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

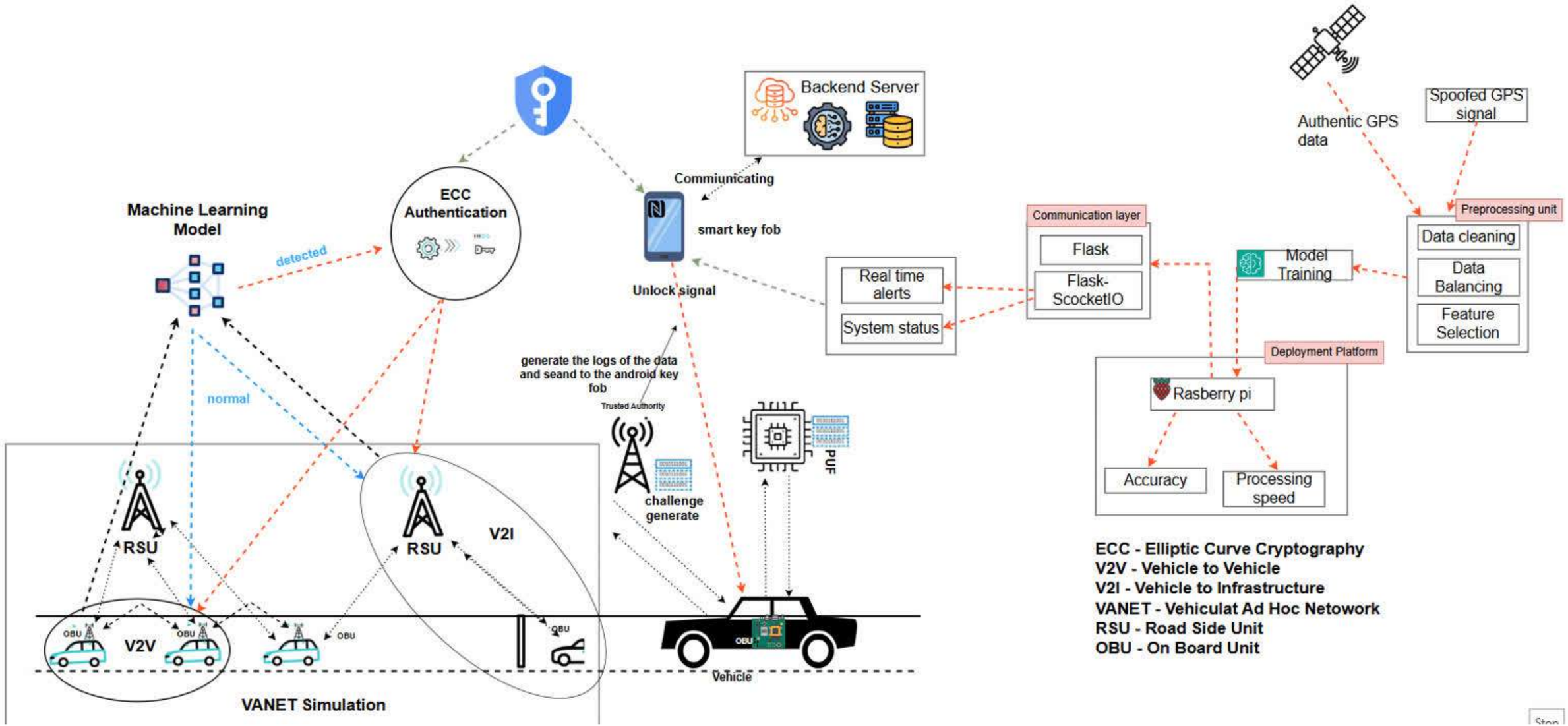
- How to enhance security by introducing a android application instead of traditional key fobs?
- How can lighweight ECC improve V2V and V2I security and efficiency?
- How effective is ECC-based authentication in mitigating black hole attacks compared to PKI?
- How can PUFs provide secure challenge-response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

Suggested Improvements

- In first component, Instead of only focusing on autonomous vehicles, focus on all the vehicle models whether its autonomous or not.

- In the RP meeting, mentioned that each components are not interconnected so we did a deep background research and changed a little bit of outline to interconnect each component.

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

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.
- In the current automotive world most of the vehicles such as Honda Fit 2022, Honda Civic 2022, Honda VE-1 2022, Honda Breeze 2022 are vulnerable to Rolling-PWN attack.
- 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	Communication using NFC	Key Fob Anomaly detection & Risk Calculation	VIN Number Theft Protection
Research [1]	✓	✓	✗	✗	✗
Research [2]	✓	✗	✗	✗	✗
Research [3]	✓	✓	✗	✗	✗
Proposed Solution	✓	✓	✗	✗	✗

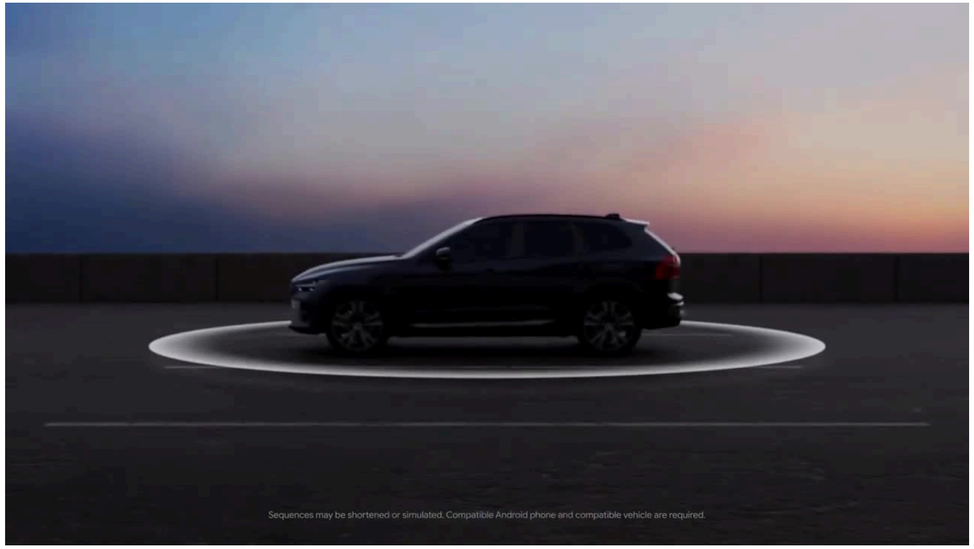
OBJECTIVES

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.

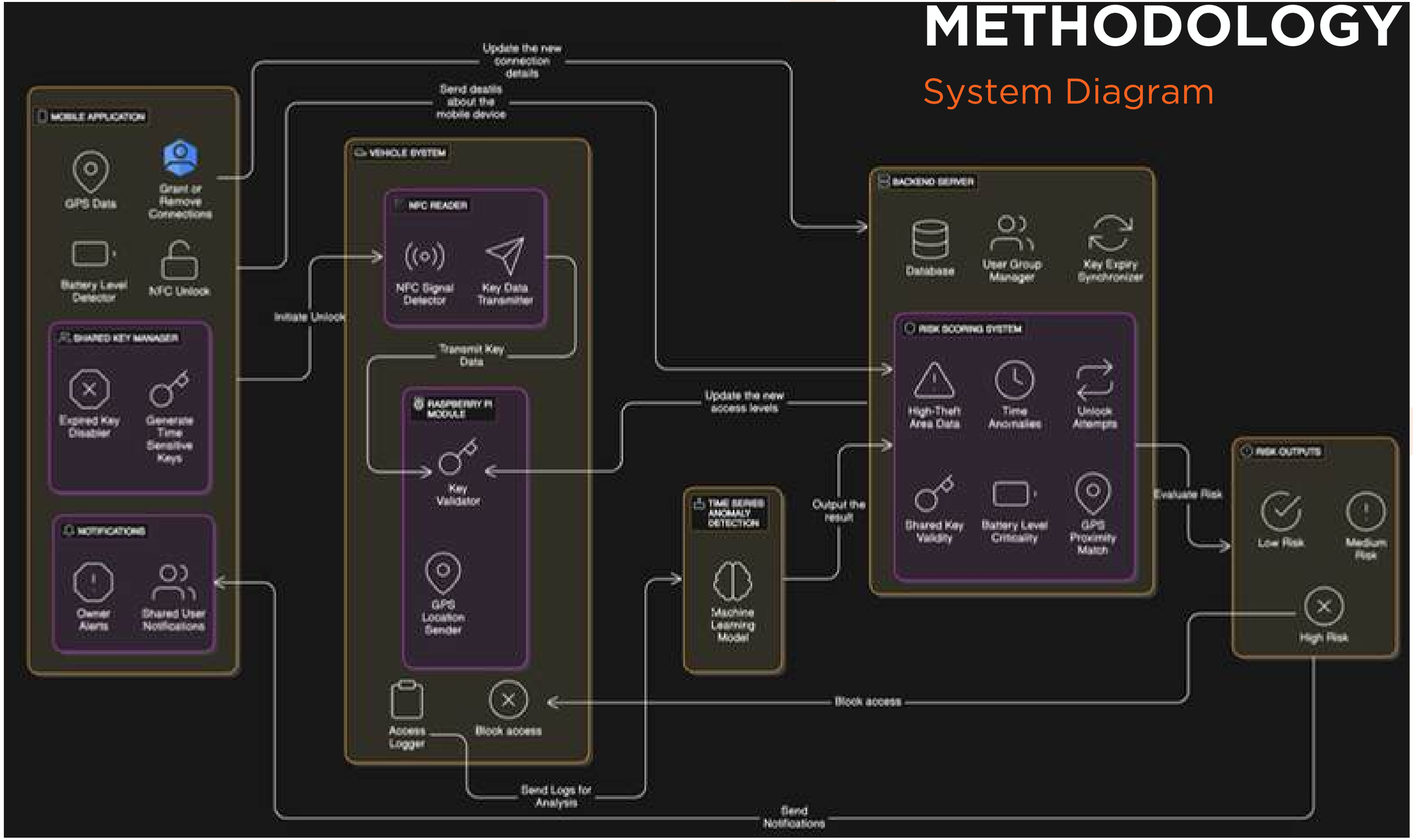
Sub Objectives

- 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

- Flutter(Android App Development)
- Firebase
- NFC (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

Current Progress

- Train ML Model to identify time series access anomalies.
- Use a dynamic risk matrix to calculate risk values.
- Design wireframe for the mobile application.
- Start to design UI for the mobile application.
- Test and check model and the function.

Future Step

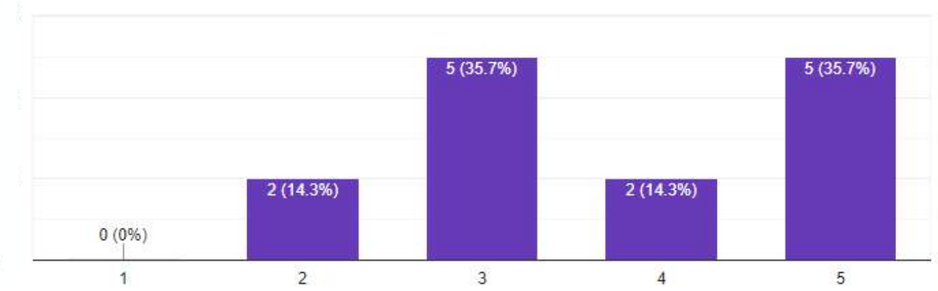
- Complete a mobile application.
- Create user groups and dynamic secret key for communication
- Connect Raspberry pi with the application
- Use a Backend server for communication with Hardware component and the application.

Current Progress

Survey to identify Sri Lankan user perspective and security knowledge

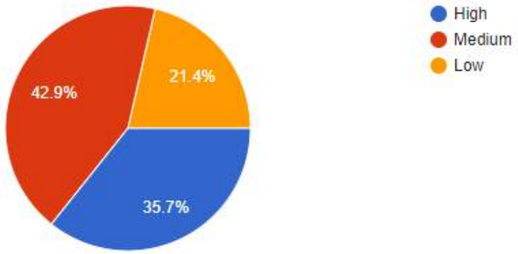
How secure do you think your current unlocking system is?

Copy chart



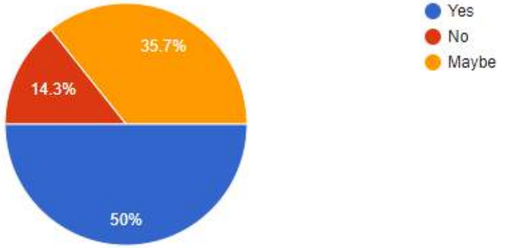
How would you rate your concern about unauthorized access or misuse of the vehicle?

Copy chart



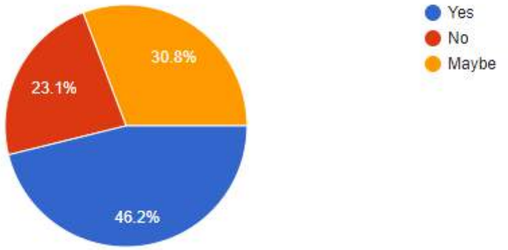
If we introduced an NFC-based unlocking system to mitigate such risks, would you consider transferring to it?

Copy chart



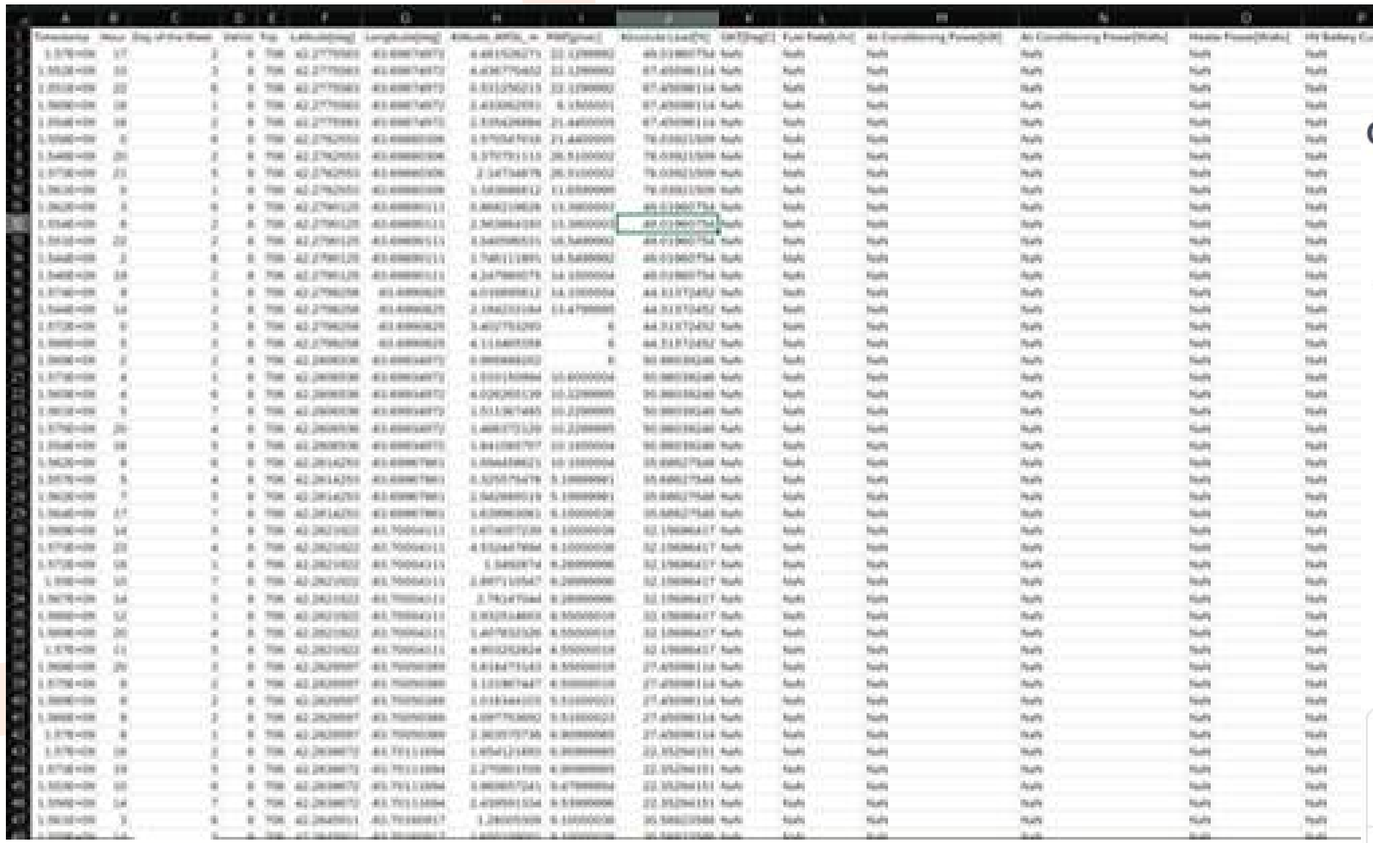
This system may require additional hardware installation. Would you still be interested if the answer is yes?

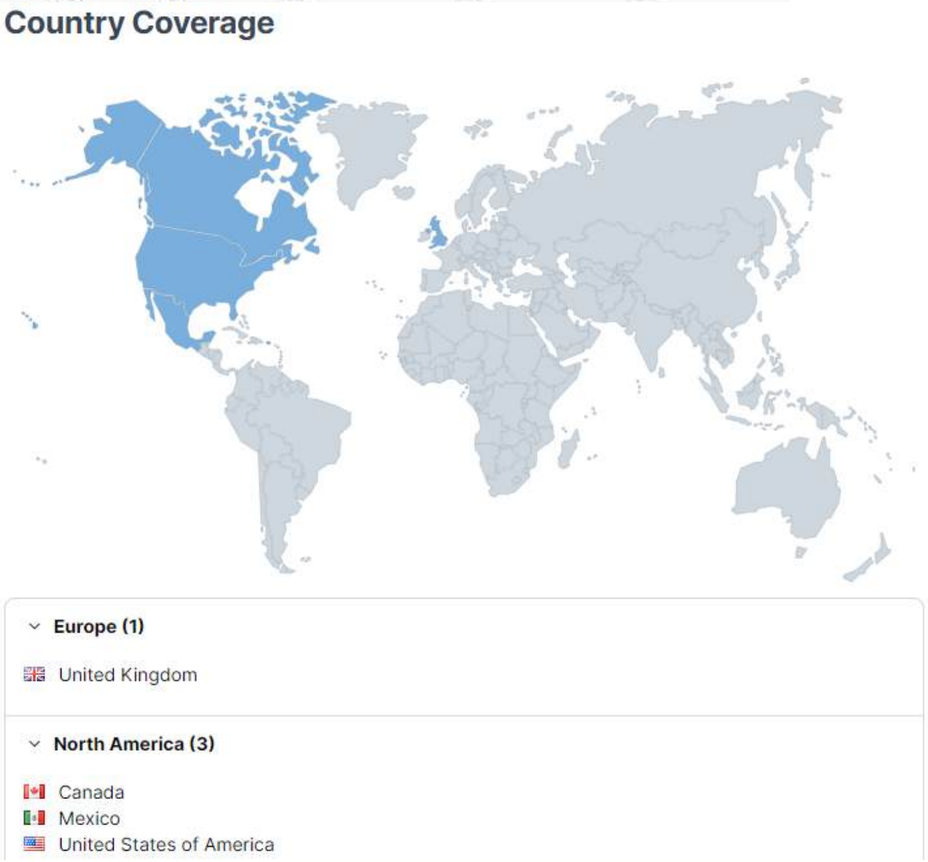
Copy chart



Current Progress

ML and -Data set



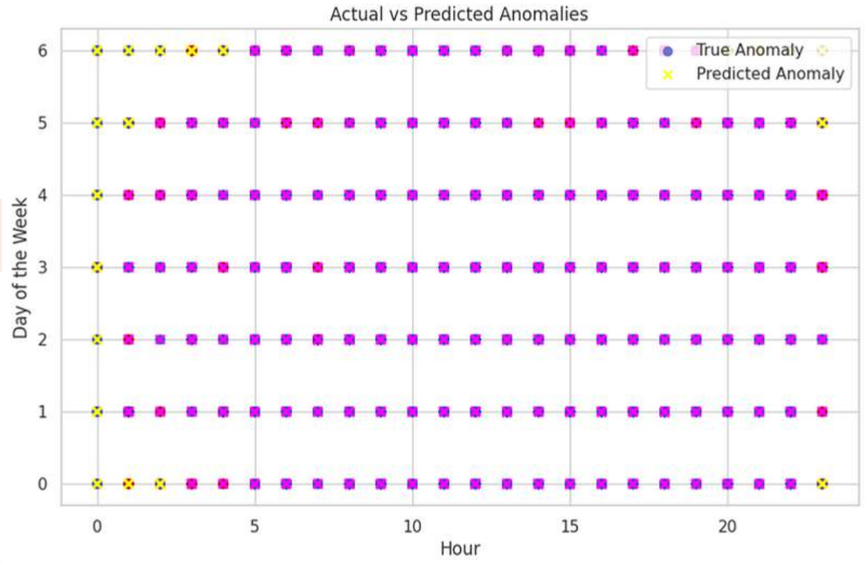


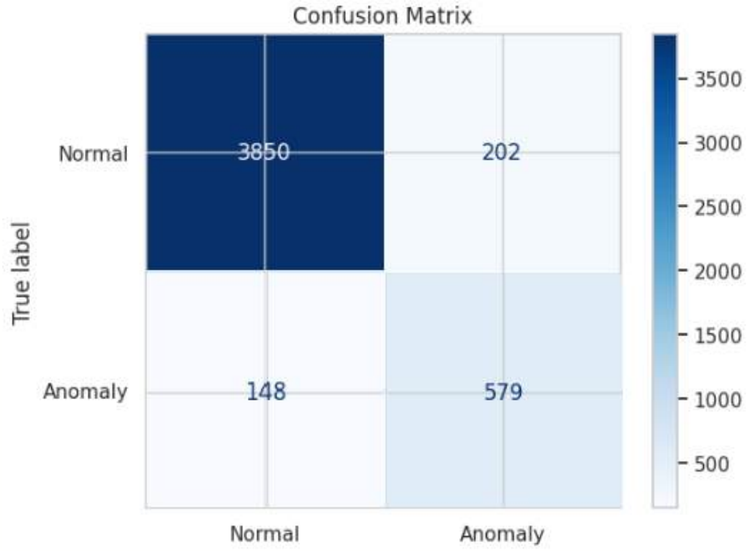
Current Progress

Accuracy - Isolation forest

```
merged_dataset.isnull().sum()

merged_dataset['True Anomaly'].fillna(0, inplace=True)

merged_dataset['True Anomaly'] = merged_dataset['True Anomaly'].astype(int)

accuracy = accuracy_score(merged_dataset['True Anomaly'], merged_dataset['Predicted Anomaly'])

accuracy
```

```
<ipython-input-171-41a8b70877da>:6: FutureWarning: A value is trying to be set on a copy of a DataFrame or Series through chained assignment using an inplace method.
The behavior will change in pandas 3.0. This inplace method will never work because the intermediate object on which we are setting values always behaves as a copy.

For example, when doing 'df[col].method(value, inplace=True)', try using 'df.method({col: value}, inplace=True)' or df[col] = df[col].method(value) instead, to perform the operation inplace on the

  merged_dataset['True Anomaly'].fillna(0, inplace=True)
0.8365766809840343
```





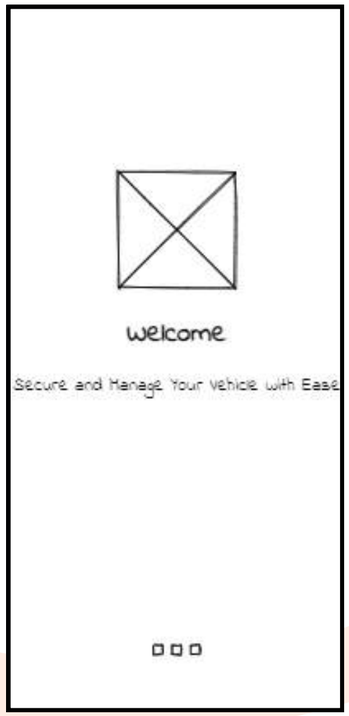
Current Progress

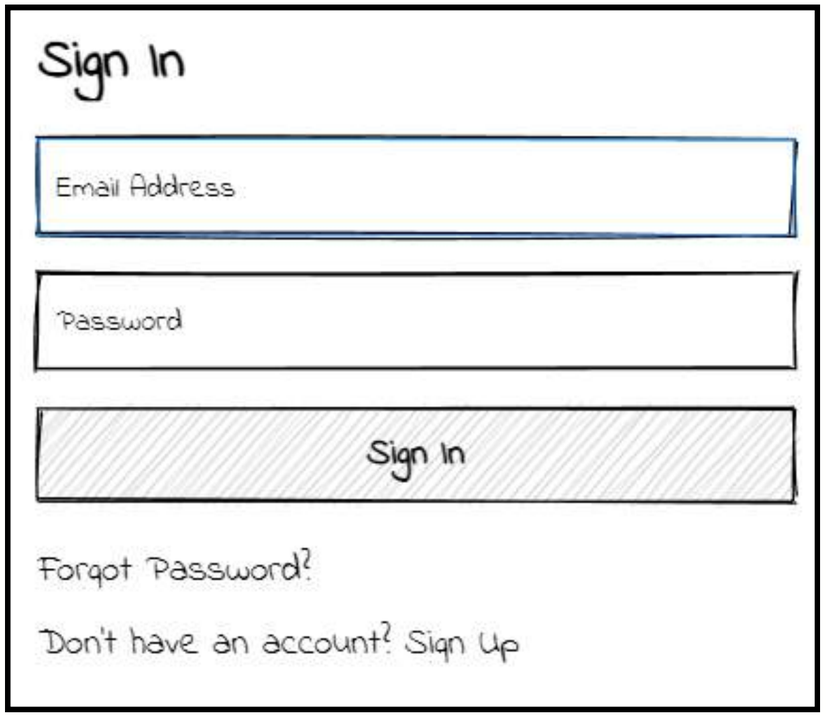
Accuracy - Autoencoders


```
3/3 ━━━━━━━━━━━━━━━━━━━━ 0s 3ms/step
3/3 ━━━━━━━━━━━━━━━━━━━━ 0s 3ms/step
Normal Data Metrics: Accuracy=0.9436619718309859, Precision=0.0, Recall=0.0, F1=0.0
/usr/local/lib/python3.10/dist-packages/sklearn/metrics/_classification.py:1531: UndefinedMetricWarning: Recall is ill-defined and being
  _warn_prf(average, modifier, f"{metric.capitalize()} is", len(result))
```

Current Progress

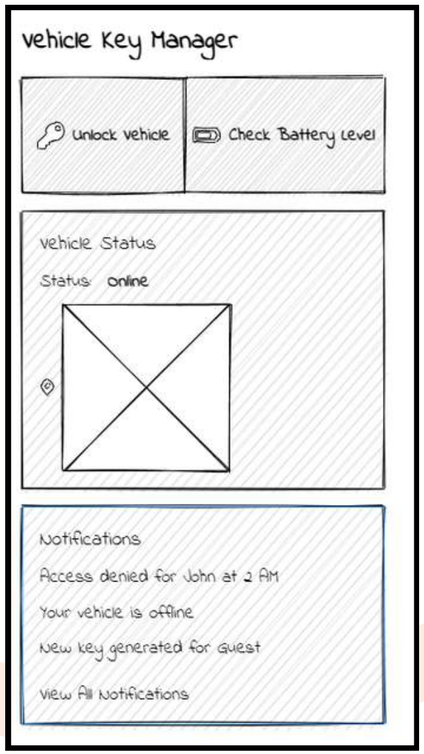
Wireframes

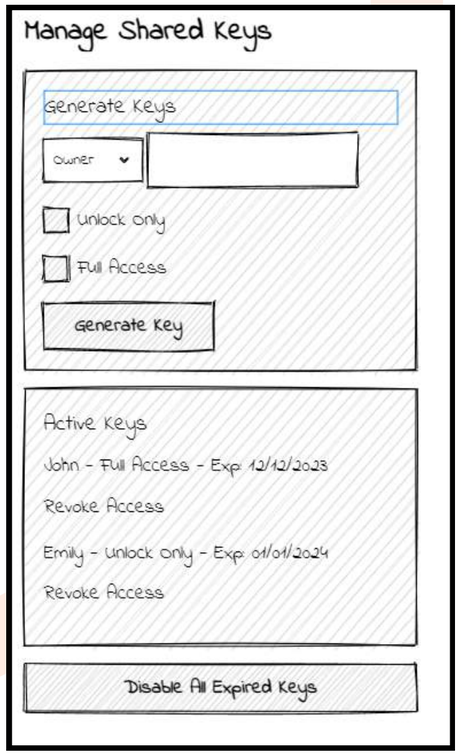


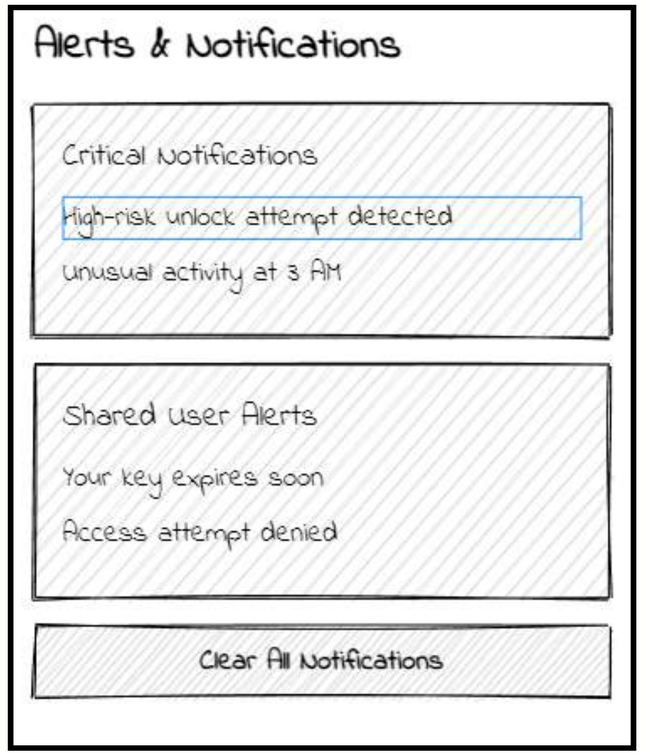


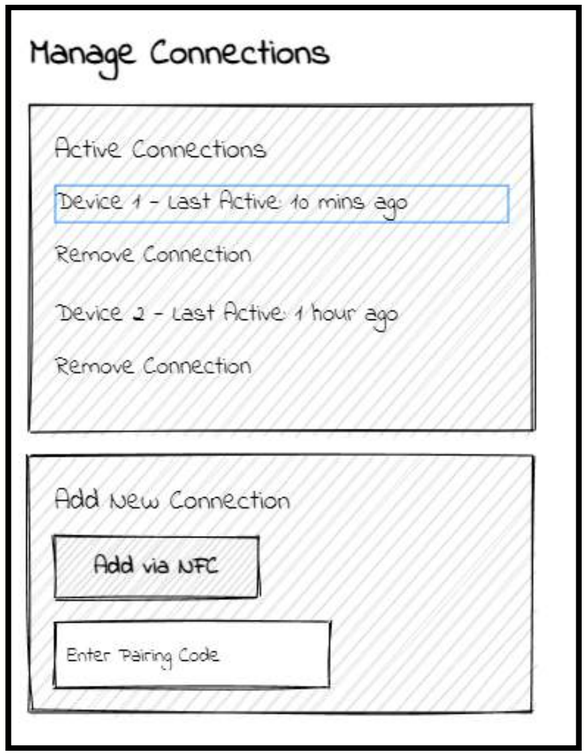
Current Progress

Wireframes



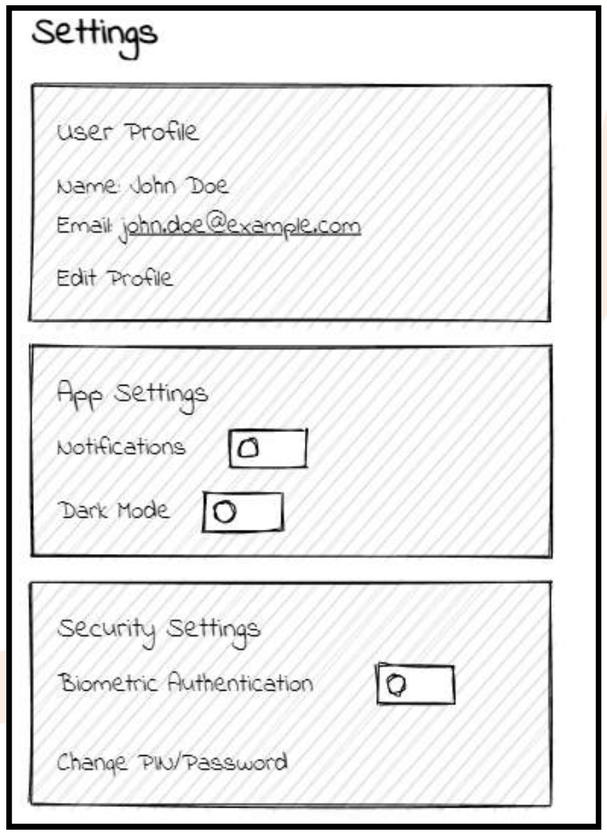


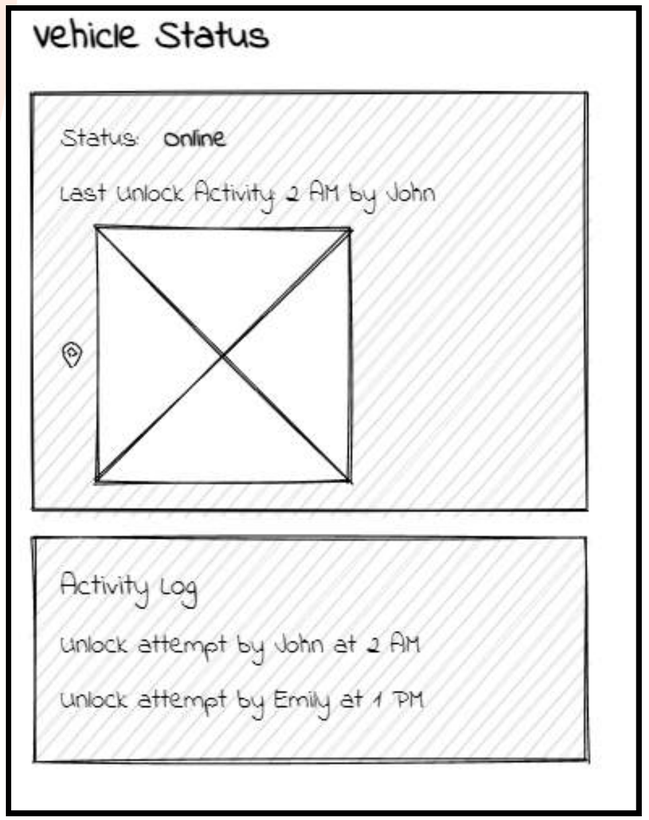




Current Progress

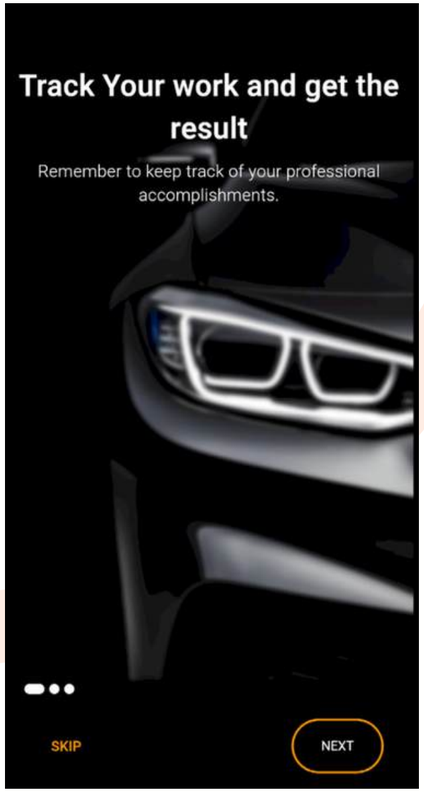
Wireframes

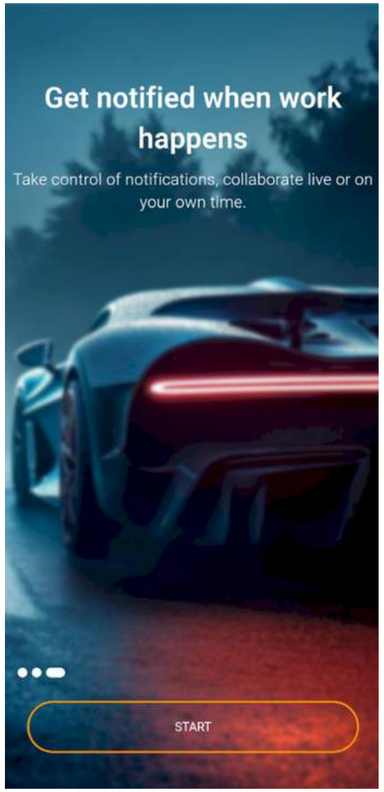


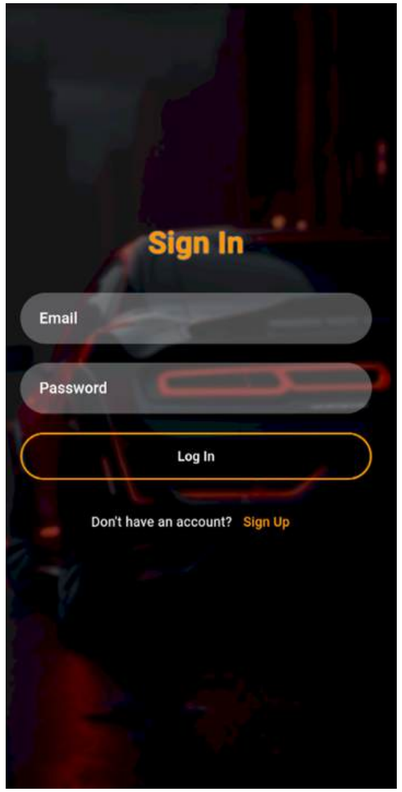


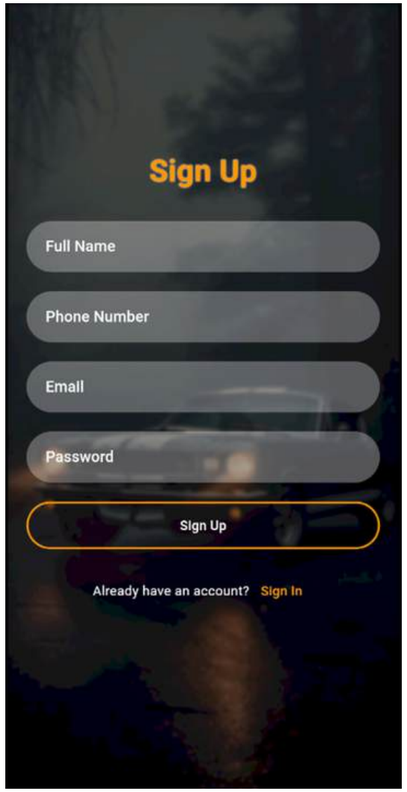
Current Progress

Designed UI









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,

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

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

Incorporating Machine Learning

Adds a proactive layer to traditional authentication by detecting potential threats before authentication. Enhances efficiency and precision in mitigating black hole attacks in real-time.

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	ML-Based Detection
Research [1]	✓	✗	✓	✗	✗
Research [2]	✗	✓	✗	✗	✗
Research [3]	✗	✓	✗	✗	✗
Proposed Solution	✓	✓	✓	✓	✓

OBJECTIVES

Completed Objectives

- **Machine Learning Model:**

Developed a model to detect black hole attacks by classifying nodes as normal or malicious using dataset-driven training.

- **Setup Simulation Environment:**

Set up a simulation environment on Ubuntu using NS-3 and SUMO.Simulated vehicular communication scenarios with normal and black hole-affected nodes.

Ongoing Objectives

- **Implementing ECC Framework:**

Currently working on refining Elliptic Curve Cryptography (ECC) for efficient and lightweight authentication in vehicular networks.

- **Integration of ML Model:**

Work in progress to integrate the trained ML model with the simulation to enable real-time detection of black hole attacks.

OBJECTIVES

Future Objectives

- **Real-Time Demonstration:**

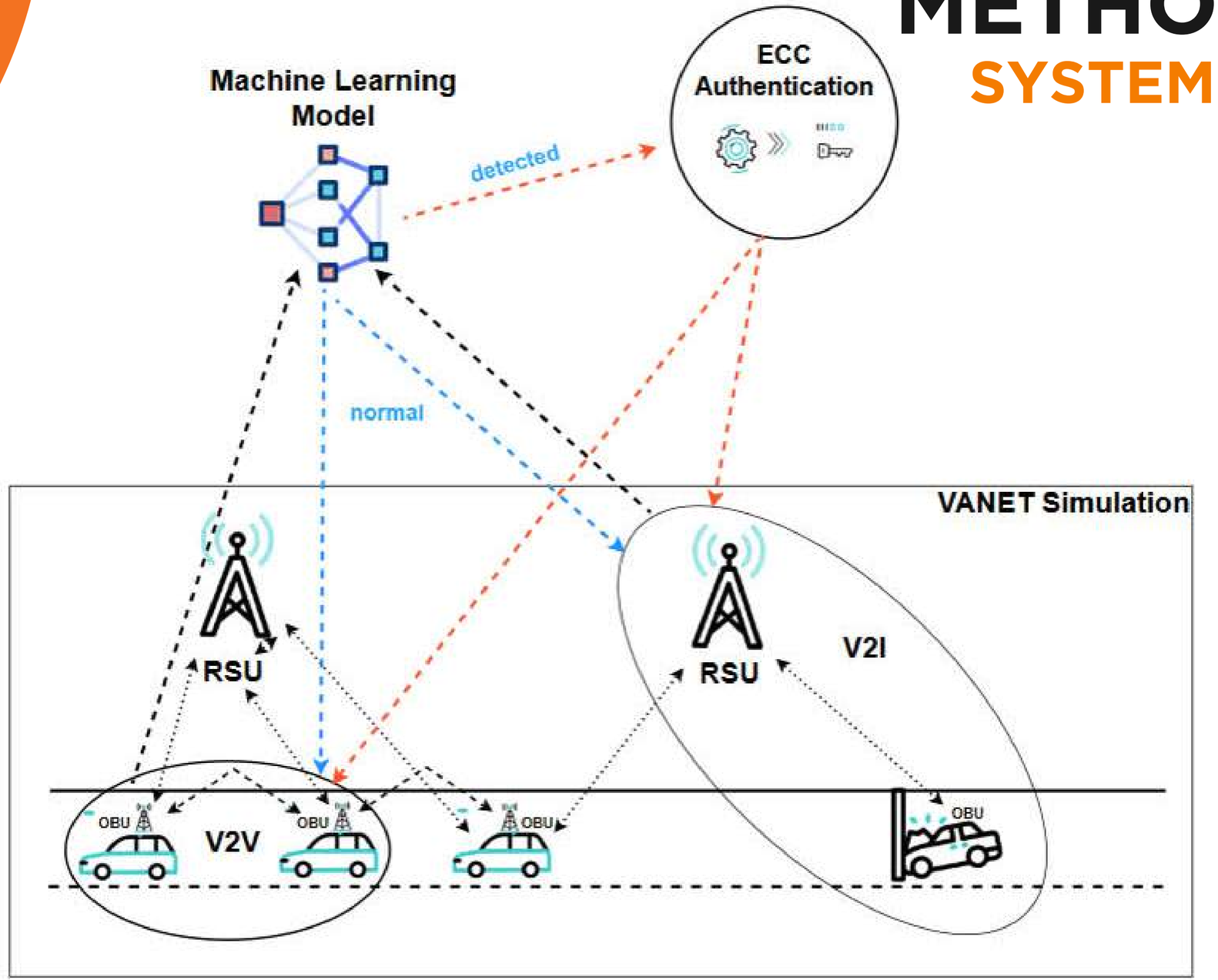
Fully integrate the ML model and ECC in the simulation for real-time attack detection and response.

- **System Validation:**

Test the integrated system in more extensive, realistic vehicular scenarios to validate performance and scalability.

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

DATA COLLECTION

type	rcvTime	pos_0	pos_1	pos_noise_0	pos_noise_1	spd_0	spd_1	spd_noise_0	spd_noise_1	acl_0	acl_1	acl_noise_0	acl_noise_1	hed_0	hed_1	hed_noise_0	hed_noise_1	attack
GPS	0	-109.573	287.549	-3.92907267	6.00016271	27.7892	15.7051	-0.77524956	0.53365519	1.9562	-1.668	-0.2554996	-0.39004892	-118.5	119.19	-1.21592946	-1.05246344	1
BSM	1.001	487.3762	-339.877	-6.14722937	5.72010904	26.6934	19.1428	-1.57825401	1.193406939	0.8389	1.6362	-0.20438355	-0.24988099	157	-51.43	-4.76071093	0.266247784	0
BSM	2.002	-24.961	96.0545	-8.01048327	-2.70920453	16.901	9.90384	-0.15620927	0.185081125	-0.44	-1.009	0.18866933	0.09863776	-5.442	-41.62	-3.8942819	4.336322026	0
BSM	3.003	-66.1353	-3.40851	3.34910331	-8.13506081	14.0279	14.7598	-1.07674088	0.856007578	-2.238	-2.603	0.1370648	0.04612584	-165.1	-116.7	-2.49653072	1.083006623	0
BSM	4.004	-31.6757	-279.222	1.86460217	5.37779842	26.8281	15.9346	-0.78015121	0.913671091	0.6292	-0.065	-0.48538901	-0.42504498	-1.542	-19.81	2.31002245	1.009585707	0
BSM	5.005	203.6874	426.287	-4.15377449	-3.42282051	2.54312	12.6945	1.195901308	-0.00681106	2.2466	1.0418	0.34262087	-0.24145896	159.75	144.61	4.41377672	-4.39494849	1
BSM	6.006	34.25132	391.431	-9.83908539	-1.5208741	14.1455	12.2568	-0.46128052	0.362185445	-1.714	-0.254	0.25109079	0.35001234	-11.59	106.09	-2.8274189	2.808411489	0
BSM	7.007	384.7821	194.719	6.59392492	4.82176345	1.79338	4.46311	1.721635686	0.568678707	2.6735	-1.027	0.24033991	-0.41177207	102.64	-142.4	-2.4351974	-0.2358924	0
BSM	8.008	-387.494	-144.494	-5.22389335	2.89626984	15.6878	22.051	-1.68864585	-1.10590493	-1.711	-0.872	-0.01367979	-0.2472051	176.45	135.47	1.53727805	-1.19698558	0
BSM	9.009	367.2151	-231.078	2.84039923	7.82128717	11.6286	17.9625	-0.90666658	-1.64848143	-0.162	-2.807	0.15720348	-0.12981764	5.0423	95.172	-4.28644839	-2.49148548	0
BSM	10.01	270.2904	-320.605	-1.9567971	-6.07710188	26.4405	18.862	1.517657597	0.897291753	0.7881	-2.428	-0.02562855	0.48435128	-21.96	-37.49	3.00874143	2.19830276	0
BSM	11.011	-72.3277	-125.2	-0.28567547	7.84875999	0.6829	13.5006	1.146767807	1.692878894	2.7227	-2.578	0.24249633	-0.14485633	39.64	-8.132	1.81204948	0.138166832	1
GPS	12.012	491.7047	483.566	-0.21224239	5.12773859	8.98145	27.1851	1.028145634	-1.22378665	-2.593	-0.608	0.05939683	0.3475178	155.81	170.9	-0.80194525	-2.97677892	0
GPS	13.013	112.4314	360.307	8.97775526	-0.16373168	10.9056	21.0167	1.03628613	0.051373114	1.0984	2.595	0.19072192	-0.33870395	-4.345	-146.7	-4.30656056	-4.48125838	0
BSM	14.014	-36.3064	249.837	-9.53637425	9.37343745	9.26546	11.662	0.481146415	0.535353154	2.8029	1.9117	0.18607732	-0.23495763	-134.4	178.93	3.68008709	4.035118408	1
BSM	15.015	485.9472	-35.8542	8.89175767	9.79398406	10.0452	2.24937	1.282195174	-0.68787887	-0.276	2.5092	0.12541061	-0.47562098	-18.62	-51.46	0.79923853	2.408142257	0
BSM	16.016	458.8979	-499.403	-5.36718108	6.68463119	15.0783	8.25409	1.679009444	-1.1907191	-0.001	-2.342	-0.35703326	-0.12757653	-104.3	141.33	4.59693799	2.948079365	0
BSM	17.017	-444.294	-15.016	6.7172673	8.901198	2.99519	25.6172	-1.82374056	0.237604327	-1.404	-1.944	0.1157172	-0.46150701	77.844	39.062	4.94455033	-0.47941149	0
GPS	18.018	-165.923	452.456	4.65923668	9.80266474	19.0329	17.0624	0.874774843	-0.41158079	1.0634	-1.021	0.01962723	-0.05960059	161.55	-174.6	-4.20476081	-4.77258058	0
GPS	19.019	-337.977	165.744	7.84104536	-1.98463992	15.9222	21.8722	1.515575545	-1.83359728	2.9916	-1.155	0.01882971	0.44204808	136.53	37.437	3.24124895	-4.90507828	0
BSM	20.02	179.0575	-312.58	-7.64693144	-7.66852348	27.9298	11.3708	1.146500411	-0.18253599	-1.507	0.7029	0.31849702	-0.41913124	2.1497	171.12	2.21996146	-2.66770485	0
GPS	21.021	355.5466	9.12712	-2.81577275	-1.18228034	8.99494	20.0166	1.532603655	-1.72097476	-2.13	2.1239	0.14134932	0.0138211	-110.3	-51.71	-1.3406489	1.362599762	0
BSM	22.022	433.8472	136.607	7.12899351	4.76535354	29.962	8.02722	1.167431643	0.486379737	2.4733	-2.731	-0.03913758	0.1768655	-99.39	-70.05	-3.72447216	-0.65671572	0
BSM	23.023	-467.657	-315.289	4.11030559	-3.30911639	17.747	0.67886	-0.06882004	0.137372679	-0.559	2.8223	-0.47828002	-0.02077663	72.418	-83.49	3.84727347	2.48471651	0
BSM	24.024	314.5719	-221.636	-7.56557662	-4.72324124	6.7297	8.89431	-1.13446529	-1.52635854	1.8847	-0.023	-0.0434428	0.08268107	171.32	-63	-1.52445362	0.169633265	0
GPS	25.025	-492.236	334.508	6.94835715	2.39924395	8.58744	3.54157	-0.63898206	-0.22426971	1.0643	2.9334	-0.13981662	-0.25868516	166.99	-28.03	1.17739122	-3.00359862	0
BSM	26.026	-316.11	-175.352	3.41252759	8.90227044	21.5095	20.4096	-0.61503423	1.422205149	2.415	-0.091	0.48613592	-0.24828194	-130	-3.824	-1.48215853	-2.28196081	0
BSM	27.027	-164.316	-35.8934	3.9454088	-2.19756839	27.7141	3.56874	1.692014623	-1.62796618	1.5155	-2.439	0.31782532	-0.16506873	-45.79	60.683	1.12109994	4.114547142	0
GPS	28.028	-395.084	310.617	8.81046967	-6.63857971	14.9232	15.0893	-1.32357214	1.964949764	-0.464	2.1464	-0.0836822	-0.36654321	132.15	148.62	-1.86174846	-4.01288613	0
GPS	29.029	139.2964	334.361	6.88242325	-7.16368756	3.95601	26.4202	-0.84244739	-0.83081606	1.059	0.0811	0.4747405	-0.40817439	163.42	176.74	0.88552794	3.433072989	0
BSM	30.03	184.4015	362.234	-1.25572288	-7.40811697	5.90686	0.75672	-0.18969665	0.02152143	1.6615	0.9727	0.06008518	-0.42572846	-131.7	24.131	-2.871787	1.185331184	1
BSM	31.031	-375.317	260.321	9.15027767	-3.48346204	2.55836	24.3636	-0.55131628	0.427924479	-0.202	-0.572	0.13435724	-0.39800496	-167.7	32.86	-4.79162647	-2.05170247	0
BSM	32.032	-220.175	411.922	-4.1813008	1.34559192	9.89706	7.68818	-0.64523786	-1.13557746	-0.034	1.088	0.16419827	-0.33075635	-46.39	111.95	-3.93996138	2.37065496	0

Data Set

The dataset was already cleaned and preproccessed

How These Factors Detect Blackhole Attacks

- **Packet Dropping Behavior:** Components like **rcvTime** and attack directly reveal dropped packets or delays caused by malicious nodes.
- **Inconsistent Vehicle Dynamics:** Fields like **pos, spd, and acl,** along with their noisy counterparts, help detect irregularities in movement patterns.
- **Tampered Data Patterns:** Noise components **(pos_noise, spd_noise, acl_noise, hed_noise)** highlight inconsistencies in communication reliability.
- **Directional Disruptions:** Changes in **hed** and its noise components can indicate malicious activities altering routing directions or data flow.

TRAINING MODEL

Data Pre-processing

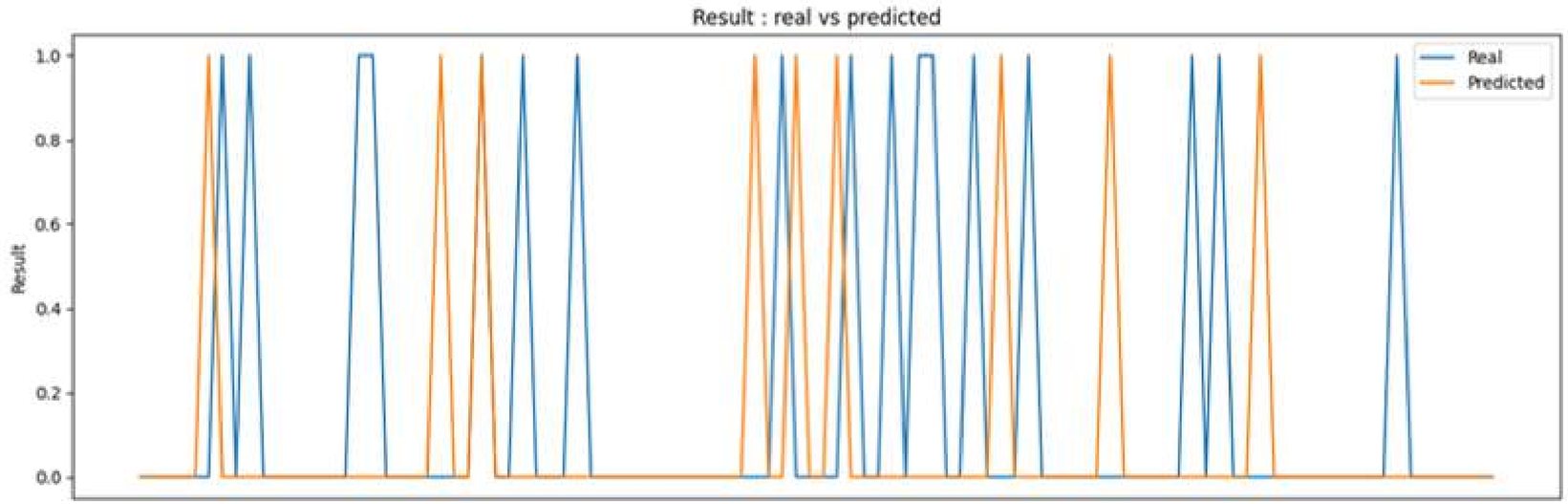
```
label_encoder = LabelEncoder()
data['type_num'] = label_encoder.fit_transform(data['type'])
```

Data Pre-processing

Model Training

```
from sklearn.svm import SVR
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.metrics import mean_squared_error

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=30)

def model_score(model):
    model.fit(X_train, y_train)
    acc = model.score(X_test, y_test)
    print(str(model)+ ' | ' +str(acc))
```

Model Training



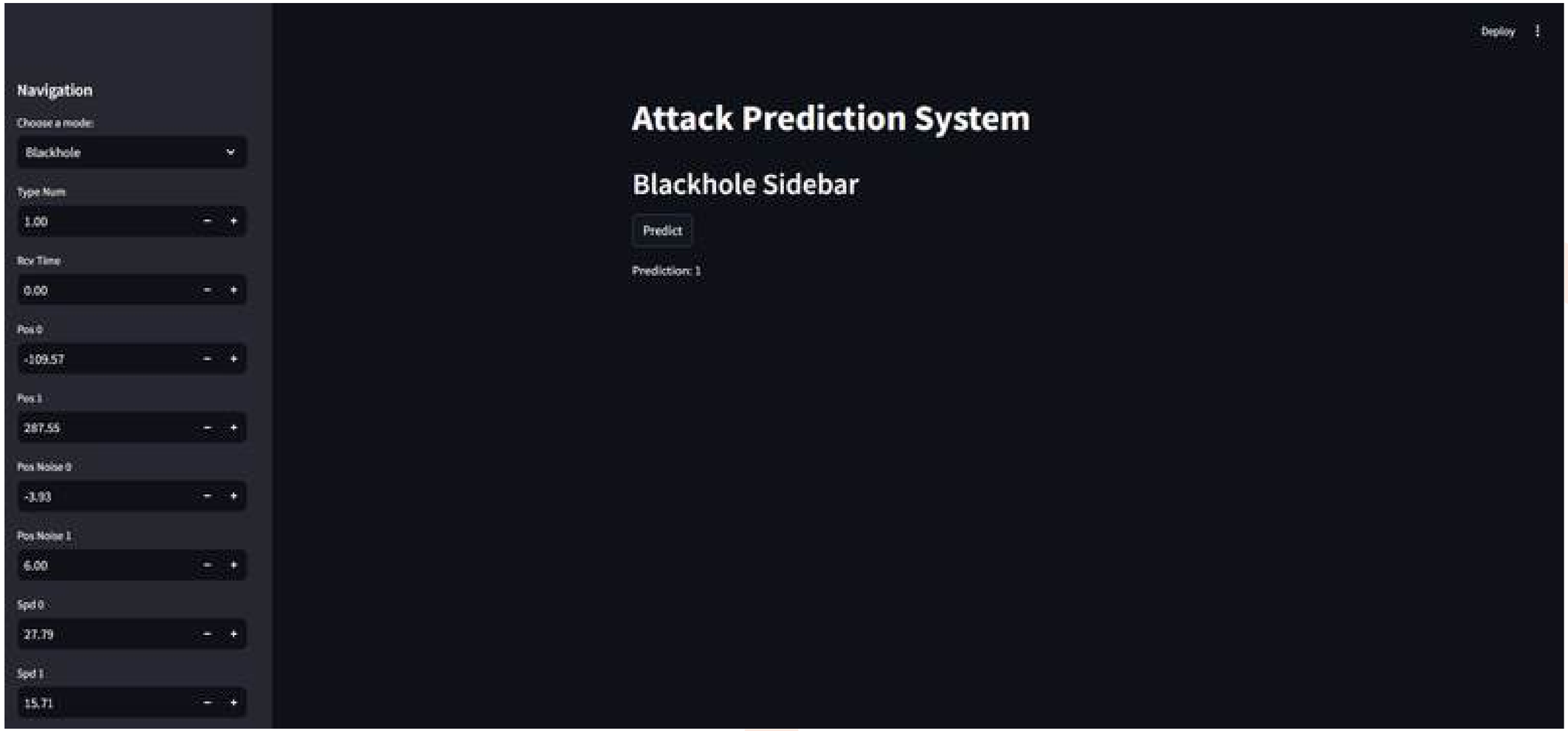
MODEL EVALUATION

```
from sklearn.ensemble import RandomForestClassifier
rf = RandomForestClassifier()
model_score(rf)

from sklearn.neighbors import KNeighborsClassifier
knn = KNeighborsClassifier(n_neighbors=3)
model_score(knn)

from sklearn.tree import DecisionTreeClassifier
dt = DecisionTreeClassifier()
model_score(dt)
```

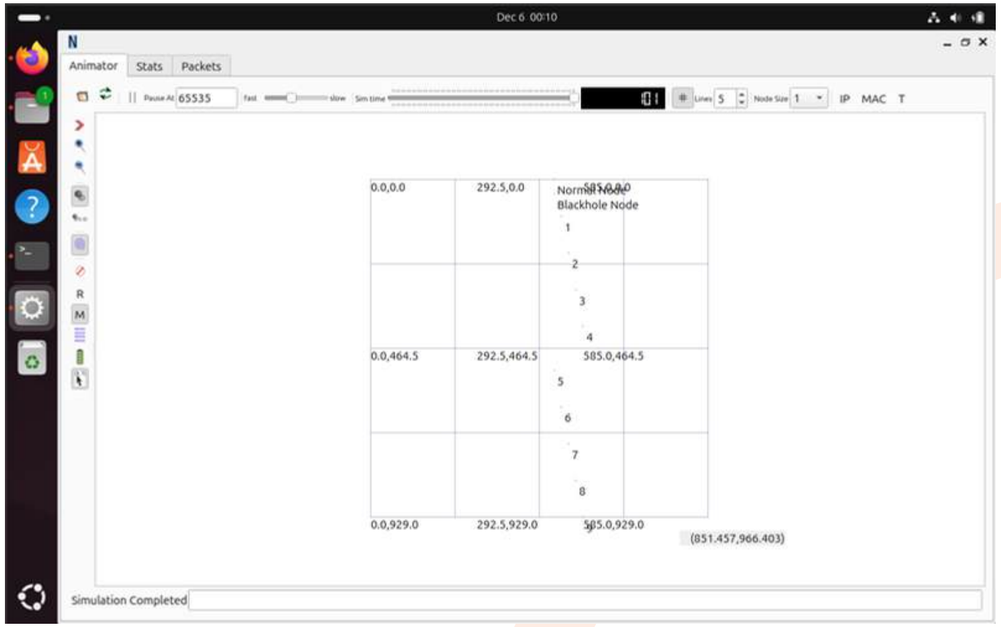
```
RandomForestClassifier() | 0.81
KNeighborsClassifier(n_neighbors=3) | 0.75
DecisionTreeClassifier() | 0.6433333333333333
```

Random Forest, K-Nearest Neighbors, and Decision Tree models were trained and optimized using Grid Search. The Random Forest model, with the highest accuracy, was selected for predictions.

CREATE A USER INTERFACE



Testing NS3, NetAnim and Sumo




```
osboxes@osboxes:~/ns-3$ sumo
Eclipse SUMO sumo Version 1.21.0
 Build features: Linux-6.8.0-45-generic x86_64 GNU 13.2.0 Release FMI Proj GUI Intl SWIG Eigen GDAL GL2PS
 Copyright (C) 2001-2024 German Aerospace Center (DLR) and others; https://sumo.dlr.de
 License EPL-2.0: Eclipse Public License Version 2 <https://eclipse.org/legal/epl-v20.html>
 Use --help to get the list of options.
```

REQUIREMENTS

Functional Requirements:

- **Black Hole Detection:** Identify black hole attacks in V2V and V2I communication.
- **Authentication Mechanism:** Use ECC to authenticate or revoke nodes after detection.
- **Real-time Simulation:** Simulate and demonstrate attack scenarios and countermeasures.
- **Data Logging:** Record communication data for analysis and validation.

Non- Functional Requirements:

- High accuracy
- low latency
- Availability
- User friendly Visualisation
- Scalability

Technical Requirements:

- **NS-3 and NetAnim:** Simulation environment for vehicular networks.
- **Python & ML Libraries:** Develop and train the detection model.
- **SUMO Integration:** Optional for mobility simulation of vehicles.
- **Hardware Requirements**: Ubuntu system with sufficient resources for simulation and training.

TOOLS & TECHNOLOGIES

Technologies

- **NS3 and NetAnim**

Network simulation and visualization.

- **SUMO**

Vehicular mobility modeling.

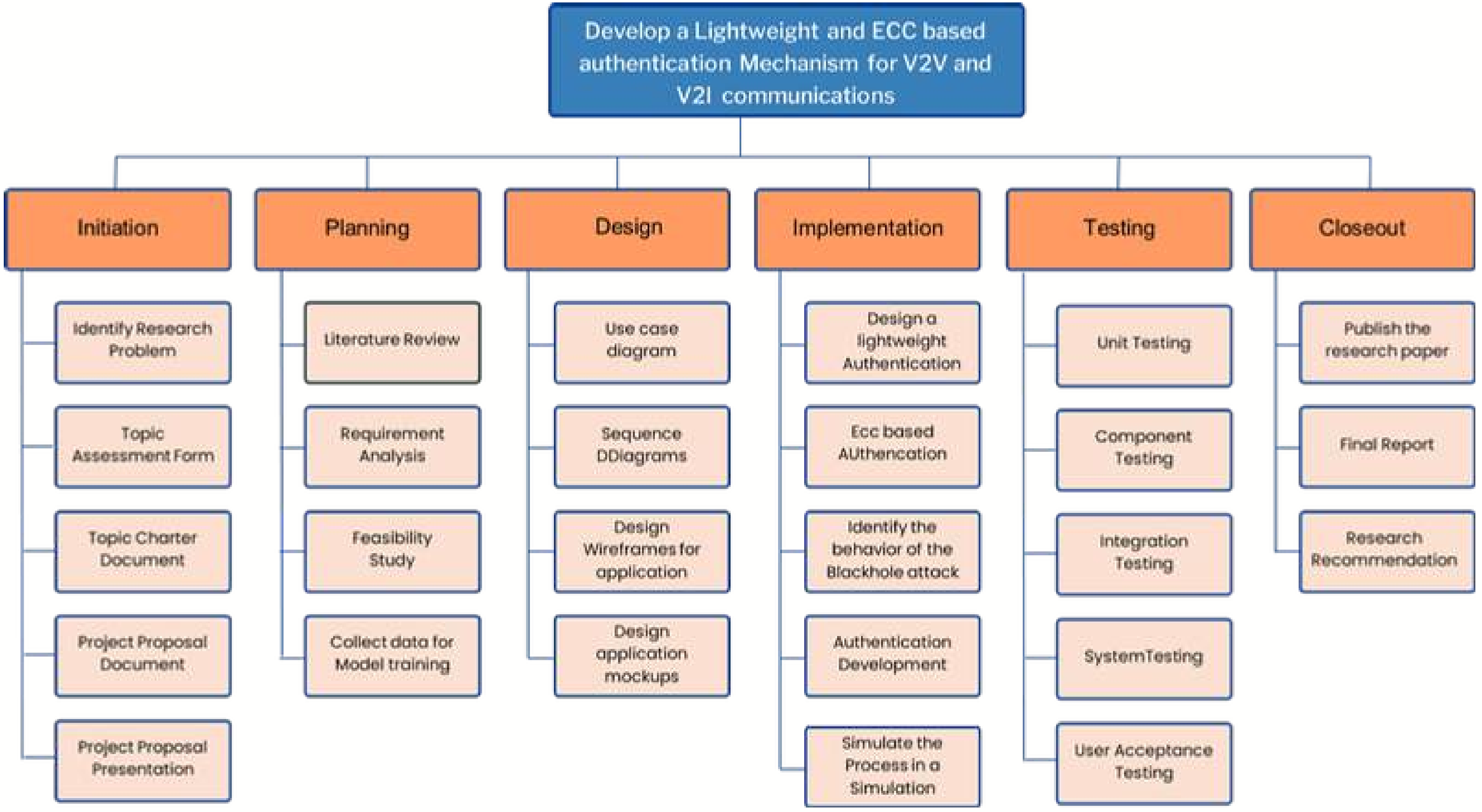
- **Python**

Algorythm & Architechtures

- **Random Forest:** Best-performing model for attack detection.
- **Elliptic Curve Cryptography (ECC):**
- Lightweight authentication mechanism.

Techniques

- **Feature Engineering:** Identify critical factors like position, speed, and header values.
- **Simulation:** Demonstrate attack behavior and mitigation strategies visually.


Develop a Lightweight and ECC based authentication Mechanism for V2V and V2I communications
Initiation
Identify Research Problem
Topic Assessment Form
Topic Charter Document
Project Proposal Document
Project Proposal Presentation
Planning
Literature Review
Requirement Analysis
Feasibility Study
Collect data for Model training
Design
Use case diagram
Sequence DDiagrams
Design Wireframes for application
Design application mockups
Implementation
Design a lightweight Authentication
Ecc based AUthencation
Identify the behavior of the Blackhole attack
Authentication Development
Simulate the Process in a Simulation
Testing
Unit Testing
Component Testing
Integration Testing
SystemTesting
User Acceptance Testing
Closeout
Publish the research paper
Final Report
Research Recommendation

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).
- PUF-based authentication mechanisms face challenges in resisting predictive attacks and lack robust frameworks for real-world adversarial testing.

PUF-Physical Unclonable Function

- The Physical Unclonable Function (PUF) is a hardware-based security technology that uses the unique physical characteristics of devices to generate identifiers. This helps protect the device from being copied or tampered with.

On-Board Units (OBUs)

- On-Board Units (OBUs) are electronic devices installed in vehicles to enable communication with other vehicles, infrastructure, or systems.

Trusted Authority (TA)

- A Trusted Authority (TA) is a reliable organization or system that verifies identities, manages security credentials, and ensures trust in digital communications, such as in authentication or encryption processes.

Challenge Response Mechanism

- The Challenge-Response Mechanism is a security method where a system sends a random question (challenge) to a user or device, and the user/device must provide the correct answer (response) to prove their identity.

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.

OBJECTIVES

Completed Objectives

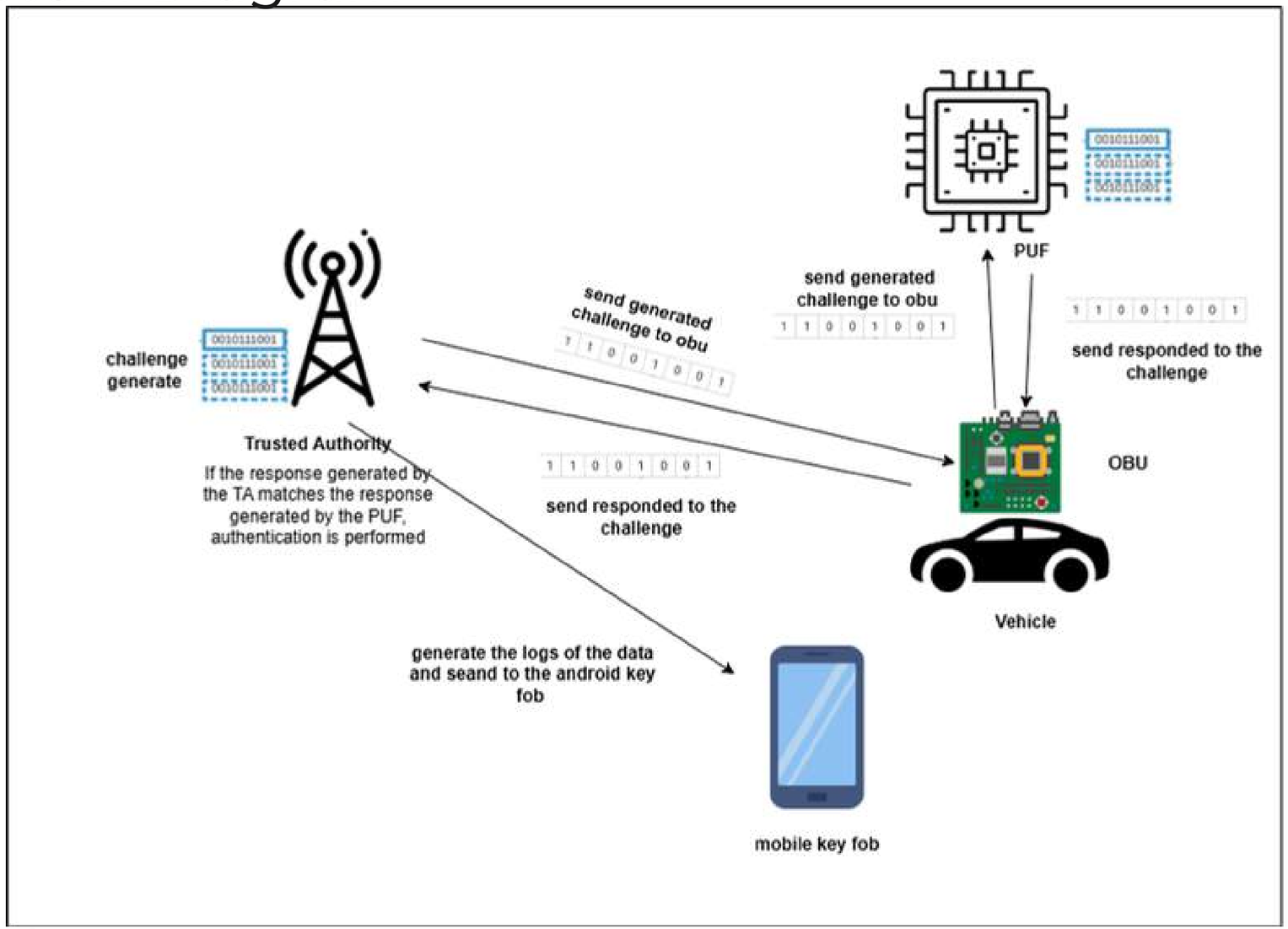
- implement the Challenge Response Mechanism using the Cryptographically Secure Pseudorandom Number Generators(CSPNG).
- Developed logging mechanism when genrate logs when authentication happen and save the challenges and the response.
- An ML model is trained to simulate attacks, rigorously testing the PUF's robustness

Ongoing Objectives

- Developed the Physical Unclonable Function (PUF) technologies and their use cases in security systems.
- 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

- Performance Evaluation
- Data Encryption and Decryption

Hardware Components Needed

- Microcontroller/FPGA (Optional)
- Inverters (Odd Number)- ensuring uniqueness and unpredictability in responses.
- Multiplexers (MUX) -
- Counters
- Comparator
- Clock Source
- Power Supply Circuit
- Pull-Up/Pull-Down Resistors
- Output Buffer

Challenge-Response Mechanism

Challenge generate

The Challenge-Response System uses secure cryptographic challenges and hash-based response validation for user authentication. It ensures detailed logging, robust file management, and strong security against replay attacks.

```python
import hashlib
from datetime import datetime
import logging
from logging.handlers import RotatingFileHandler
import atexit

# Configure enhanced logging
def configure_logging():
    logger = logging.getLogger("ChallengeResponseGenerator")
    logger.setLevel(logging.INFO)
    handler = RotatingFileHandler(
        "challenge_response.log", maxBytes=10000, backupCount=5
    )
    formatter = logging.Formatter("%(asctime)s - %(levelname)s - %(message)s")
    handler.setFormatter(formatter)
    logger.addHandler(handler)
    return logger

logger = configure_logging()

# Handle file operations
class ChallengeFileHandler:
    def __init__(self, filename="challenges_responses.txt"):
        self.filename = filename
```

```
OUTPUT  PROBLEMS  TERMINAL  PORTS  DEBUG CONSOLE

PS C:\Users\Chamal Jayasinghe\Desktop\New folder (9)> & "C:/Users/Chamal Jayasinghe/AppData/Local/Microsoft/WindowsApps/python3.11.exe" "c:/Users/Cham
al Jayasinghe/Desktop/New folder (9)/crpserver.py"
Generating a challenge...
Generated Challenge: 68CC79F7A1953AB3
Enter the PUF-generated response for the challenge:
```

Challenge-Response Mechanism

Responses Generate

crpclient.py > generate_expected_response

```python
import hashlib

# Generate the expected response for a given challenge (client-side)
def generate_expected_response(challenge):
    """
    Generates the expected response for a given challenge.
    Uses a hash function for simplicity.

    :param challenge: The challenge string.
    :return: A hexadecimal string representing the response.
    """
    hashed_response = hashlib.sha256(challenge.encode('utf-8')).hexdigest().upper()
    return hashed_response[:16]  # Return the first 16 hex characters for simplicity

def main():
    print("Enter the received challenge:")

    try:
        # Step 1: Get the challenge as input from the user
        challenge = input("Challenge: ").strip().upper()

        # Step 2: Generate the expected response based on the challenge
```

OUTPUT PROBLEMS TERMINAL PORTS DEBUG CONSOLE

```
PS C:\Users\Chamal Jayasinghe\Desktop\New folder (9)> & "C:/Users/Chamal Jayasinghe/AppData/Local/Microsoft/Wi
al Jayasinghe/Desktop/New folder (9)/crpclient.py"
Enter the received challenge:
Challenge:  68CC79F7A1953AB3
Calculated Response: E7C785503569C3B2
Thank you for using the Challenge-Response Client!
PS C:\Users\Chamal Jayasinghe\Desktop\New folder (9)>
```

Challenge-Response Mechanism

authentication successful

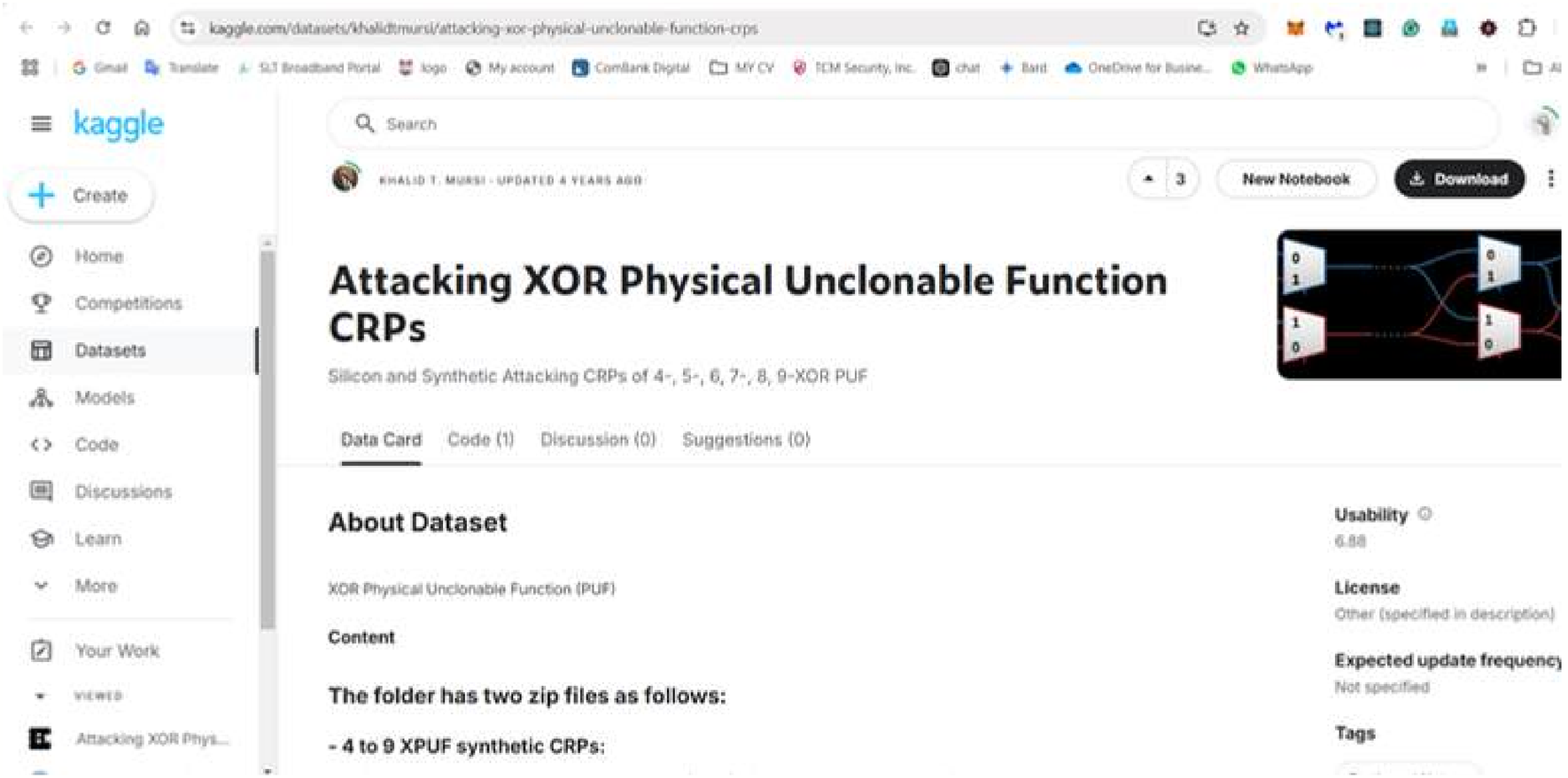
```
OUTPUT  PROBLEMS  TERMINAL  PORTS  DEBUG CONSOLE

PS C:\Users\Chamal Jayasinghe\Desktop\New folder (9)> & "C:/Users/Chamal Jayasinghe/AppData/Local/Microsoft/WindowsApps
al Jayasinghe/Desktop/New folder (9)/crpserver.py"
Generating a challenge...
Generated Challenge: 68CC79F7A1953AB3
Enter the PUF-generated response for the challenge: E7C785503569C3B2
Authentication Successful!
Thank you for using the Challenge-Response System!
PS C:\Users\Chamal Jayasinghe\Desktop\New folder (9)>
```

Log generate

challenge_response.log

```
1  2024-12-06 11:09:15,715 - INFO - Challenge-response system started.
2  2024-12-06 11:09:22,445 - ERROR - Invalid user input for response.
3  2024-12-06 11:09:35,465 - INFO - Challenge-response system started.
4  2024-12-06 11:10:04,681 - INFO - Authentication successful for challenge.
5  2024-12-06 11:10:04,682 - INFO - Challenge and Response saved: Challenge: 7B1946FB8FEE7A51, Response: 9087A569E4345223, Result: Success
6  2024-12-06 11:10:04,683 - INFO - Challenge-response system finished.
7  2024-12-06 11:10:37,252 - INFO - Challenge-response system started.
8  2024-12-06 11:11:03,757 - INFO - Authentication successful for challenge.
9  2024-12-06 11:11:03,758 - INFO - Challenge and Response saved: Challenge: 0F4B6A0D40EE8805, Response: 047AB64E524D8630, Result: Success
10 2024-12-06 11:11:03,758 - INFO - Challenge-response system finished.
11 2024-12-06 11:13:40,906 - INFO - Challenge-response system started.
12 2024-12-06 11:20:19,011 - INFO - Authentication successful for challenge.
13 2024-12-06 11:20:19,014 - INFO - Challenge and Response saved: Challenge: 68CC79F7A1953AB3, Response: E7C785503569C3B2, Result: Success
14 2024-12-06 11:20:19,015 - INFO - Challenge-response system finished.
15
```

Dataset Used to Train Attack ML Model for Testing PUF Response Unpredictability



https://www.kaggle.com/datasets/khalidtmursi/attacking-xor-physical-unclonable-function-crps

Dataset Used to Train Attack ML Model for Testing PUF Response Unpredictability

```
2E14E835024DD8C9;1
7FBD869A2EFF6F2E;1
67ADE2FFD8C8C393;0
1099FD640A5DD5F8;1
5D35D5C98672A65D;1
E8356C2EC7BB34C2;1
044CC09300EB8127;1
BC2FD2F81CB78B8C;1
D292A35DBDD353F1;0
C22931C23EF2DA56;1
BDA77E27B2CA1EBB;1
AFC1888CE40D2120;0
3B2B50F1556FE185;0
BA98D75641A65FEA;1
40BE1BBB9B649C4F;1
984F1E200D5E96B4;1
43FFDE85FA484F19;1
7E845CEA7CD5C57E;0
3A90994F67BAF9E3;1
22D893B445ABEC48;1
9A104C19595C9CAD;1
BAEBC27E9D810B12;0
```

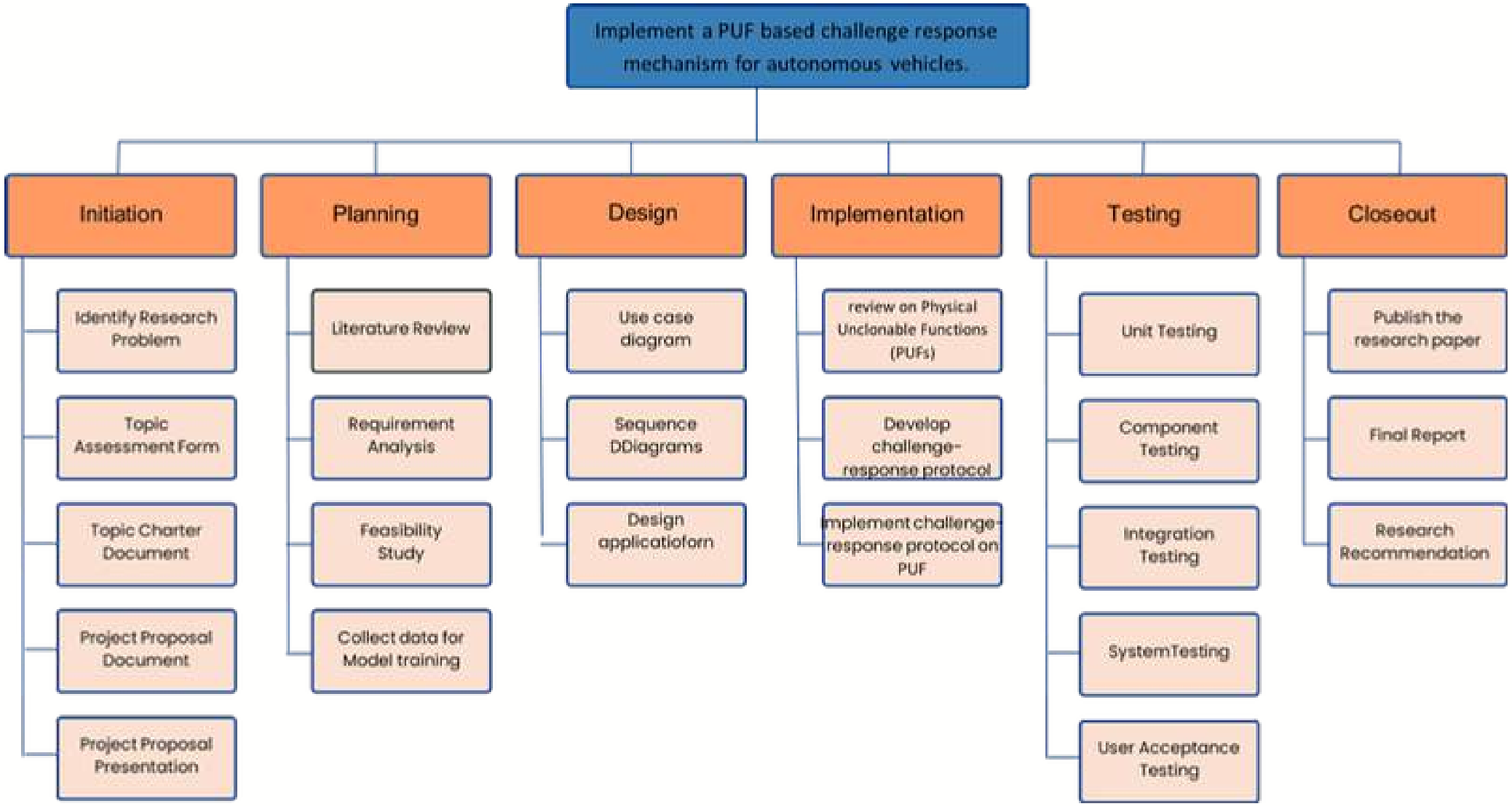
Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
4XOR_64bit_LUT_2239B_attacking_1M	Text Document	10,325 KB	No	18,555 KB	45%	10/16/2020 4:58 PM
5XOR_64bit_LUT_2239B_attacking_1M	Text Document	10,325 KB	No	18,555 KB	45%	10/16/2020 4:58 PM
6XOR_64bit_LUT_2239B_attacking_1M	Text Document	10,325 KB	No	18,555 KB	45%	10/16/2020 4:58 PM
7XOR_64bit_LUT_2239B_attacking_5M	Text Document	51,617 KB	No	92,774 KB	45%	10/16/2020 4:58 PM
8XOR_64bit_LUT_2239B_attacking_5M	Text Document	51,617 KB	No	92,774 KB	45%	10/16/2020 4:58 PM
9XOR_64bit_LUT_2239B_attacking_5M	Text Document	51,617 KB	No	92,774 KB	45%	10/16/2020 4:58 PM

The firs column shows the input challenges printed in hexadecimal.
The second column indicates the output response of the giving challenge.

Dataset Used to Train Attack ML Model for Testing PUF Response Unpredictability

```
RandomForestRegressor() | -0.011215328177698103
KNeighborsClassifier(n_neighbors=3) | 0.49856
LogisticRegression() | 0.51992
Lasso() | -7.1227827189712666-06
DecisionTreeRegressor() | -0.9965516101635832
Ridge() | 0.0005188718068925846
```

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 is crucial in modern applications, from navigation to autonomous vehicles.
- Integration of GPS into critical systems has advanced rapidly, improving efficiency and autonomy.
- Increased reliance on GPS makes systems vulnerable to threats, particularly spoofing attacks.
- Spoofing involves transmitting fake GPS signals to mislead navigation systems.
- This can result in erroneous positioning data, leading to misrouting of vehicles, accidents, or unauthorized access to restricted areas.

OBJECTIVES

Main Objectives

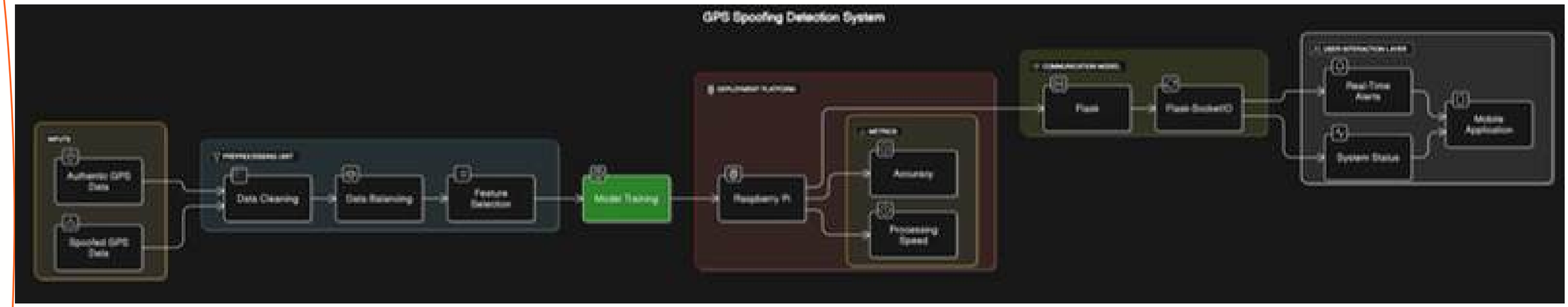
- The objective is to design and deploy a machine learning-based GPS spoofing detection system that shall be capable of real-time analysis and immediate threat notification.

Sub Objectives

- Collect high-quality GPS data (authentic and spoofed) for model training and validation.
- Evaluate and select suitable machine learning/deep learning models (e.g., RF, FCNN, KNN, SVM, XGBoost) for GPS anomaly detection.
- Implement the detection system on an embedded device (e.g., Raspberry Pi) for real-world deployment.
- Sending real-time alerts and system status to the Android app to enhance user interaction.
- Measure system performance using key metrics: accuracy, false positive rate, and processing speed to ensure reliability and robustness.

METHODOLOGY

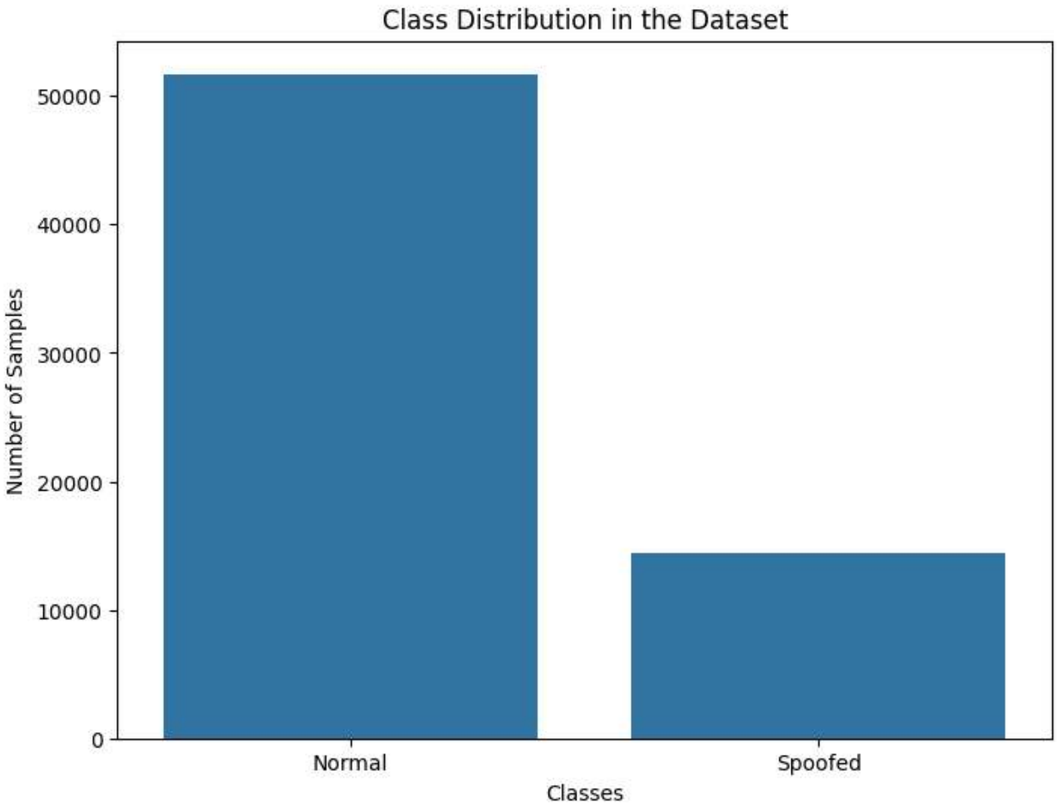
System Diagram

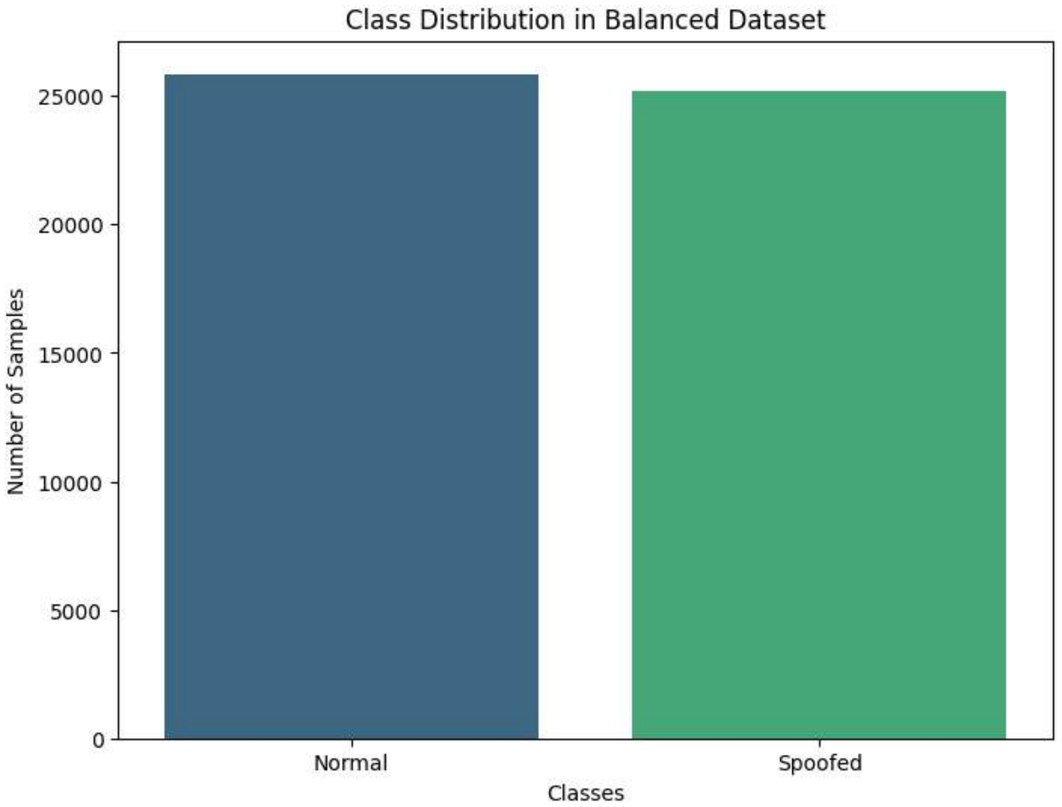


CURRENT PROGRESS

Balancing Data-set

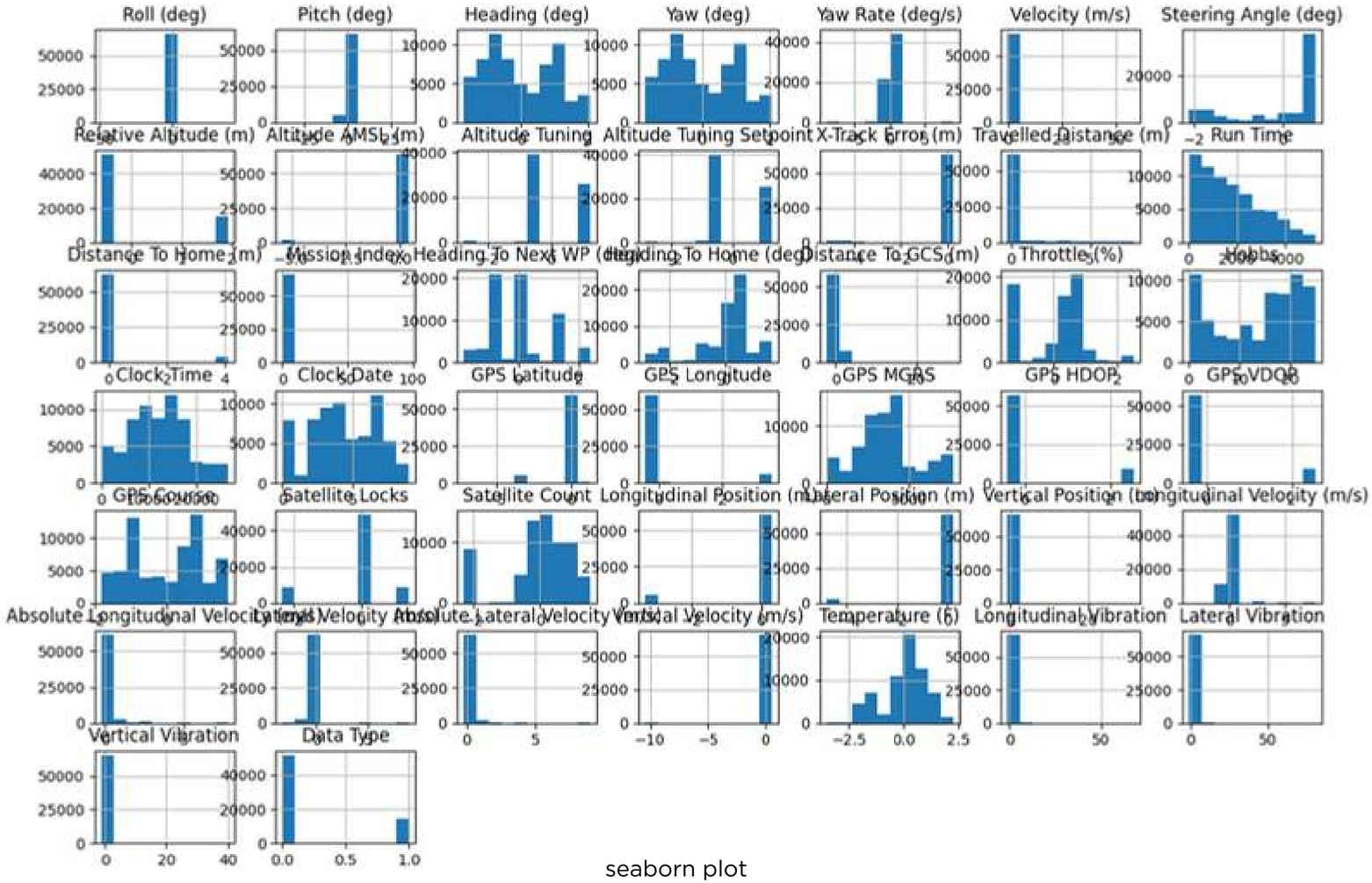
- SMOTE
- RandomunderSampler





CURRENT PROGRESS

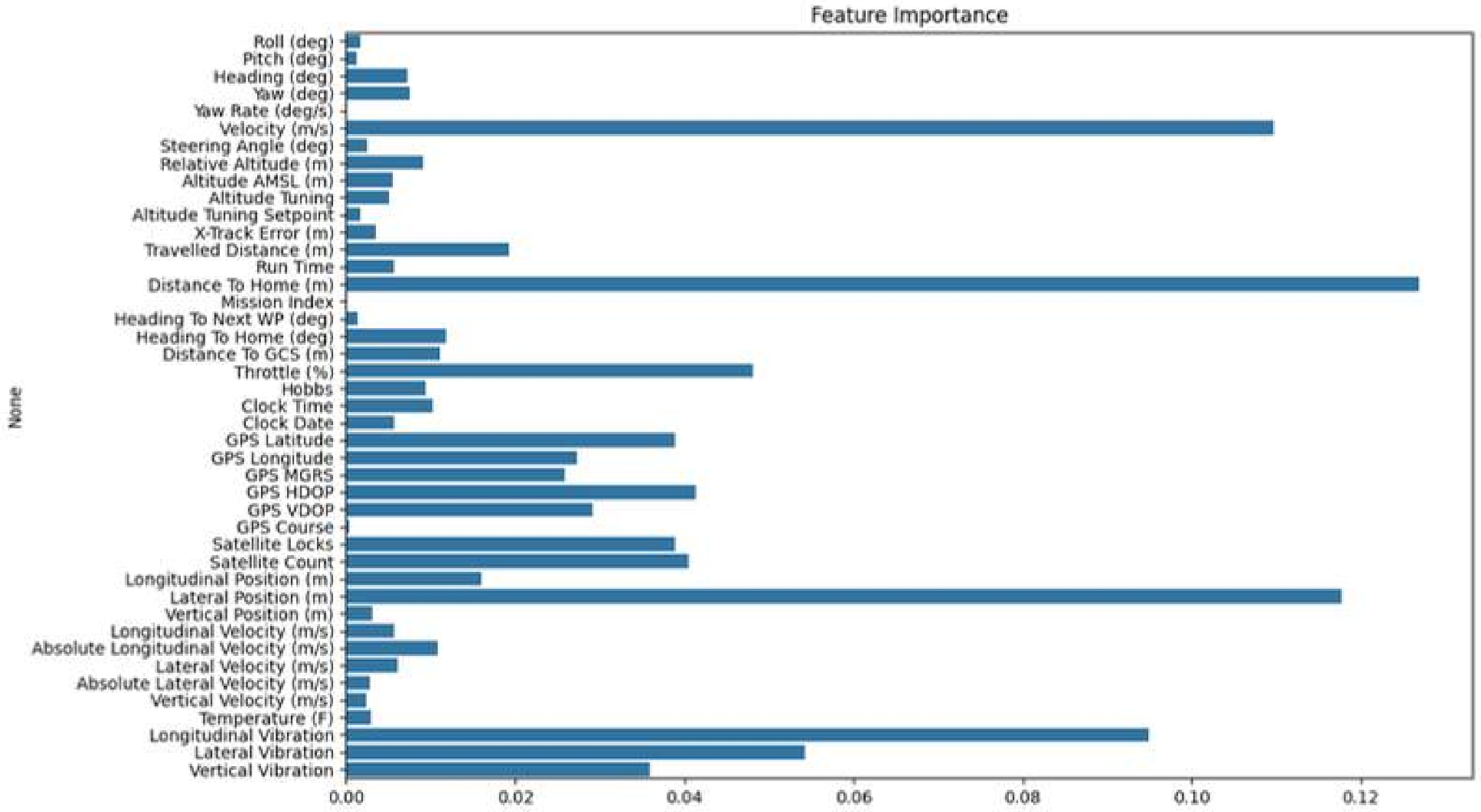
correlations of the Features



seaborn plot

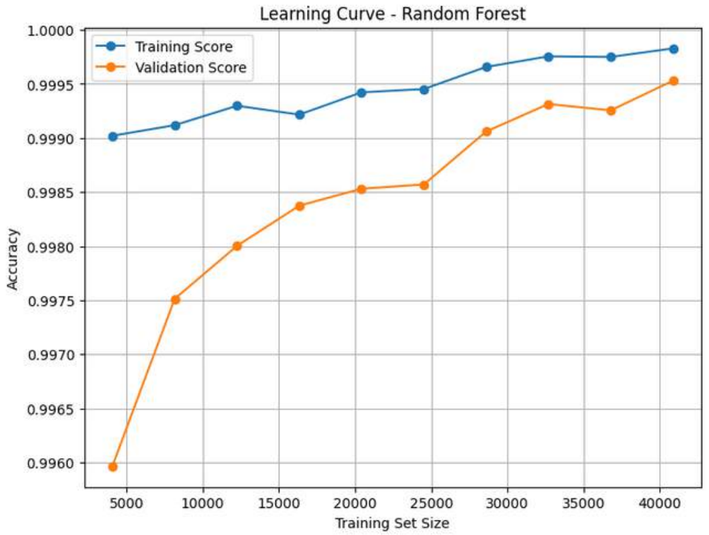
CURRENT PROGRESS

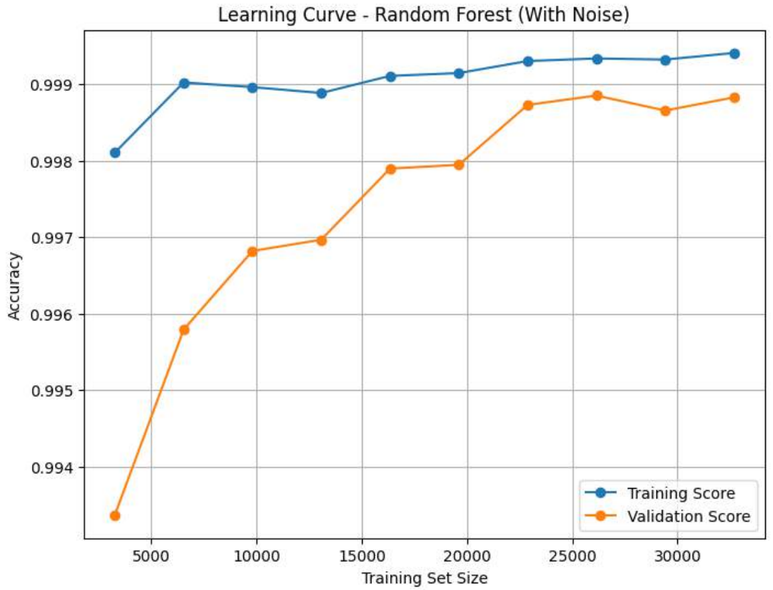
Selecting top features

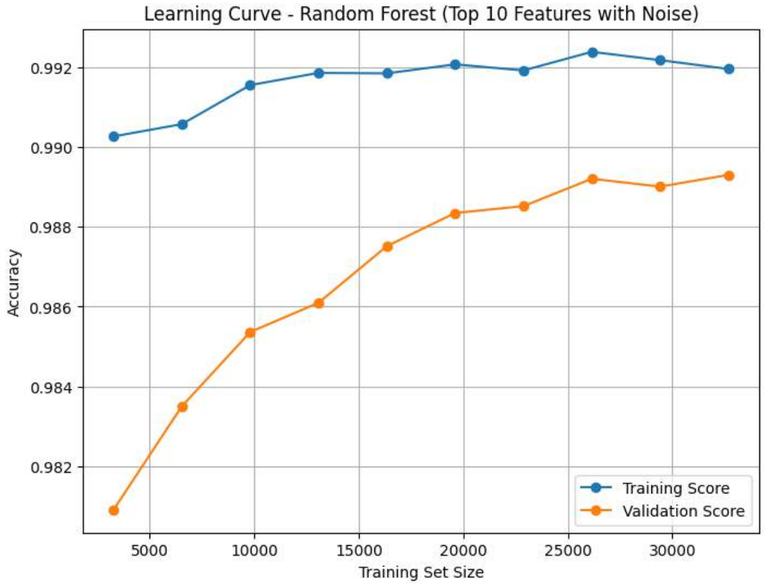


CURRENT PROGRESS

Learning curves after training the Random forest model

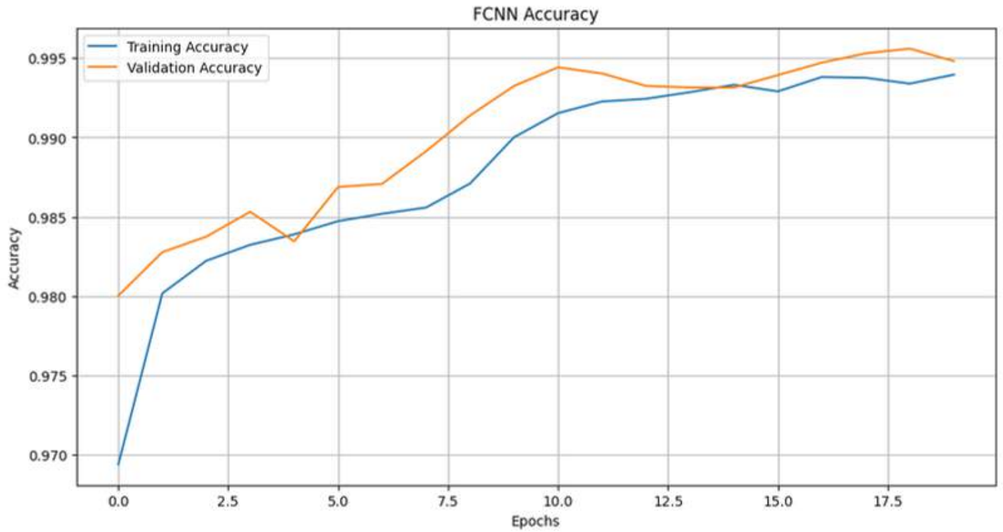


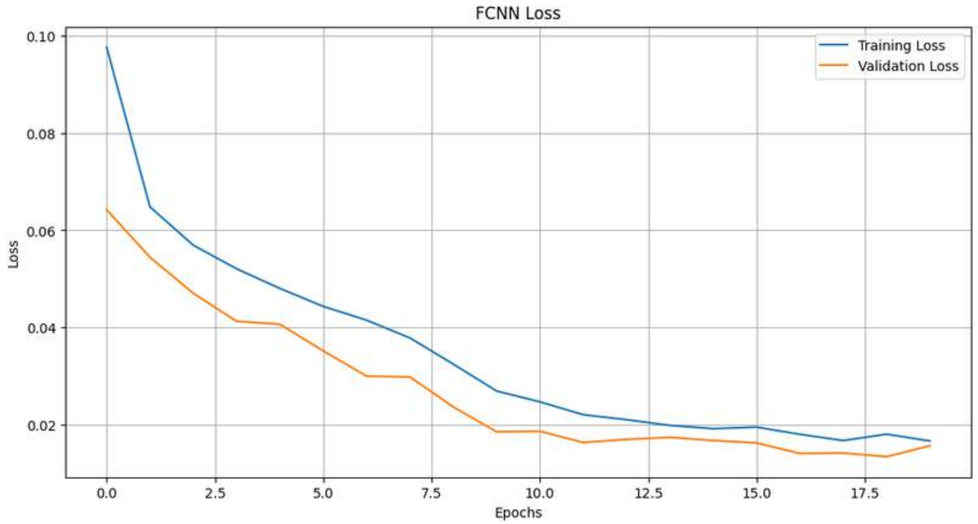




CURRENT PROGRESS

Deep learning (FCNN)





CURRENT PROGRESS

Accuracy compared with other models with all features

```
Training Logistic Regression...

Classification Report for Logistic Regression:
              precision    recall  f1-score   support

           0       0.95      0.98      0.97      5171
           1       0.98      0.94      0.96      5044

    accuracy                           0.96     10215
   macro avg       0.97      0.96      0.96     10215
weighted avg       0.96      0.96      0.96     10215

Logistic Regression ROC-AUC Score: 0.9916
```

```
Classification Report for SVM:
              precision    recall  f1-score   support

           0       0.97      0.99      0.98      5171
           1       0.99      0.97      0.98      5044

    accuracy                           0.98     10215
   macro avg       0.98      0.98      0.98     10215
weighted avg       0.98      0.98      0.98     10215

SVM ROC-AUC Score: 0.9938
```

```
Training Gradient Boosting...

Classification Report for Gradient Boosting:
              precision    recall  f1-score   support

           0       0.99      0.99      0.99      5171
           1       0.99      0.99      0.99      5044

    accuracy                           0.99     10215
   macro avg       0.99      0.99      0.99     10215
weighted avg       0.99      0.99      0.99     10215

Gradient Boosting ROC-AUC Score: 0.9999
```

```
Classification Report for KNN:
              precision    recall  f1-score   support

           0       1.00      0.99      0.99      5171
           1       0.99      1.00      0.99      5044

    accuracy                           0.99     10215
   macro avg       0.99      0.99      0.99     10215
weighted avg       0.99      0.99      0.99     10215

KNN ROC-AUC Score: 0.9992
```

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
- Sklearn
- Jupyter

Architectures & Algorithms

- Random forest
- KNN
- FCNN
- XGBoost
- SVM

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.

Thank you