IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SPOOFER CHAIN: BLOCKCHAIN INTEGRATED FRAMEWORK TO DETECT AND PREVENT CAV LOCATION SPOOFING ATTACK USING GPS TIME SERIES DATA LEARNING AND QUANTUM CRYPTOGRAPHY

[1]Harishankar A, [2]Ashwin D, [3]Aswin AG, [4]Erin Jeri E

[1]Assistant Professor, [2]Student, [3]Student, [4]Student

[1]Department Of Computer Science and Engineering,

[1,2,3,4]Adhiyamaan College of Engineering, Hosur, Tamil Nadu

Abstract: Related and self sufficient automobiles (CAVs) face cybersecurity threats via GPS spoofing attacks, manipulating their navigation information. This entails transmitting false GPS signals to lie to CAVs' onboard receivers, main to incorrect region and navigation choices. To counter this, a complete solution is proposed, integrating blockchain, LSTM algorithms, and quantum cryptography. Blockchain guarantees GPS data integrity with a tamper-resistant ledger. LSTM algorithms examine GPS time series records, improving anomaly detection skills. Quantum cryptography establishes secure verbal exchange channels, leveraging quantum mechanics to encrypt facts, making it nearly immune to hacking. The Spoofer Chain framework amalgamates these technologies, supplying a resilient protection against location spoofing attacks on CAVs. This no longer most effective guarantees passenger safety and right automobile functioning but additionally units the foundation for a comfy and truthful CAV environment within the destiny

***Index Terms* – CAV vehicle, location spoofing attack, communication.**

I. INTRODUCTION

The Spoofer Chain framework represents a pioneering and comprehensive technique to fortifying connected and autonomous cars (CAVs) towards the developing threat of vicinity spoofing assaults. in the realm of CAV cybersecurity, the mixing of cutting-edge technology, namely blockchain, GPS time collection records gaining knowledge of thru long quick-term memory (LSTM) algorithms, and quantum cryptography, creates a sturdy defense mechanism. At its middle, Spoofer Chain addresses the vulnerability of CAVs to GPS spoofing, an advanced shape of cyber hazard wherein malicious actors transmit falsified GPS alerts, manipulating the automobile's navigation information and potentially leading to hazardous results. The incorporation of blockchain era performs a pivotal role in safeguarding the integrity of GPS statistics via establishing a tamper-resistant ledger. This decentralized and dispensed ledger ensures that any attempts to govern or modify GPS statistics are right away detectable, presenting a obvious and comfy basis for the CAV ecosystem. moreover, the Spoofer Chain framework employs advanced LSTM algorithms to investigate GPS time collection records. This method complements the machine's ability to hit upon anomalies and suspicious patterns in actual-time, allowing fast responses to capacity assaults. by using leveraging LSTM algorithms, the framework adapts to the dynamic nature of CAV environments, always mastering and refining its detection competencies. This not best bolsters the machine's accuracy in figuring out region spoofing tries however additionally minimizes fake positives, ensuring a reliable and efficient protection mechanism for CAVs running in numerous and evolving eventualities. within the pursuit of an unassailable defense in opposition to place spoofing assaults, Spoofer Chain integrates quantum cryptography into its framework. Quantum cryptography harnesses the ideas of quantum mechanics to comfy verbal exchange channels among CAVs and records processing centers. The quantum nature of this encryption technique introduces remarkable degrees of security, as it is based on the fundamental properties of quantum states to discover any unauthorized get right of entry to or eavesdropping attempts. with the aid of incorporating quantum cryptography, Spoofer Chain establishes conversation channels which are practically resistant to hacking, providing a further layer of protection important for securing the transmission of sensitive GPS facts inside the CAV atmosphere. The synergy of blockchain, GPS time series facts gaining knowledge of, and quantum cryptography within the Spoofer Chain framework marks a large advancement inside the subject of CAV cybersecurity. This multifaceted technique not most effective addresses the on the spot hazard of area spoofing attacks however additionally anticipates destiny demanding situations in an ever-evolving technological panorama. The blockchain integration ensures data integrity, the LSTM algorithms enhance anomaly detection competencies, and quantum cryptography elevates the security of conversation channels, together forming a holistic protection approach. The SpooferChain framework not most effective specializes in technological fortification however additionally emphasizes the importance of creating a truthful and resilient environment for CAVs. via supplying a transparent and comfy basis, the framework instills self assurance in passengers and stakeholders, fostering the considerable attractiveness and adoption of self reliant automobiles. because the automotive enterprise more and more relies on connectivity and automation, SpooferChain stands as a pioneering solution, placing new standards for cybersecurity in the age of CAVs. In end, the SpooferChain framework represents a groundbreaking initiative to fight the rising chance of area spoofing attacks on linked and independent motors. Its integration of blockchain, GPS time series data learning, and quantum cryptography creates a formidable defense mechanism, ensuring the integrity of GPS information, improving anomaly detection skills, and securing conversation channels. because the automotive landscape continues to conform, SpooferChain emerges as a beacon of innovation, selling safety, security, and consider within the technology of connected and independent automobiles.

I. RELATED WORK

1. S. Filippou, et al. (2023) - Presented a machine learning approach for detecting GPS location spoofing attacks in autonomous vehicles. The study focused on leveraging machine learning algorithms to identify anomalies in GPS data indicative of spoofing attacks.

2. N. Souli, et al. (2022) - Explored online relative positioning of autonomous vehicles using signals of opportunity. The research aimed to improve the accuracy of vehicle positioning by utilizing available signals in the environment.

3. H. Sathaye, et al. (2022) - Introduced SemperFi, an anti-spoofing GPS receiver designed for Unmanned Aerial Vehicles (UAVs). The study focused on enhancing the resilience of UAVs against GPS spoofing attacks.

4. D. Y. Jeon, et al. (2022) - Conducted a performance analysis of authentication protocols for GPS, Galileo, and BeiDou systems. The research aimed to evaluate the effectiveness of authentication mechanisms in preventing spoofing attacks.

5. M. Jayaweera (2021) - Proposed a novel deep learning GPS anti-spoofing system with Direction of Arrival (DOA) time-series estimation. The study focused on leveraging deep learning techniques to enhance the resilience of GPS systems against spoofing attacks.

6. E. Basan, et al. (2021) - Developed GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence. The research aimed to detect and mitigate GPS spoofing attacks targeting UAVs.

7. E. Ranyal and K. Jain (2021) - Conducted a review of unmanned aerial vehicles' vulnerability to GPS spoofing attacks. The study provided insights into the susceptibility of UAVs to spoofing attacks and potential mitigation strategies.

8. Z. Wu, et al. (2020) - Presented BD-II NMA&SSI, a scheme for anti-spoofing and open BeiDou II D2 navigation message authentication. The research aimed to enhance the security and authenticity of BeiDou navigation messages.

9. Y. Dang, et al. (2020) - Proposed a GPS spoofing detector with adaptive trustable residence area for cellular-based UAVs. The study focused on developing a detector capable of adapting to dynamic UAV environments.

10. S. Semanjski, et al. (2020) - Utilized supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data. The research aimed to detect and mitigate spoofing attacks using machine learning algorithms validated with real-world data.

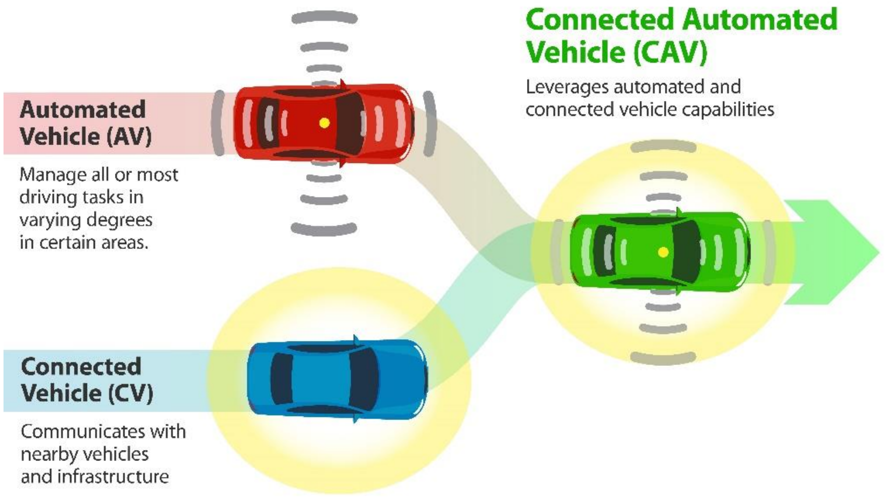
II. OBJECTIVE

To increase a blockchain-included framework for CAVs (connected and self sufficient motors) that utilizes GPS time collection facts mastering with LSTM and quantum cryptography, with the subsequent targets:

- To beautify CAV safety by mitigating the risks related to area spoofing assaults and capacity injuries or disruptions.
- To analyze GPS time collection facts using LSTM to discover anomalies and styles indicative of spoofing tries, permitting early detection.
- To integrate blockchain era to preserve a tamper-evidence ledger of GPS records, ensuring data integrity and imparting a transparent report of CAV movements.
- To put in force quantum cryptography to cozy conversation channels between CAVs and infrastructure, stopping eavesdropping and hacking.
- To allow real-time detection and response to area spoofing attacks, minimizing their effect on CAV operations and safety.
- To make sure the interoperability of the SpooferChain framework with numerous CAV systems and applications, facilitating broader adoption.
- To align the mission with relevant policies and standards, making sure prison and ethical use of the generation.
- To train CAV customers and stakeholders about the dangers of region spoofing and the importance of at ease navigation structures.
- To layout the framework for scalability and efficiency, accommodating the growing extent of facts generated by means of CAVs in real-international eventualities.
- To foster collaboration with enterprise professionals, researchers, and stakeholders, leveraging collective know-how to ensure the success of the SpooferChain assignment.

III. OVERVIEW

Related and self sustaining automobiles (or CAVs) integrate connectivity and automated technologies to help or replace humans in the task of driving. this could be through a mixture of superior sensor generation; on-board and faraway processing skills; GPS and telecommunications structures. linked and self sustaining vehicles (CAV) represent a floor-breaking evolution in the international of transportation. these vehicles are geared up with advanced technologies that allow them to operate with various degrees of autonomy and to talk seamlessly with different automobiles, infrastructure, and outside structures. at the middle of CAV's competencies is their capacity to force autonomously, ranging from fundamental driver-assistance functions to complete self-using abilties. To reap this, they rely upon a plethora of sensors, including lidar, radar, cameras, and ultrasonic sensors, to perceive their surroundings, detect obstacles, and make actual-time using selections.


Connected Automated Vehicle (CAV)
Leverages automated and connected vehicle capabilities
Automated Vehicle (AV)
Manage all or most driving tasks in varying degrees in certain areas.
Connected Vehicle (CV)
Communicates with nearby vehicles and infrastructure

CONNECTED VEHICLE

A linked vehicle is a car ready with unique data transmission technology like a web of things (IoT) device. as an instance, you can software a smart home to show at the heating one hour earlier than you return domestic, and in the same manner, you may command a related automobile to turn on windshield heating 5 mins before your deliberate departure. extra advanced related automobiles additionally have sensors, computer vision, wireless communique, and facts analysis capabilities embedded. A connected car is a facts-powered car with a massive set of customized capabilities aimed at better safety, much less power intake, and greater comfort for the driving force and passengers.

AUTOMATED VEHICLE

An automated transportation automobile is a vehicle geared up with the identical records switch and programming opportunities as connected automobile systems, plus it's far able to making unbiased decisions and behaving accordingly. as an instance, if the driving force of an automotive connection-powered automobile exceeds the speed, that car independently comes to a decision to put at the brakes to acquire most protection for the driving force.

CONNECTED VEHICLE (CV) TECHNOLOGIES

Connected and self reliant vehicles are powered by the equal idea, but at the same time as the latter is still in improvement, related car solutions are already here. below are the technology that currently energy connected vehicles.

- Significant pc. A crucial facts processing system with a person interface embedded in a motive force panel.
- GPS. it's miles a standard generation for the automobile enterprise. related motors come with an embedded GPS device, so the driver doesn't want a cellular app or an extra device to observe a course.
- Motive force help sensors. The best instance of that is a rearview digital camera, which permits you to returned up safely, whilst it estimates the space from the bumper to an impediment and offers the motive force a sign when to forestall. This generation is a trendy for related vehicles, but in relation to autonomous vehicles, they're powered with the aid of a sophisticated driving force assistance system (ADAS) which can collect, system, and analyze the real-time environment the use of sensors and gadget learning, and take safety-first choices on its simple
- Wireless verbal exchange. This technology is at the center of connected independent automobiles since it lets in on the spot data switch, which gives the motive force with driving behaviour optimization tips and better responses to emergencies.

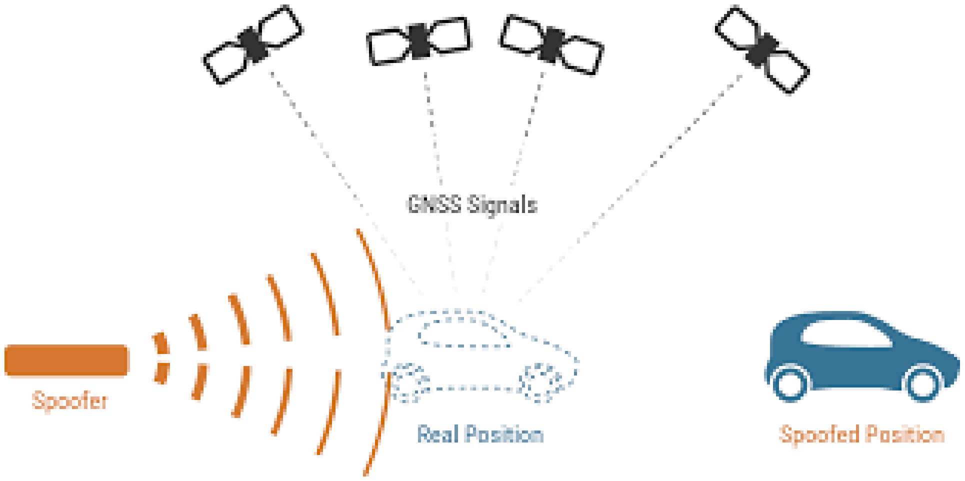
CONNECTED VEHICLES COMMUNICATION TYPES

- Linked vehicle offerings talk with every other the usage of several strategies to switch data.
- Automobile-to-vehicle. It means that statistics from one automobile transfers to another one. for instance, in case of a crash, other drivers can be made aware about this emergency.
- Car-to-infrastructure. inside the case of a vehicle to infrastructure technology, a linked car can transfer statistics to another infrastructure like an emergency reaction center.
- Automobile-to-device. A vehicle can send a notification to a driving force's telephone.
- Vehicle-to-cloud. V2C records switch implies delivering information to the cloud for in addition storage and evaluation.
- Automobile-to-pedestrian. In this situation, a automobile sends a sign to pedestrians if the pedestrian's behaviour seems dangerous for their health.
- Automobile-to-everything. V2E opportunities mean a strong and all-encompassing facts management infrastructure.

BENEFITS OF AUTONOMOUS CARS

The benefits of car software program for vehicles are difficult to predict since self-driving technology remains in development. The handiest exception is drones which are prohibited in some international locations. furthermore, a few specialists observe that self-using car improvement will take longer than predicted considering that there's a want to develop specific felony regulation and self reliant car infrastructure. nevertheless, in addition they agree that self-using motors can also supply the following blessings. remaining protection. As for self-riding motors, humans expect they will be programmed and taught to make clever choices supporting a secure surroundings on the road. that is, we may additionally expect fewer instances of beaten because of distractions, speeding, and drugged riding. cost financial savings. the less incidents are predicted to decrease the fee of hospital therapy and coverage. Plus, the preventive maintenance device embedded in independent automobiles can also reduce charges due to the timely servicing and spare components alternative. Time savings and better productiveness. The owners of self-riding motors may be capable of remedy their non-public and business responsibilities right on the cross, with out the want to be distracted from driving. The independent motors with a self-parking function may even permit the owners to save numerous time considering, after the advent, the car will part itself independently; and the owner might be capable of proceed with duties. more independence. Self-riding motors are predicted to grow to be an option for humans with impairment and disabilities. controlled with voice commands, they acquire better mobility with the auto making all the essential choices.

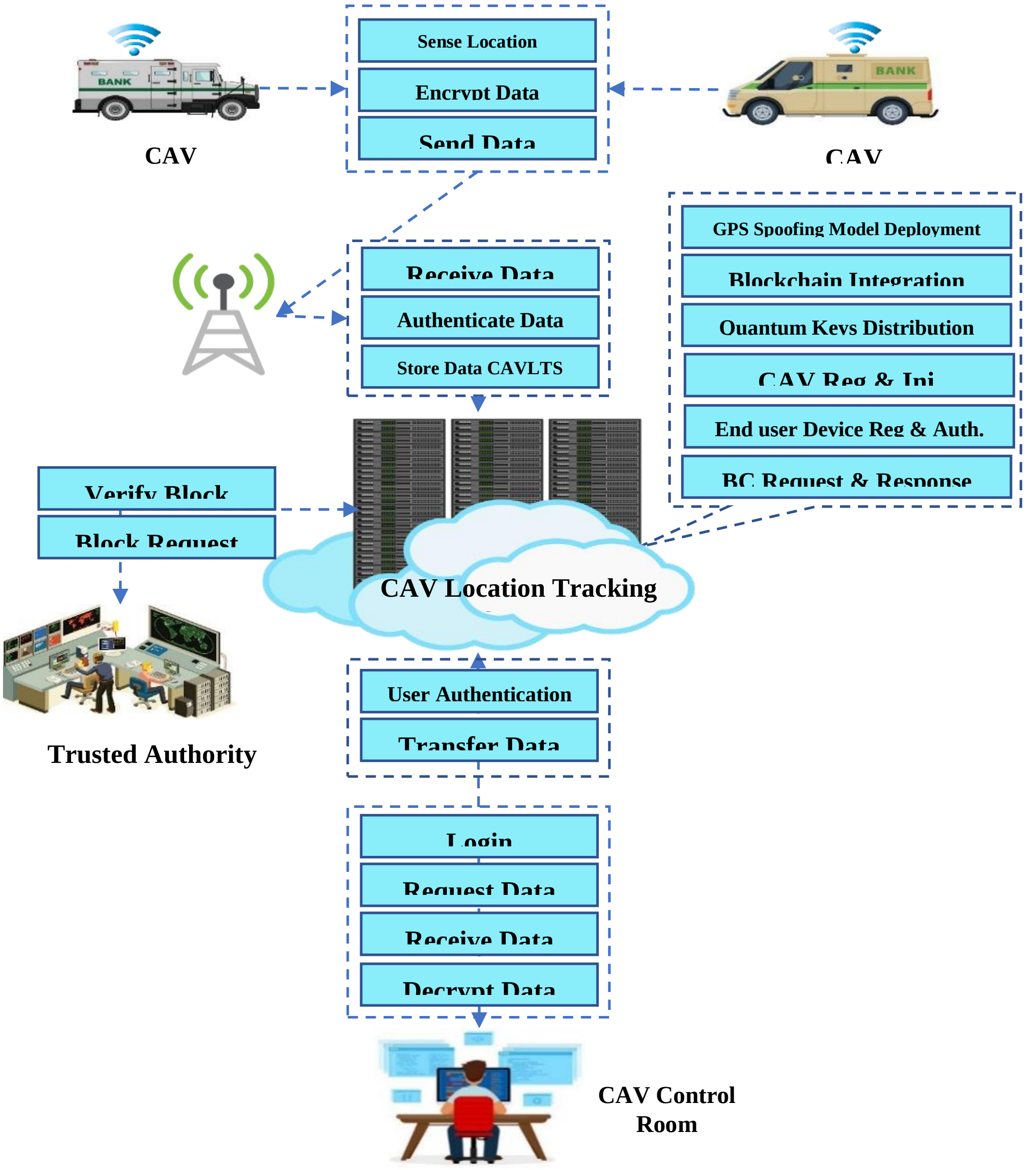
CAV GPS SPOOFING ATTACK



Connected and self sustaining motors (CAV) are reliant on worldwide Positioning device (GPS) era for navigation and region-primarily based offerings. however, GPS spoofing attacks have emerged as a widespread hassle in the context of CAV. In a GPS spoofing attack, malicious actors manage the GPS signals acquired via CAV structures, causing the cars to misinterpret their geographical places. those attacks can have numerous destructive consequences on CAV, which includes misdirecting the vehicles, compromising protection, elevating privateness worries, disrupting information and verbal exchange structures, and posing monetary dangers, specially in industries dependent on CAV generation. additionally, GPS spoofing assaults can avoid emergency response efforts, making it hard for rescue offerings to find affected CAV. CAV structures are prone to such assaults because of their heavy reliance on GPS data for navigation, choice-making, and communique, which makes them appealing goals for malicious sports. To counter those threats, CAV manufacturers and builders are investing in superior detection and mitigation methods, consisting of multi-sensor fusion, relaxed signal authentication, and anomaly detection. Addressing GPS spoofing in CAV also involves grappling with felony and liability problems, particularly when determining duty in spoofing-related accidents. developing strong security features, together with relaxed and encrypted GPS signals, progressed cybersecurity protocols, and public cognizance campaigns, is essential to making sure the secure and reliable operation of autonomous automobiles and keeping public accept as true with on this evolving generation.

3.3. ARCHITECTURE DESIGN

The proposed structure entails GPS Time collection data studying, Quantum Cryptography, Blockchain Integration and assault Detection & Prevention Layer to develop an blockchain included framework. The architecture of the Proposed device is proven within the figure.3.1.



1.GPS Time Series Data Learning :

Makes use of system studying algorithms to research historic GPS facts. Establishes a baseline of everyday vehicle movement styles. Identifies anomalies and deviations from anticipated conduct. Contributes to the detection of potential spoofing attacks with the aid of recognizing ordinary automobile trajectories.

2. Quantum Cryptography Module:

Implements quantum key distribution protocols to comfy verbal exchange channels. complements the confidentiality and integrity of location records exchanged among CAVs and infrastructure. provides a quantum-secure layer for encryption and decryption processes, ensuring resistance in opposition to quantum assaults.

3. Blockchain Integration:

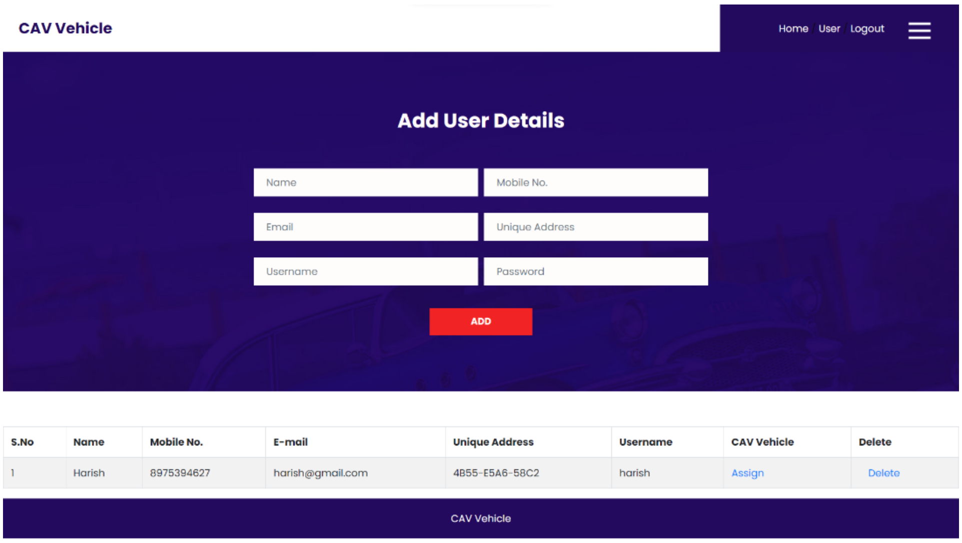
Utilizes a decentralized and tamper-resistant ledger to save validated vicinity statistics. Timestamps and statistics place updates from CAVs in a obvious and immutable way. smart contracts govern the consensus mechanism, making sure the accuracy of place statistics and preventing unauthorized changes.

4. Attack Detection and Prevention Layer:

Analyzes records from the GPS Time collection facts studying Module and Blockchain for inconsistencies. Implements actual-time anomaly detection to discover capability spoofing attacks. Triggers reaction mechanisms, inclusive of alerting government or activating fail-safe protocols, to prevent the fulfillment of a spoofing strive.

IV. RESULTS AND DISCUSSION

Spoofer Chain gives a comprehensive and innovative method to address the developing risk of area spoofing assaults on CAVs. via combining GPS time collection statistics getting to know, Quantum Cryptography, and Blockchain era, Spoofer Chain enhances the security, integrity, and trustworthiness of CAV region information, thereby bolstering the safety and reliability of autonomous transportation structures. because the automobile industry maintains to embody independent technology, Spoofer Chain stands as a important protection in opposition to malicious manipulation of vicinity information, ensuring a safer and more secure future for related and self reliant automobiles.

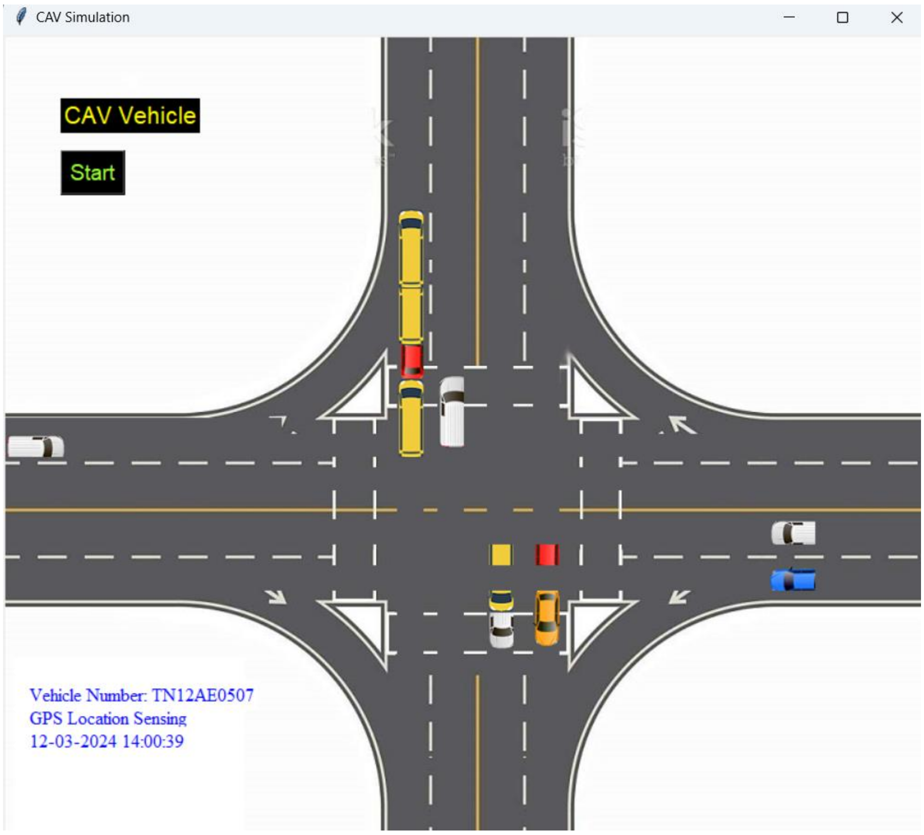


Add User Details

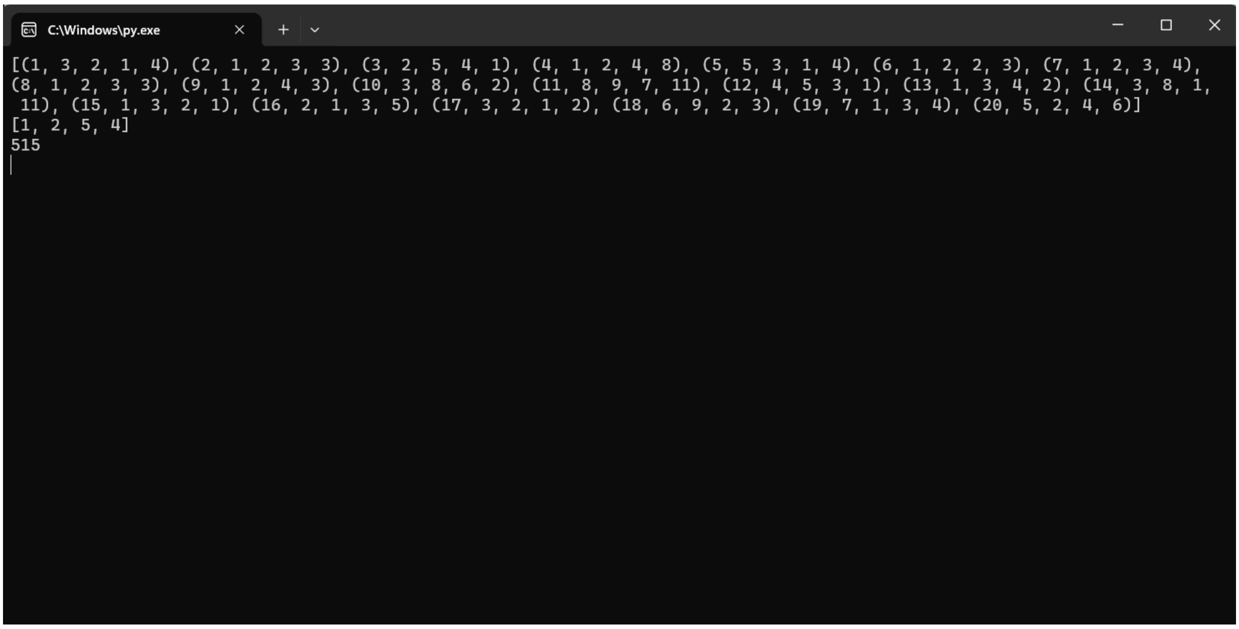
Name
Mobile No.
Email
Unique Address
Username
Password

S.No	Name	Mobile No.	E-mail	Unique Address	Username	CAV Vehicle	Delete
1	Harish	8975394627	harish@gmail.com	4B55-E5A6-58C2	harish	Assign	Delete

CAV Vehicle



Vehicle Number: TN12AE0507
GPS Location Sensing
12-03-2024 14:00:39



```
[(1, 3, 2, 1, 4), (2, 1, 2, 3, 3), (3, 2, 5, 4, 1), (4, 1, 2, 4, 8), (5, 5, 3, 1, 4), (6, 1, 2, 2, 3), (7, 1, 2, 3, 4),
(8, 1, 2, 3, 3), (9, 1, 2, 4, 3), (10, 3, 8, 6, 2), (11, 8, 9, 7, 11), (12, 4, 5, 3, 1), (13, 1, 3, 4, 2), (14, 3, 8, 1,
 11), (15, 1, 3, 2, 1), (16, 2, 1, 3, 5), (17, 3, 2, 1, 2), (18, 6, 9, 2, 3), (19, 7, 1, 3, 4), (20, 5, 2, 4, 6)]
[1, 2, 5, 4]
515
```

REFERENCES

[1]S. Filippou, A. Achilleos, S. Z. Zukhraf, C. Laoudias, K. Malialis, M. K. Michael, and G. Ellinas, ‘‘Amachine learning approach for detecting GPS location spoofing attacks in autonomous vehicles,’’ in *Proc. IEEE 97th Veh. Technol. Conf.*, Jun. 2023, pp. 1–7.

[2]N. Souli, P. Kolios, and G. Ellinas, ‘‘Online relative positioning of autonomous vehicles using signals of opportunity,’’ IEEE Trans. Intell. Vehicles, vol. 7, no. 4, pp. 873–885, Dec. 2022.

[3]H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, ‘‘SemperFi: Anti-spoofing GPS receiver for UAVs,’’ in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2022, pp. 1–17.

[4]D. Y. Jeon, T. Gaybullaev, J. H. Noh, J. M. Joo, S. J. Lee, and M.-K. Lee, ‘‘Performance analysis of authentication protocols of GPS, Galileo and BeiDou,’’ J. Positioning, Navigat., Timing, vol. 11, no. 1, pp. 1–9, 2022.

[5]M. Jayaweera, ‘‘A novel deep learning GPS anti-spoofing system with DOA time-series estimation,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2021, pp. 1–6.

[6]E. Basan, A. Basan, A. Nekrasov, C. Fidge, N. Sushkin, and O. Peskova, ‘‘GPS-spoofing attack detection technology for UAVs based on Kullback–Leibler divergence,’’ Drones, vol. 6, no. 1, p. 8, Dec. 2021.

[7]E. Ranyal and K. Jain, ‘‘Unmanned aerial vehicle’s vulnerability to GPS spoofing a review,’’ J. Indian Soc. Remote Sens., vol. 49, no. 3, pp. 585–591, Mar. 2021, doi: 10.1007/s12524-020-01225-1.

[8]Z. Wu, Y. Zhang, and R. Liu, ‘‘BD-II NMA&SSI: An scheme of antispoofing and open BeiDou II D2 navigation message authentication,’’ IEEE Access, vol. 8, pp. 23759–23775, 2020.

[9]Y. Dang, C. Benzaïd, Y. Shen, and T. Taleb, ‘‘GPS spoofing detector with adaptive trustable residence area for cellular based-UAVs,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1–6.

[10]. Semanjski, I. Semanjski,W. DeWilde, and A. Muls, ‘‘Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I,’’ Sensors, vol. 20, no. 4, p. 1171, Feb. 2020.