[3] Cyber Security Challenges and Solutions for V2X Communications	2019

RESEARCH GAP

Research / Review Paper / Article	Lightweight ECC based Authentication	Blackhole Attack Mitigation	Trust based Mechanism	Scalable Solution for V2V and V2I
Research [1]	✓	✗	✓	✗
Research [2]	✗	✓	✗	✗
Research [3]	✗	✓	✗	✗
Proposed Solution	✓	✓	✓	✓

OBJECTIVES

Main Objectives

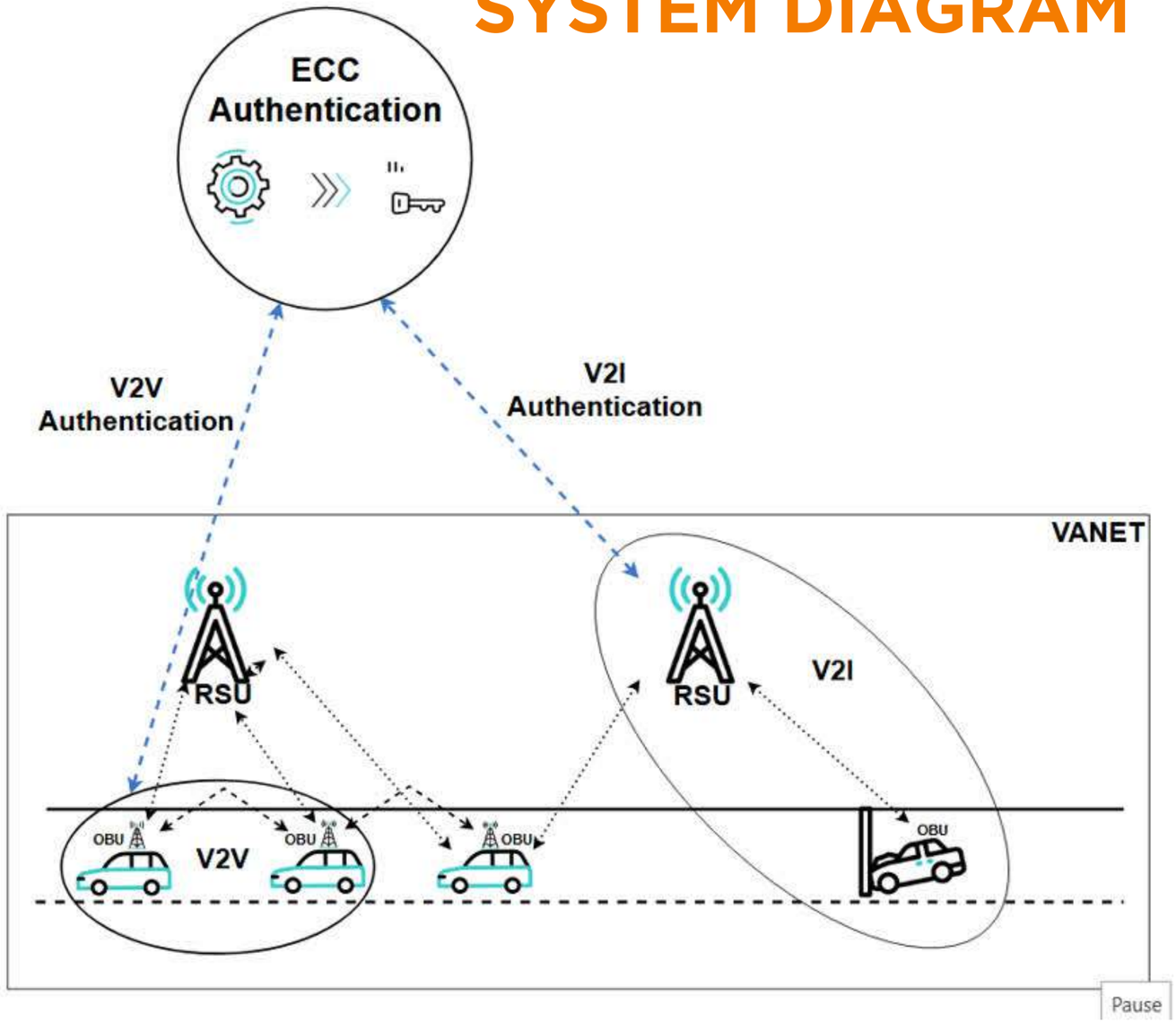
- Develop a lightweight ECC-based authentication mechanism to enhance the security of V2V and V2I communications, effectively mitigating black hole attacks

Sub Objectives

- Study current V2V/V2I authentication methods and ECC benifits.
- Design a lightweight ECC-based protocol for real-time use.
- Test the authentication mechanism in various scenarios to ensure security to mitigate black hole attacks

METHODOLOGY

SYSTEM DIAGRAM



ECC - Elliptic Curve Cryptography
V2V - Vehicle to Vehicle
V2I - Vehicle to Infrastructure
VANET - Vehiculat Ad Hoc Netowork
RSU - Road Side Unit
OBU - On Board Unit

REQUIREMENTS

Functional Requirements:

- **Authentication:** The system must verify the identity of vehicles to ensure only legitimate vehicles can communicate.
- **Data Integrity:** Ensure that the data exchanged between vehicles and infrastructure remains intact and unaltered.
- **Resource Efficiency:** Use lightweight cryptographic methods to minimize computational overhead on vehicle devices.

Non- Functional Requirements:

- Accuracy
- Performance
- Availability
- Security
- Scalability

Technical Requirements:

- **Cryptographic Libraries**: Implement ECC based cryptographic libraries for lightweight encryption and decryption.
- **Simulation Tools:** Use tools like OMNeT++ for simulating and illustrating the process.
- **Secure Communication Protocols:** Ensure secure communication channels between vehicles and infrastructure.

TOOLS & TECHNOLOGIES

Technologies

- OMNET++
- C++
- Python

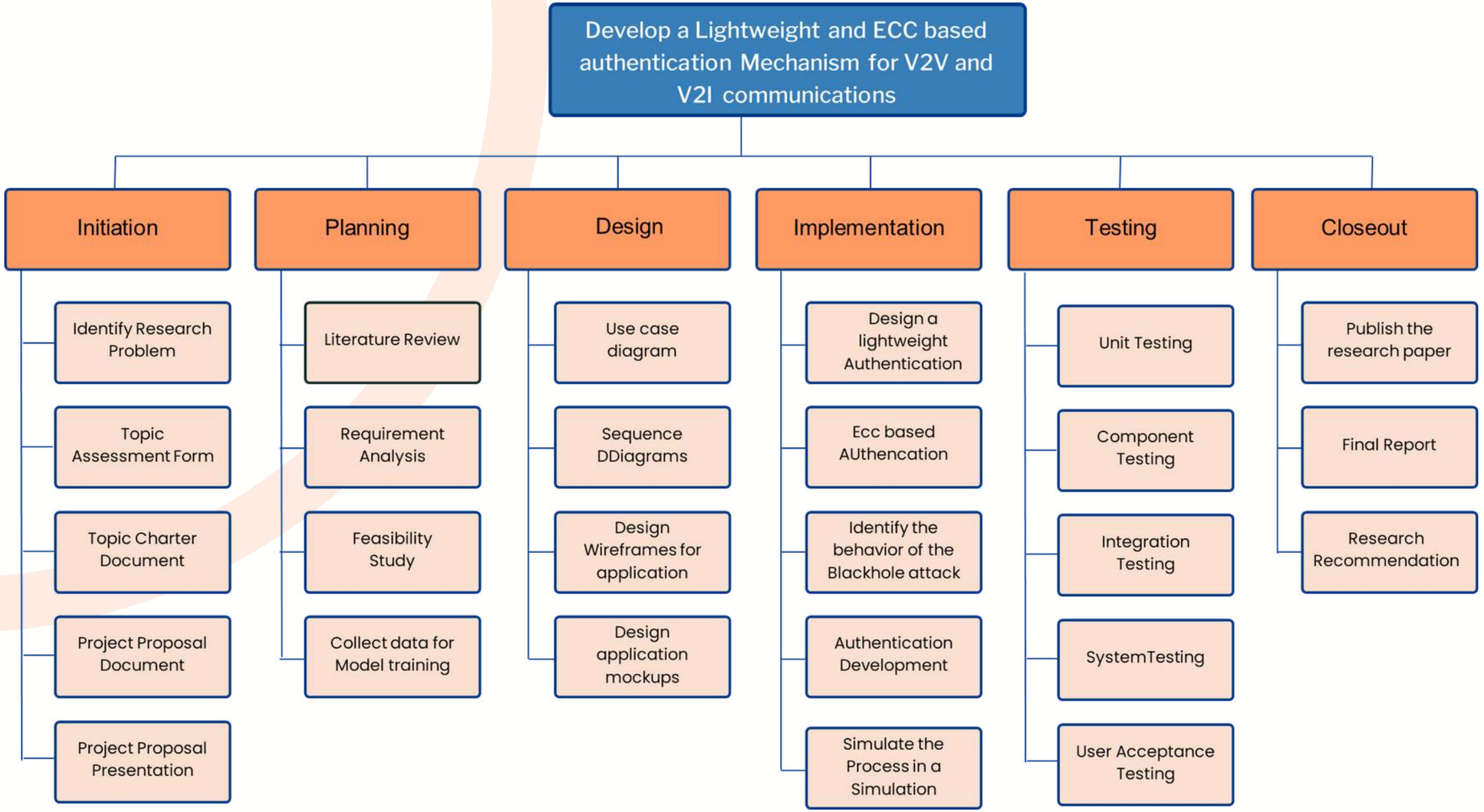
Algorythm & Architechtures

- Elliptic Curve Cryptography [ECC]
- ECDSA
  (Elliptic Curve Digital Signature Algorythm)
- AES (Advanced Encryption Standard)

Techniques

- Simulation: OMNet++
- Performance Evaluation
- Data Encryption and Decryption

Work Breakdown Structure



References

T. Ali, X. Li, H. Zhang, and J. Pan, "An ECC-Based Conditional Privacy-Preserving Authentication Scheme for V2V Communication in VANETs," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 1-6, 2022. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-16-8586-6_6

"An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANET," *Sensors*, vol. 22, no. 5, pp. 1897, Mar. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/5/1897

"Cyber Security Challenges and Solutions for V2X Communications," *arXiv preprint arXiv:1901.01053*, Jan. 2019. [Online]. Available: https://arxiv.org/pdf/1901.01053

IT21146442

Jayasinghe K.A.C.T

Cyber Security

BACKGROUND & RESEARCH PROBLEM

- Traditional cryptographic methods are becoming insufficient because they are vulnerable to sophisticated side-channel attacks, cloning attempts, and tampering threats.

- Physical Unclonable Functions (PUFs) offer a promising solution due to their inherent uniqueness and resistance to cloning.

- The challenge lies in integrating PUFs into a comprehensive challenge-response mechanism that ensures the security and efficiency required for Autonomous Vehicles (AVs).

EXISTING RESEARCH

Title	Authors	Published Year
Two-Factor Authentication Protocol Using Physical Unclonable Function for IoV	• Qi Jiang • Xin Zhang • Ning Zhang • Youliang Tian • Xindi Ma • Jianfeng Ma	2019
Chaotic map-based authentication scheme using physical unclonable function for Internet of autonomous vehicle	• Jie Cui • Hong Zhong • Lu Wei	2022
Cyber Security Protocol for Secure Traffic Monitoring Systems using PUF-based Key Management **(** Key Generation module**)**	• Vikramkumar Pudi • Srinivasu Bodapati • Sachin Kumar • Anupam Chattopadhyay	2021

RESEARCH GAP

Research / Review Paper / Article	Resistant to Side-Channel Attacks	Implemented Challenge-Response Mechanism	Environmental Variability
Research [1]	✗	✓	✓
Research [2]	✓	✗	✗
Research [3]	✗	✗	✓
Proposed Solution	✓	✓	✓

OBJECTIVES

MAIN OBJECTIVES

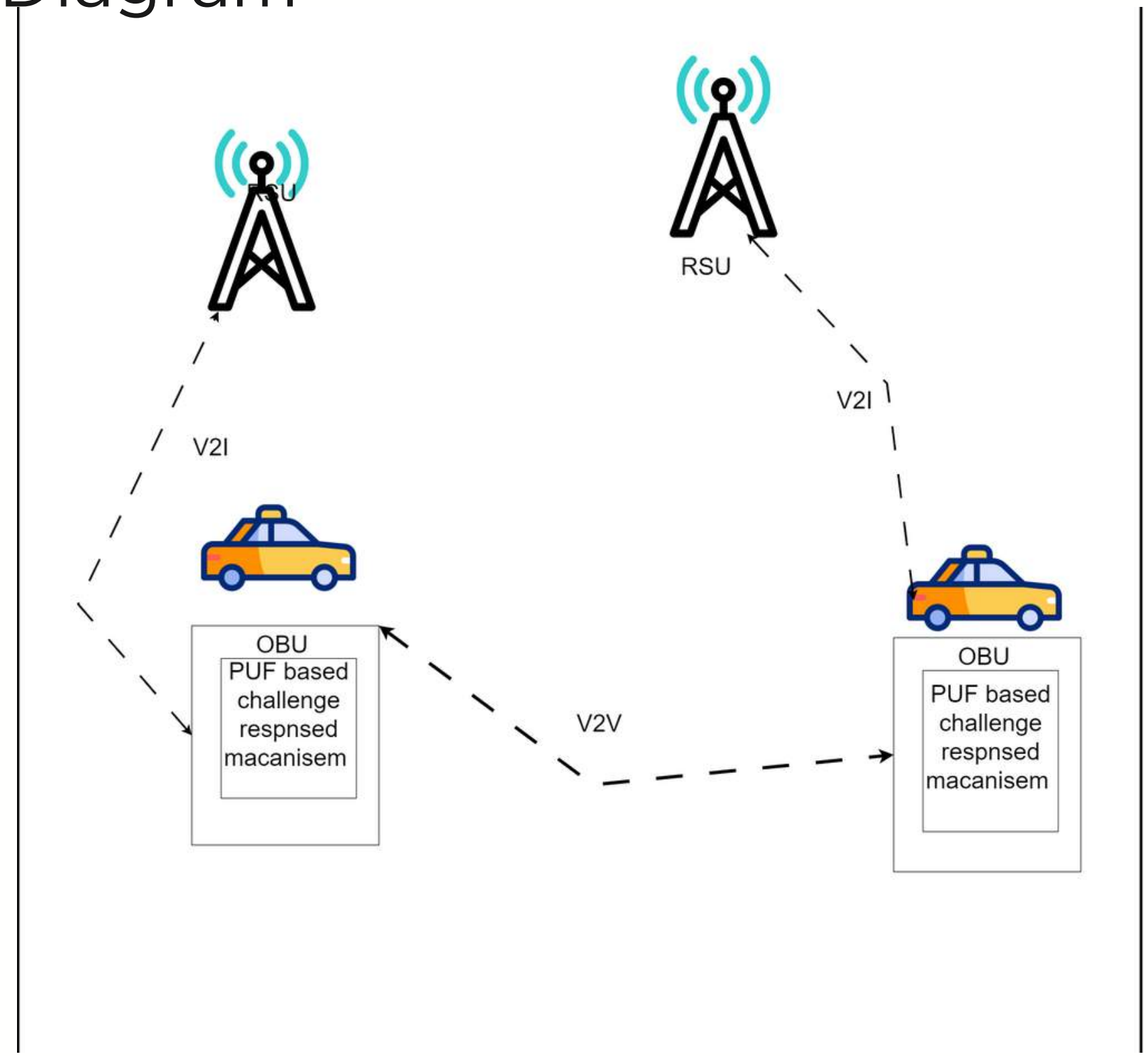
Develop a PUF-based challenge-response mechanism to ensure robust vehicle authentication and protection against physical attacks.

SUB OBJECTIVES

- Research current Physical Unclonable Function (PUF) technologies and their use cases in security systems.
- Analyze the benefits of different PUF types (e.g., SRAM, Ring Oscillator) for vehicle authentication.
- Develop a challenge-response mechanism utilizing PUF technology that is tailored for vehicle authentication.
- Conduct rigorous testing of the PUF-based authentication mechanism under various Environmental scenarios.

METHODOLOGY

System Diagram



REQUIREMENTS

Functional Requirements:

- The PUF must be implemented in such a way that it can generate unique, unpredictable responses based on physical hardware characteristics.
- The system must support a challenge-response protocol where a vehicle can generate a response to a given challenge using the PUF.
- The system must verify the authenticity of vehicles based on their challenge-response pairs

Non- Functional Requirements:

- Security
- Performance
- Reliability
- Usability
- Scalability

Technical Requirements:

- Implement a secure random number generator (RNG) to produce unique and unpredictable challenges.
- Test PUF responses under various environmental conditions (temperature, voltage) to ensure stability.
- Implement a system to periodically regenerate challenges to ensure they are unpredictable.

TOOLS & TECHNOLOGIES

Technologies

- C++
- Python
- PyCrypto
- Raspberry Pi

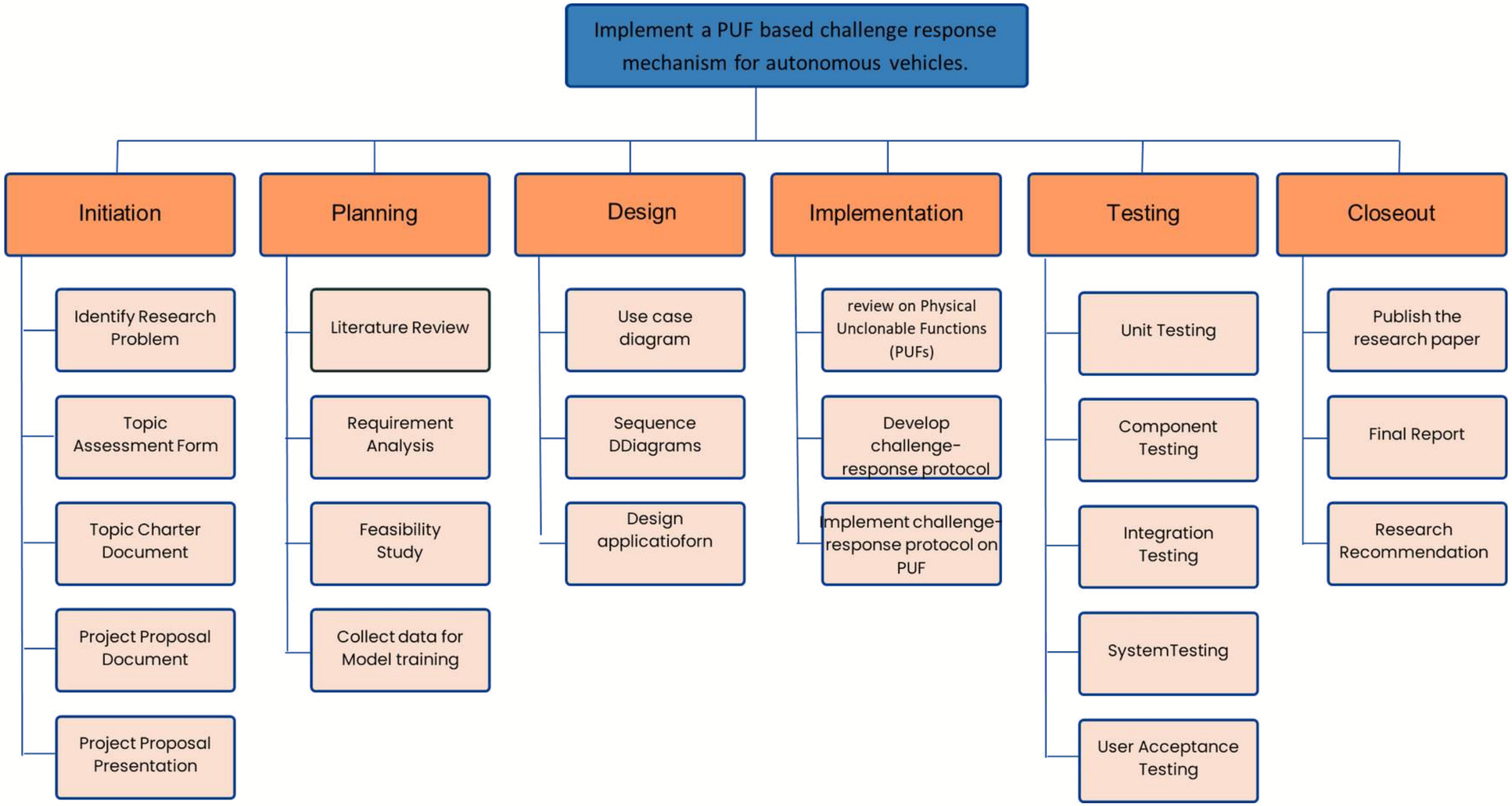
Algorythm & Architechtures

- challenge-response mechanism
- Physical Unclonable Functions

Techniques

- Simulation: OMNet++
- Performance Evaluation
- Data Encryption and Decryption

WORK BREAKDOWN STRUCTURE



References

- Cyber Security Protocol for Secure Traffic Monitoring Systems using PUF-based Key Management https://ieeexplore.ieee.org/abstract/document/9426088

- Chaotic map-based authentication scheme using physical unclonable function for Internet of autonomous vehiclehttps://ieeexplore.ieee.org/document/9994238

- Two-Factor Authentication Protocol Using Physical Unclonable Function for IoV doi:https://ieeexplore.ieee.org/document/8855828

IT21249648

Wanigasekara W.M.I.W

Cyber Security

SLIIT
FACULTY OF COMPUTING

BACKGROUND & RESEARCH PROBLEM

- GPS spoofing attacks involve deliberately manipulating GPS signals to deceive the vehicle's onboard navigation system, which can cause the vehicle to deviate from its intended path, leading to accidents or even hijacking.

- The GPS spoofing attack generates fabricated GPS signals and interferes with the GPS receivers, which can degrade the performance of the localization system. The fake GPS signal usually has a higher strength to mislead the GPS receiver

EXISTING RESEARCH

Title	Authors	Published Year
[1] Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration	• Zhen Yang • Jun Ying • Junjie Shen	2023
[2] Detection of GPS Spoofing Attacks on Unmanned Aerial Systems	• Mohsen Riahi Manesh • Jonathan Kenney • Wen Chen Hu	2020

RESEARCH GAP

Research / Review Paper / Article	Hardware Implementation (out put)	Real world dataset	Combine ML models
Research [1]	✗	✓	✗
Research [2]	✗	✓	✗
Proposed Solution	✓	✓	✓

OBJECTIVES

Main Objectives

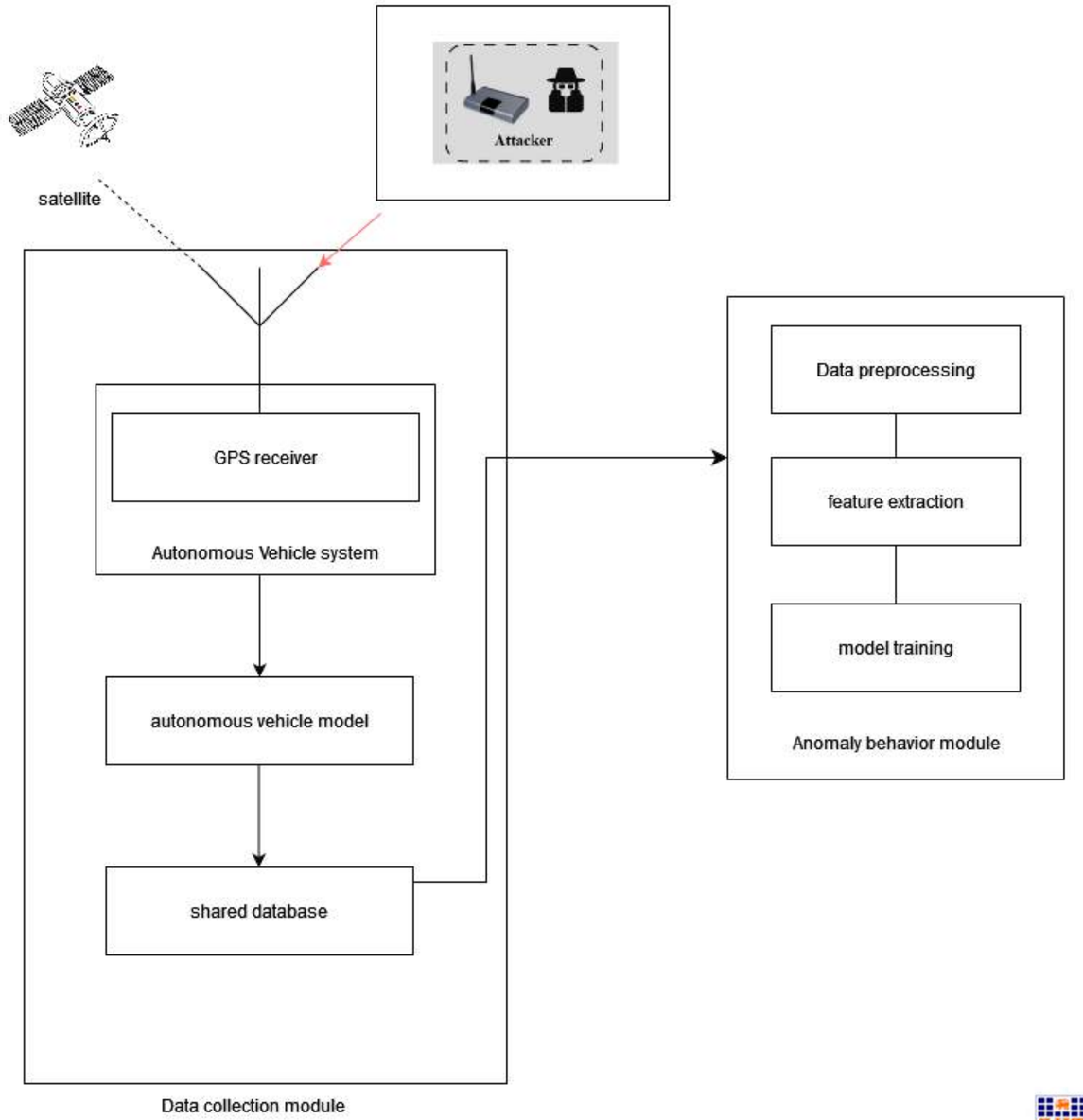
- Developing an anomaly-based GPS spoofing detection system involves combining machine learning models with existing datasets and using a Raspberry Pi to simulate and mitigate GPS spoofing attacks on autonomous vehicles.

Sub Objectives

- Identify and acurate relevant datasets for GPS signal and trajectory data.
- Evaluate and select suitable machine learning models for anomaly detection.
- Set up a Raspberry Pi environment to simulate GPS spoofing attacks.

METHODOLOGY

System Diagram



REQUIREMENTS

Functional Requirements

- Analyze deviations from expected routes to identify possible spoofing.
- Detect irregular patterns in the GPS data that indicate spoofing attacks.
- The system should identify spoofing attacks in real time.
- Train the models and check the accuracy levels of the data set

Non- Functional Requirements

- Security
- Performance
- Reliability
- Usability
- Scalability

Technical Requirements

- Implement machine learning or statistical models for trajectory and anomaly detection.
- Deploy sufficient computational resources to handle real-time data processing and analysis.
- Use appropriate programming languages (e.g., Python, C++) for system development.

TOOLS & TECHNOLOGIES

Technologies

- TensorFlow
- Python
- SQL

Architectures & Algorithms

- kNN
- Dynamic Time Warping (DTW)

Techniques

- Combining multiple detection algorithms to improve overall detection accuracy and reduce false positives/negatives.

- Extracting relevant features from raw GPS data (e.g., speed, acceleration, heading changes) to improve model performance.

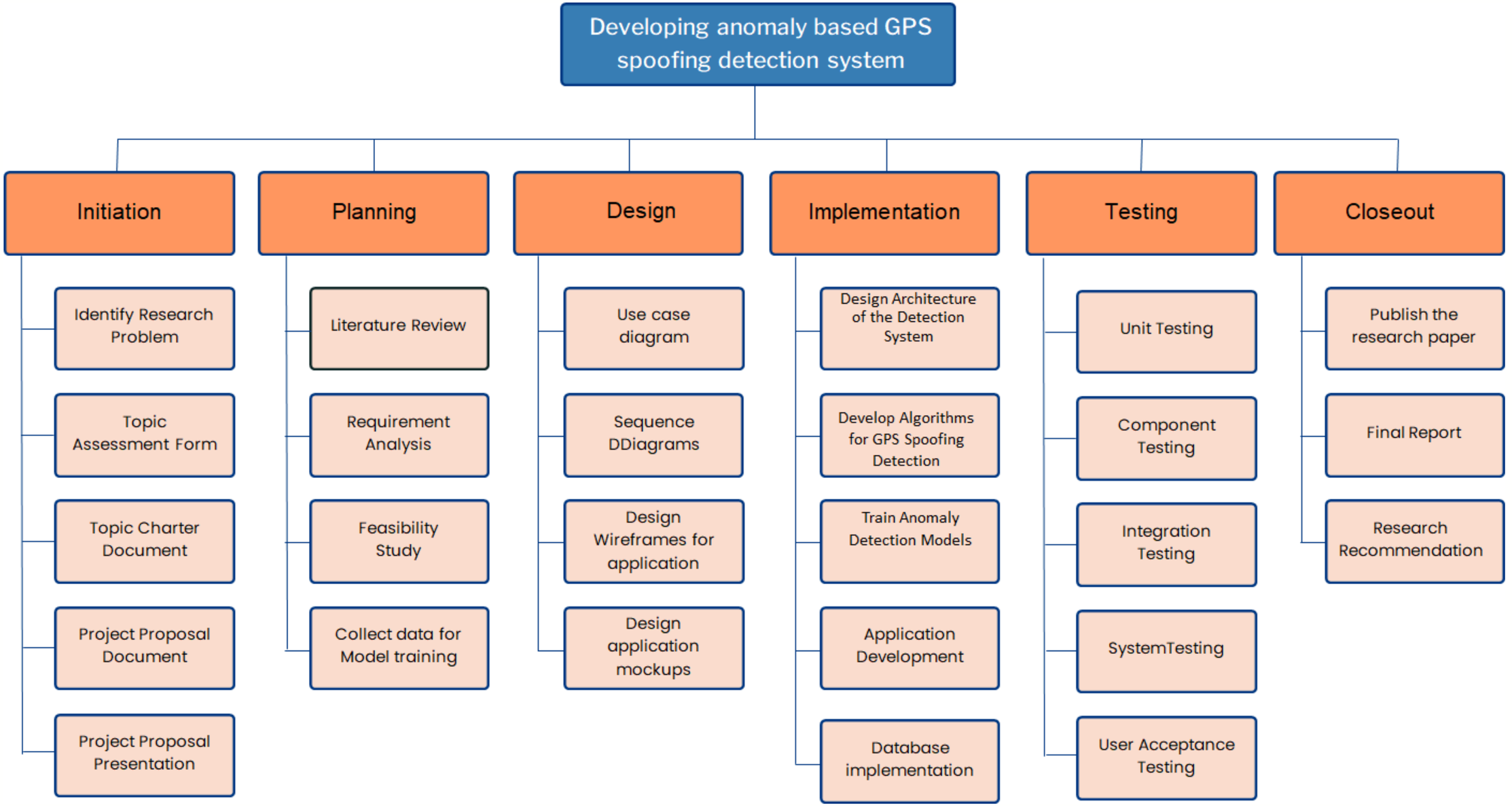
References

- Yang, Zhen, et al. “Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning From Demonstration.” IEEE Transactions on Intelligent Transportation Systems (2023).

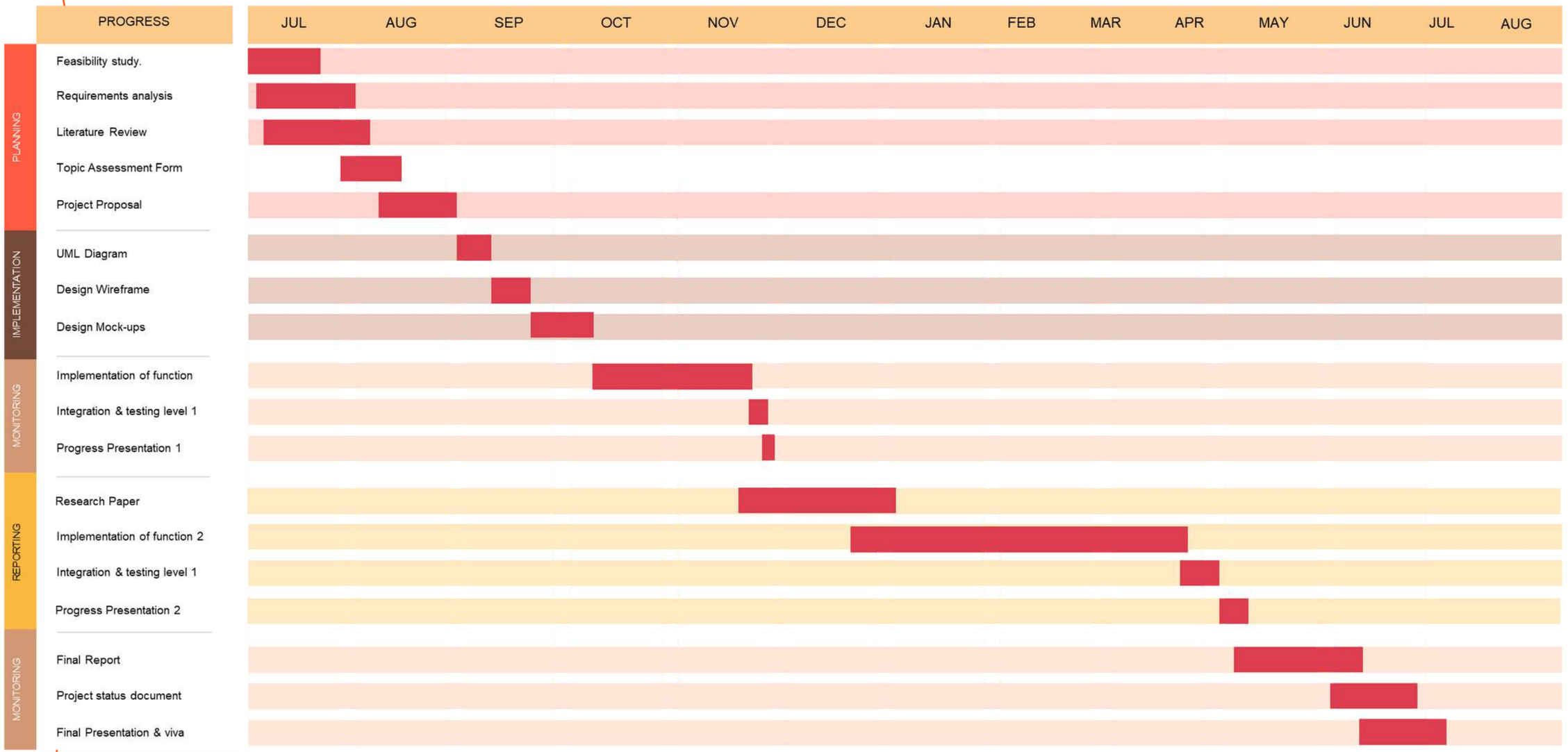
- Manesh, Mohsen Riahi, et al. “Detection of GPS spoofing attacks on unmanned aerial systems.” 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019..

- D. G. Yang et al., “Intelligent and connected vehicles: Current status and future perspectives,” Sci. China-Technol. Sci., vol. 61, no. 10, pp. 1446–1471, Oct. 2018.

WORK BREAKDOWN STRUCTURE



GANNT CHART


PROGRESS
JUL
AUG
SEP
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
PLANNING
Feasibility study.
Requirements analysis
Literature Review
Topic Assessment Form
Project Proposal
IMPLEMENTATION
UML Diagram
Design Wireframe
Design Mock-ups
MONITORING
Implementation of function
Integration & testing level 1
Progress Presentation 1
REPORTING
Research Paper
Implementation of function 2
Integration & testing level 1
Progress Presentation 2
MONITORING
Final Report
Project status document
Final Presentation & viva

Thank you