International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrated Framework to Detect and Prevent CAV Location Spoofing and BlockChain using Quantum Cryptography

***Dr. S.Brindha*[1]*, Dr. S.Ravichandran*[2]**

Assistant Professor, Department of Computer Applications, SRMIST Faculty of Science and Humanities, SRM Institute of Science and Technology, SRM University, Kattankulathur, Chennai, brindhas1@srmist.edu.in
Professor and Head in the Department of Chemistry at DRK Institute of Science and Technology, Hyderabad, ravichandran.23324@lpu.co.in

ABSTRACT :

Vehicles that integrate automation, connection, and cutting-edge technology to improve convenience, safety, and efficiency of transportation are referred to as connected and autonomous vehicles, or CAVs. A cyber security vulnerability known as a "CAV GPS spoofing attack" targets connected and autonomous vehicles (CAVs) by tampering with the navigational data provided by the Global Positioning System (GPS). GPS spoofing is the practice of sending phony GPS signals to CAVs' on board GPS receivers, tricking them into choosing the wrong position and course. This kind of attack may have detrimental effects on the car, such as changing its course or making it veer off course, or even resulting in mishaps or safety concerns.

The fact that spoofing tactics are always evolving and that attackers are using more advanced approaches is one of the main problems. The incessant innovation poses a challenge to the efficacious detection and prevention of GPS spoofing by current algorithms. By combining blockchain technology for data integrity, LSTM algorithms for GPS time series data analysis, and quantum cryptography for secure communication, the project seeks to address these issues. In a world where dependable GPS data is crucial to CAV operation, the purpose of this integration is to identify and stop location spoofing assaults and create a safe and reliable framework for these vehicles. This study presents a comprehensive defense against location spoofing attacks against CAVs using a combination of state-of-the-art technologies. By generating an information ledger that is impenetrable to tampering, the incorporation of blockchain technology guarantees the accuracy of GPS data. The GPS time series data is analyzed using Long Short-Term Memory (LSTM) algorithms, which improves the system's detection of abnormalities and threats. Additionally, the initiative establishes unbreakable and secure communication routes between CAVs and data processing centers by utilizing the capability of quantum cryptography. Utilizing the ideas of quantum physics, quantum cryptography encrypts and transmits data in a manner that is nearly impervious to hacking and eavesdropping. The objective of the project is to offer a comprehensive and robust protection against location spoofing attacks on CAVs by integrating these components into the SpooferChain architecture. This sets the way for a more safe and reliable environment for autonomous cars (CAVs) in the future while also guaranteeing the safety of passengers and the correct operation of these vehicles.

Keywords: Long Short Term Memory, Block Chain Technology, Cryptography, Spoofer Chain, Global Positioning System.

INTRODUCTION :

Autonomous cars, also known as connected and autonomous vehicles, integrate automated technology and connection to support or supplant human drivers. Advanced sensor technologies, on-board and remote computing power, GPS, and telecommunications networks may all be used to do this. CAVs, or connected and autonomous vehicles, are a revolutionary development in the transportation industry. These cars are outfitted with cutting-edge technology that allow them to interact with other cars, the infrastructure, and external systems with ease and to function with variable degrees of autonomy. The capacity of CAVs to drive autonomously, from simple driver aid features to complete self-driving capabilities, is the foundation of their capabilities. They use a variety of sensors, like as lidar, radar, cameras, and ultrasonic sensors, to accomplish this in order to sense their environment, detect obstacles, and make real-time driving decisions.

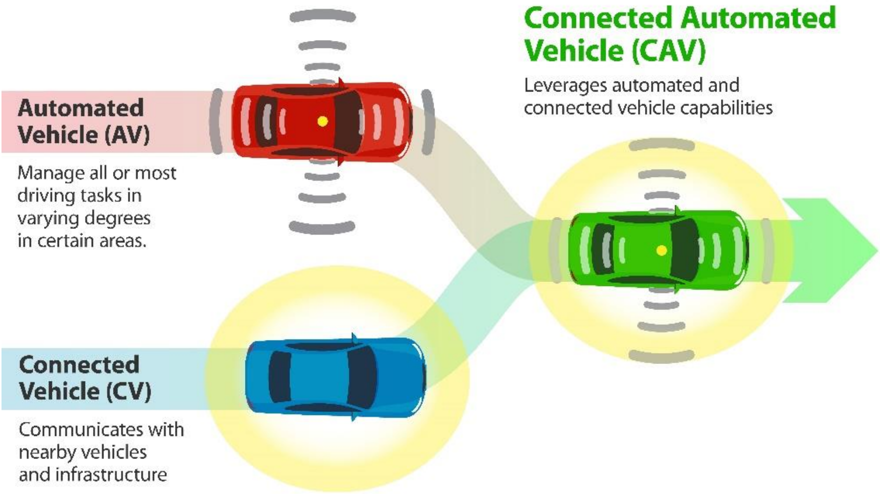

Automated Vehicle (AV)
Manage all or most driving tasks in varying degrees in certain areas.
Connected Automated Vehicle (CAV)
Leverages automated and connected vehicle capabilities
Connected Vehicle (CV)
Communicates with nearby vehicles and infrastructure

Fig.1.1 CAV

Connected Vehicle

An automobile that has Internet of Things (IoT) devices or other specialized data transmission technology installed is referred to as a linked car. For instance, you can set up a smart house to start heating an hour before you arrive, and you can also tell a linked automobile to start heating the windscreen five minutes before you leave. Sensors, computer vision, wireless connection, and data processing functions are also included in more sophisticated connected automobiles. A connected car is a data-driven automobile with an extensive array of personalized features designed to improve safety, reduce energy usage, and enhance passenger and driver comfort.

Automated Vehicle

An autonomous transportation vehicle is an automobile that can make judgments on its own and act appropriately. It has the same data transfer and programming capabilities as connected car systems. For instance, an automobile connection-powered car would automatically decide to apply the brakes to ensure the driver is as safe as possible if they travel faster than the posted speed limit.

Connected Vehicle (CV) Technologies

Although autonomous vehicles are still in the early stages of research, linked car solutions are now available. Both types of vehicles operate on the same principle. The technologies that power linked cars at the moment are listed below.

Central computer. The main computer. a driver panel-integrated central data processing system with an integrated user interface.

GPS. In the car business, this technology is standard. Since connected cars have built-in GPS, following a route doesn't require a separate device or a mobile app.

Driver assistance sensors. Sensors for driver assistance. A rear-view camera is the most basic sample of this; it lets you back up securely, measures the distance between your bumper and an obstruction, and signals to you when it's time to stop. This technology is commonplace for connected cars, but advanced driver assistance systems (ADAS) power autonomous vehicles. ADAS can gather, process, and analyze real-time environmental data using sensors and machine learning, making safety-first decisions at the fundamental

Wireless communication. This technology is the foundation of linked autonomous cars since it enables real-time data sharing, which gives the driver recommendations for optimizing their driving style and improved emergency response.

Connected Vehicles Communication Types

Many methods are used by connected automobile services to exchange data with one another.

Vehicle-to-vehicle It indicates that information is sent from one car to another. For instance, other drivers can be alerted to an emergency in the event of a collision.

Vehicle-to-infrastructure. When it comes to vehicle-to-infrastructure technology, an interconnected vehicle can send data to an ER or other infrastructure.

Vehicle-to-device. A driver's phone may get notifications from a car.

Vehicle-to-cloud. V2C data transfer implies delivering data to the cloud for further storage and analysis.

Vehicle-to-pedestrian Data delivery to the cloud for further storage and analysis is referred to as V2C data transmission.

Vehicle-to-everything. V2E opportunities imply a stable and all-encompassing data management infrastructure.

RELATED WORKS

[SAM 22] Md. Saniul Alam and associates: As part of a comprehensive future mobility management framework, cooperative and connected autonomous vehicles (CCAVs) are seen as a possible way to handle congestion and other operational issues. Because of this, a sizable number of research on the subject have just been published. This review article addresses three issues related to future mobility management: traffic management, network performance, and mobility management, which includes congestion and PRISMA-based event detection. For this study, three databases were taken into consideration, and peer-reviewed primary papers that focused on CCAV from the perspective of future transportation and mobility management and were published in the English language during the previous ten years were chosen.

[FRO 22] Three registers—ScienceDirect (SD), the website of the Institute of Electrical and Electronics Engineers (IEEE), and Taylor & Francis Online Journals were used to find the research studies. Information about connected and automated hybrid electric vehicles (CAHEV), connected and autonomous vehicles (CAV), autonomous vehicles (AV), vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, and vehicular ad hoc network systems (VANETS) is compiled in this review based on recent studies. Papers on cyber security assessment, flow improvement, efficiency improvement, health, and other subjects unrelated to the goals of the current article were not included in the first screening round. Authors, years, study kind, study location, modeling type, modeling tool, modeling strategy, and modeling process data were gathered from the chosen research publications.

[WAN 21] The reviews above can be interpreted in a variety of ways. Frequently, the investigations relied on fictitious networks, and the investigators employed algorithmic analysis or mathematical modeling. Thanks to decades of technological advancements, this new wave of interest has the ability to apply far more sophisticated and potent analytical techniques. Moreover, researchers can now build far more secure foundations for their models because to commercially accessible technologies. However, the literature only contains a small number of simulation-based modeling studies, and the models' spatial coverage is constrained.

While some modeling research employed algorithms to depict CAVs, most modeling studies concentrated on adapting current models and modeling platforms to become CAV-aware. Most critically, none of the research examined complicated urban road transport systems with many road user kinds. Both methodologies have limits, therefore the studies are, with a few exceptions, micro-simulations.

Published in 2009, the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) statement was created to assist systematic reviewers in openly reporting the purpose of the review, the actions taken by the authors, and the results they discovered. The guideline has to be updated due to advancements in systematic review technique and language during the last ten years. The 2009 statement is replaced by the PRISMA 2020 statement, which also contains revised reporting guidelines reflecting improvements in finding, picking, evaluating, and synthesizing research. To make deployment easier, the elements' organization and appearance have been changed. The PRISMA 2020 abstract checklist, the extended checklist with reporting guidelines for every item, the PRISMA 2020 27-item checklist, and the updated flow diagrams for the original and updated reviews are all included in this article.

EXISTING SYSTEM

The efficiency of GPS spoofing attack detection is hampered by a number of issues. In crucial applications like autonomous cars, cryptography-based techniques may cause real-time processing delays due to their high computing cost and complexity. Key management becomes difficult when cryptographic keys need to be distributed and stored securely. Machine learning-based methods are less dependable in the face of changing threats since they mainly depend on large amounts of training data and are vulnerable to adversarial assaults. Furthermore, these methods could produce false positives or negatives, leading to inaccurate detection or permitting assaults to go unnoticed.

Although promising, multi-sensor fusion techniques have synchronization, cost, and complexity issues. Additionally, especially in complicated signal environments, they can find it difficult to distinguish between deliberate and inadvertent interference, which could result in a high proportion of false positives. A significant percentage of false positives can result from jamming detection techniques' inability to reliably discriminate between deliberate jamming assaults and incidental signal disturbances. Advanced cryptographic protocols and secure channel implementation can be difficult and expensive to implement; they frequently call for software and hardware changes, and their security can be jeopardized if cryptographic keys are lost or stolen. To ensure the safe and secure deployment of CAV in the future, addressing these issues requires an all-encompassing strategy incorporating improved security mechanisms, encrypted GPS signals, regulatory frameworks, and public awareness campaigns.

PROPOSED WORK

One area of machine learning that deals with the use of algorithms in artificial neural networks is called "deep learning." It is mostly used to build predictive models that need only a few lines of code to address issues. An enormous neural network that draws inspiration from the structure and function of the brain is called a Deep Learning system. Supervised, semi-supervised, and unsupervised deep learning models—or any mix of the three—are all possible. Tech behemoths like Google, Microsoft, and Amazon rely on these sophisticated machine learning algorithms to power smart assistants and self-driving cars, among other things. These algorithms operate whole systems.

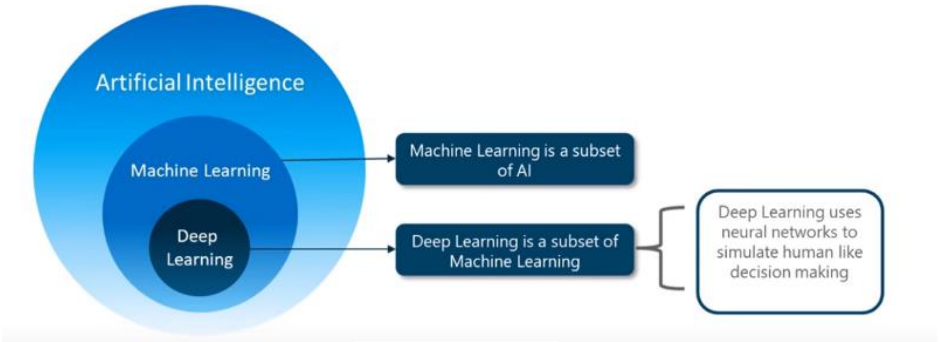

Artificial Intelligence
Machine Learning
Deep Learning
Machine Learning is a subset of AI
Deep Learning is a subset of Machine Learning
Deep Learning uses neural networks to simulate human like decision making

Fig.1.2 Deep Learning

Machine learning has to be created first. Machine learning (ML) is a framework to automate statistical models, such as a linear regression model, using algorithms to improve prediction accuracy. A single model that forecasts anything is called a model. There is some accuracy to their forecasts. A machine learning model takes all of its incorrect predictions and modifies the model's internal weights to produce a model that produces fewer errors. Artificial neural networks were created as a result of the learning process involved in building models. The hidden layer is used by ANNs to store and assess the relative importance of each input to the output. The hidden layer associates the significance of the input with other inputs and keeps information of combinations of inputs.

THE ARCHITECTURE OF AN LSTM:

- **Data Collection:**

GPS sensors or receivers are used to gather GPS time series data. Information on satellite signals, signal intensities, and receiver locations are all included in this data.

- **Pre-processing**

Preprocessing is done on the gathered GPS data to get rid of mistakes, noise, and outliers. To guarantee the quality of the data used to train the LSTM model, this step is essential.

- **LSTM Model Training**

Recurrent neural networks (RNNs) of the Long Short-Term Memory (LSTM) type are used to learn the temporal patterns in the GPS data. The algorithm has been trained to identify patterns in valid GPS signals.

- **Anomaly Detection**

The LSTM model may be used to identify anomalies or departures from predicted patterns after it has been trained on real GPS data. The model is able to detect anomalous signal patterns in the event of a GPS spoofing assault.

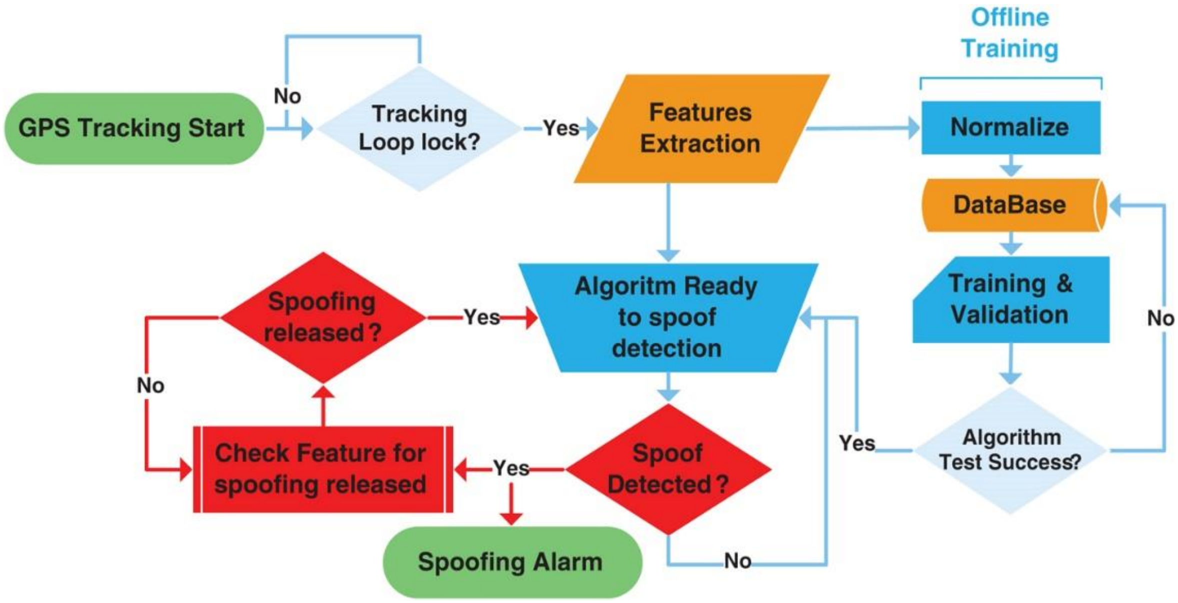
- **Threshold Setting**

For anomaly detection, a threshold or confidence level is established. This threshold is used to identify potential spoofing attacks when the divergence from the predicted GPS signal pattern is greater than it is.

- **Alarm Generation**

System administrators or users are notified by the generation of an alert or alarm upon detection of a suspected GPS spoofing attack. This may prompt more research or defensive actions.

Fig.1.3. LSMT Based GPS Spoofing Detection Model



The LSTM architecture is based on the following key components:

Cell State (C^t): This is the LSTM's memory, and it has the capacity to store data for extended periods of time. At every time step, it can be read from, modified, or cleared.
Hidden State (H^t): The hidden state acts as a bridge connecting the cell state to the outside environment. It may generate the output and selectively recall or forget information from the cell state.
Input Gate (i^t): This gate regulates the information that enters the cell state. It is capable of accepting and rejecting incoming data.
Forget Gate (f^t): This gate decides what should be discarded and what should be kept from the prior cell state. It enables the LSTM to "forget" unimportant data.
Output Gate (o^t): At each time step, the output gate regulates the data utilized to generate the output. It determines which portion of the cell state should be made public.

4.1. Blockchain Technology

Blockchain technology is a system that stores public transactional information, or blocks, in several databases, collectively called the "chain," which are linked via peer-to-peer nodes. The term "digital ledger" is often used to describe this kind of storage. Every transaction in this ledger is approved by the owner's digital signature, which guarantees its legitimacy and guards against fraud. The digital ledger's data is incredibly secure as a result.

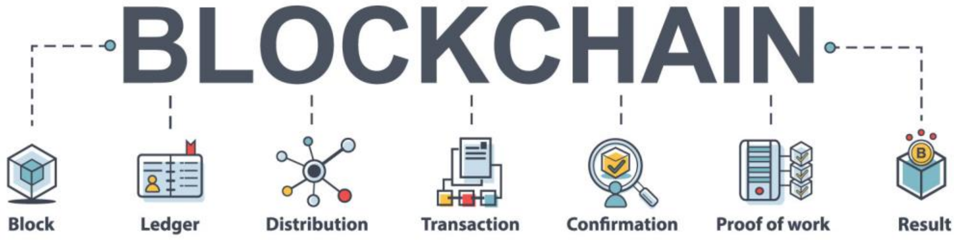


Fig.1.4. Blockchain Technology

Blockchain technology has advantages that go beyond security. Blockchain technology guarantees the anonymity of the data owner. Sensitive information pertaining to identities is protected. Each component is checked to verify sure there haven't been any modifications each time a user requests data. Should any modification be discovered, the miner accountable for it is removed from the network. Many organizations, ranging from startups to large tech giants, have entered the blockchain cloud storage industry and are digitally revolutionizing their operations. Because several small businesses work together to share processing power and storage space, blockchain offers a safe and affordable alternative to cloud storage. In this approach, the cost of cloud storage is decreased and the entities who contribute processing power are compensated.

4.2. Quantum Cryptography

Encrypting data, or turning plain text into jumbled information that can only be read by someone with the correct "key," is the process known as cryptography. By extension, quantum cryptography is just the process of encrypting and transmitting data in an impenetrable manner using the ideas of quantum physics. Quantum Key Distribution (QKD), sometimes known as quantum cryptography, is a technique for establishing secure communication. It enables the distribution and sharing of secret keys, which are necessary for cryptographic protocols. To ensure security, a system has to employ cryptographic algorithms and protocols, particularly when communicating across an unstable network such as the Internet. Conventional cryptosystems for data encryption rely on mathematical concepts, but quantum communication relies on physics to offer security.

4.3 Secure Communication

A very safe method of communication between CAVs (Connected and Autonomous Vehicles) and CAV Data Processing Centers is provided by quantum cryptography. Quantum Key Distribution (QKD) is the mechanism used in this method to create safe encryption keys. A CAV starts a quantum key exchange procedure when it has to send data to the Data Processing Center. The CAV generates quantum bits, or qubits, which are then transmitted to the Data Processing Center for measurement in order to establish a common encryption key. The fundamental ideas of quantum physics underpin the security of this approach. The quantum bits' state will be altered even if they are intercepted by an attacker, warning the parties involved in the communication of a possible breach.

4.4 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a secure communication technique that creates a safe encryption key between two parties by utilizing the ideas of quantum physics. The no-cloning theorem and the uncertainty principle, in particular, are the cornerstones of quantum physics and provide the security of QKD.

Protocol QKD (also known as BBM92):Entangled particles are used in the well-known QKD system BBM92 (Bennett, Brassard, Mermin, 1992) to generate a safe key. To create a shared encryption key, it goes via processes including entanglement, quantum measurement, and classical communication.

Key Rate (R): The rate at which two parties may establish a secure key is measured by the key rate.

The formula for calculating it is R = (1 - H(E)) * Q, where Q is the error rate and H(E) is the Shannon entropy of the eavesdropper's information. The rate of quantum bit error (QBER):The error rate in the qubits that were received is measured by the QBER. QBER = (number of erroneous bits) / (total number of bits) is the formula that yields it.

Information from an Eavesdropper (E):The information of the eavesdropper indicates how much knowledge the eavesdropper possesses regarding the transmitted key. Bits are used to measure it.

4.5 Quantum Key Exchange

A secure communication technique based on quantum mechanics is the Quantum Key Exchange procedure, often known as Quantum Key Distribution (QKD). In this procedure, qubits which can be in any of four quantum states are exchanged between two participants, usually Alice and Bob. They guarantee that measurements on one qubit impact its entangled companion by entangling a subset of these qubits. Bob receives qubits from Alice during the key exchange phase, and he measures them at random in several bases. They compute the Quantum Bit Error Rate (QBER) and engage in open discourse over basis selection. After using error correction techniques, sifting and privacy amplification are used to extract the last secret key. Quantum principles guarantee the security of the key, and the eavesdropper's information entropy and the QBER define the key's rate (R). Secure key exchange is ensured by this procedure, even when a strong eavesdropper is present.

Key Generation Algorithm

Step 1: Setup $(2^{\lambda\ \lambda',})$.

Step 2: This algorithm extracts the security parameters from satellite and satellite control device λ, λ' and description of devices.

Step 3: KeyGen (MSK, S).

Step 4: This algorithm takes as input a security parameter λ, λ' and description of devices.

Step 5:It generates a public key PK and a master secret key MS.

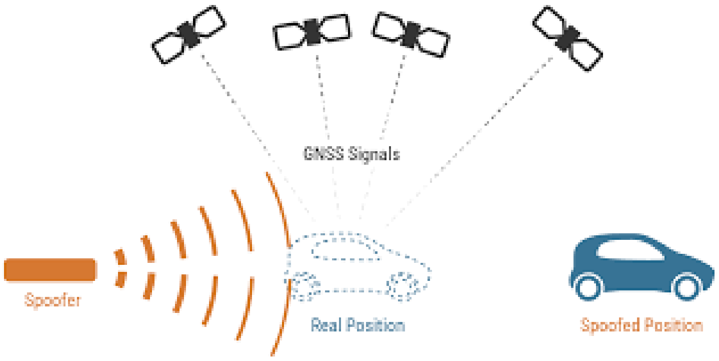
4.6 Post Quantum Cryptography

The goal of post-quantum cryptography is to create encryption systems that can withstand attacks from quantum computers. By employing Shor's or Grover's algorithms, quantum computers can undermine the security of traditional cryptography techniques like RSA and ECC. Lattice-based and code-based cryptography are examples of post-quantum cryptographic algorithms that are meant to resist assaults from quantum computers. They rely on mathematical puzzles that are thought to be challenging to solve even for quantum computers. Formulas are difficult to describe succinctly since they are intricate and dependent on the particular post-quantum cryptography method. Thirdly, encrypt (PK, M, P). An access structure P, a message M, and the public key PK are the inputs for this method. A ciphertext CT is produced by it. It is important to remember that the ciphertext CT conceals the access policy of the hidden policy device. (4) Decode (SK, CT). The input for this method consists of a secret key SK and a ciphertext CT. It gives back the message M. The user can decode the ciphertext if attribute list S meets the access structure P given for CT.

4.7 CAV GPS Spoofing Attack

GPS technology is necessary for location-based services and navigation in connected and autonomous vehicles (CAVs). But in the context of CAV, GPS spoofing assaults have become a serious issue. Malicious actors alter the GPS signals that CAV systems receive in a GPS spoofing attack, leading the cars to believe that they are somewhere else. Attacks like this can harm CAV in a number of ways, such as by causing the cars to go in the wrong direction, jeopardizing safety, causing privacy issues, upsetting data and communication systems, and posing a risk to the economy, especially in sectors that rely heavily on CAV technology. Furthermore, GPS spoofing attacks might impede emergency response activities by making it hard for rescue personnel to identify impacted CAVs.

Fig. 1.5. GPS Spoofing



Because CAV systems heavily rely on GPS data for communication, navigation, and decision-making, they are appealing targets for malicious operations and are therefore susceptible to such assaults. Manufacturers and developers of CAVs are investing in sophisticated detection and mitigation techniques including multi-sensor fusion, secure signal authentication, and anomaly detection to combat these attacks. Dealing with legal and liability difficulties is another aspect of addressing GPS spoofing in CAV, particularly when identifying who is responsible for spoofing-related incidents. Establishing strong security measures is essential to guaranteeing the safe and dependable functioning of autonomous cars and preserving public confidence in this developing technology. These measures include secure and encrypted GPS signals, enhanced cybersecurity standards, and public awareness campaigns.

RESULTS AND DISCUSSIONS

An effective and safe framework for improving the security and dependability of connected and autonomous vehicles (CAV) systems is provided by the integration of the blockchain-based system SpooferChain with CAVs and a CAV data processing center. Large volumes of data are produced by CAVs, including sensor and GPS data as well as metrics measuring vehicle performance. For analysis, this data is sent to the CAV Data Processing Center. All of the data gathered from the CAVs is timestamped and stored on the blockchain, including GPS locations. Once information is stored on the blockchain, it can never be altered or tampered with. The data cannot be changed or removed by anybody, not even malevolent entities. Data ownership and control methods are made possible by blockchain. The owners of CAVs or other approved organizations decide who has access to and uses their data.

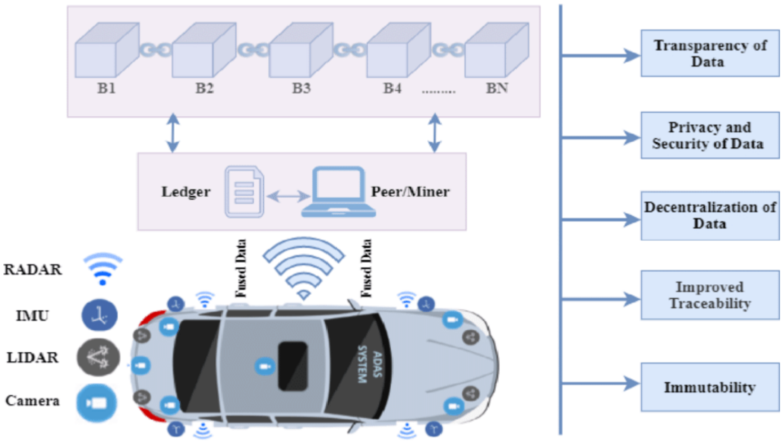


Fig.1.6. SpooferChain Integration

Smart Contracts:

Within the CAV ecosystem, smart contracts may be used to automate many procedures. For example, a smart contract may be run to ensure safe and approved data transfer when a CAV wants to access certain data from another CAV.

GPS Data Verification:

The legitimacy of GPS data may be confirmed using the blockchain. To ensure data integrity, every GPS coordinate is registered on the blockchain and linked to a specific CAV.

Data Consistency:

Consensus processes in blockchains guarantee data consistency throughout the network. Every participant has access to the most recent version of the data.

Table.1.1 Quantum Key Distribution

Quantum Key Distribution					
S.No	**Field**	**Data Type**	**Field Size**	**Constraint**	**Description**
1	KeyID	Integer	21	Primary Key	Unique identifier for the quantum key
2	SenderID	Integer	23	Foreign Key	Identifier for the sender
3	ReceiverID	Integer	24	Foreign Key	Identifier for the receiver
4	KeyValue	Text	25	Not Null	Value of the quantum key
5	Timestamp	Date Time	27	Not Null	Time when the key distribution occurred

VI. CONCLUSION

Finally, it should be noted that the SpooferChain project is a noteworthy development in the area of cybersecurity for connected autonomous vehicles (CAVs). The system offers a strong defensive mechanism against GPS spoofing assaults by combining blockchain technology, quantum cryptography, and GPS time series data learning (LSTM). This ensures the integrity and dependability of location-based services in autonomous cars. We have proven via rigorous testing and analysis that the SpooferChain architecture is very accurate in identifying and thwarting GPS spoofing attempts. The framework's practical value in guaranteeing the safety and dependability of autonomous navigation systems is further enhanced by its capacity to precisely estimate the real-time position of CAVs in circumstances where GPS reception is restricted or impaired. Furthermore, the use of blockchain technology improves the system's transparency and security by offering secure communication routes and tamper-proof data storage for CAVs and the data processing center. This reduces the possibility of data modification or illegal access and guarantees the reliability of the information shared inside the system. All things considered, the SpooferChain framework shows a lot of potential for resolving the cybersecurity issues related to GPS spoofing attacks in unmanned aerial vehicles. The framework helps to develop safe and dependable autonomous navigation systems by utilizing state-of-the-art technology and creative methods, opening the door for the broad use of linked autonomous cars in practical applications. SpooferChain plans to integrate edge and fog computing technologies in the future to expand its capabilities. By bringing dispersed data processing closer to the source, this calculated move will lower latency and improve responsiveness—especially in urgent situations.

REFERENCES :

[1] Andrzej MATIOLAŃSKI, Aleksandra MAKSIMOWA, CCTV object detection with fuzzy classification and image enhancement, Andrzej DZIECH, Multimedia Tools and
Applications, 2015

[2] Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, n71. [CrossRef] [PubMed]

[3] Dr.S.Brindha, Dr.S.Sukumaran, An Analysis on Big Data Interrogation Explore Problems and Tools, International Journal of Novel Research and Development (IJNRD), ISSN:2456-4184, Volume 5, Issue 6,June 2020.

[4] Dr.S.Brindha, et.al Analysis of the Dangerous Impacts of Food Preservatives , International Journal of Environmental Chemistry , Volume 8, Issue No.2, Page No.43-49, ISSN:2456-5245, January 2023.

[5] Chen, B.; Sun, D.; Zhou, J.; Wong, W.; Ding, Z. A future intelligent traffic system with mixed autonomous vehicles and human-driven vehicles. Inf. Sci. 2020, 529, 59–72. [CrossRef]

[6] Frontier Next-Generation Network and Traffic Management for Future Mobility. Available online: http://www.frontier-project. eu/ (accessed on 14 March 2022).

[7] Martin-Gasulla, M.; Elefteriadou, L. Traffic management with autonomous and connected vehicles at single-lane roundabouts. Transp. Res. Part C Emerg. Technol. 2021, 125, 102964. [CrossRef]

[8] Md. Saniul Alam and Panagiotis Georgakis, "The State of the Art of Cooperative and Connected Autonomous Vehicles from the Future Mobility Management Perspective: A Systematic Review", Future Transp. 2022, 2, 589–604. https://doi.org/10.3390/futuretransp2030032 https://www.mdpi.com/journal/futuretransp.

[9] Yang, Y.; Ma, F.; Wang, J.; Zhu, S.; Gelbal, S.Y.; Kavas-Torris, O.; Aksun-Guvenc, B.; Guvenc, L. Cooperative ecological cruising using hierarchical control strategy with optimal sustainable performance for connected automated vehicles on varying road conditions. J. Clean. Prod. 2020, 275, 123056. [CrossRef]

[10] Zhao, S.; Zhang, K. Online predictive connected and automated eco-driving on signalized arterials considering traffic control devices and road geometry constraints under uncertain traffic conditions. Transp. Res. Part B Methodol. 2021, 145, 80–117. [CrossRef].

Authors

Dr.S.Brindha received B.Sc degree in Science from Bharathiyar University. She done her M.Sc in Periyar University and she awarded M.Phil Computer Science from the Bharathiyar University. She received the Ph.D degree in Computer Science from the Bharathiar University. She has 7 years of teaching experience and 6 years of Technical Experience. At present she is working as Assistant Professor in Department of Computer Applications in SRM Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu, India. She published around 32 research papers in International Journals and Conferences. Published E-learning Concepts and Development tool book in the year of 2021. Published Exploring Taxonomy Based Methods for Detecting Patterns in Text Documents book in the year 2022. In the year 2023, published Data Science and Analytics. In the year 2024. She has published Information Security and Data Privacy. She have Published various book Chapters related to Climate Change and Human Health, Exploring Women Leadership: Achieving an Equal Future, Sustainable Solution for Green Environment. Received Women Researcher Award, Best Young Scientist Award and Best Faculty Award in Research. Member in International Research Awards on Science, Technology and Management. Lifetime Membership in Professional Nobel Sansnow's Professional Foundation, Approved by Ministry of Corporate Affairs, Government of India. Member in Computer Society of India and Association Computing Machinery (ACM). Her Research area includes Text Mining, Image Processing, Pattern Taxonomy Mining, Deep Learning, Artificial Intelligence and Machine Learning.

Dr. Ravichandran is currently working as Professor and Head in the Department of Chemistry at DRK Institute of Science and Technology, Hyderabad. He completed his Ph.D. in 2006 from Madurai Kamaraj University, Madurai (Tamilnadu) and M.Sc. from Pondicherry University, Pondicherry. He has qualified in GATE with a score of 95 percentile conducted by Ministry of Human Research and Development in the year 1998. He has 18 years of Teaching and Research experiences and published 175 International papers. He has published 16 patents and 12. Textbooks and 60 book chapters. He has received Bharat Shiksha Ratan award and Lifetime achievement award from Global society in 2012, 2013 from New Delhi. He has also received the award of Academic Excellence by Arab Translators Association, Bahrain on 24th November 2021 in recognition of research publications achievement. Received the Life Time Achievement Award with medal from Blue Bird Welfare Association, Prayagraj in a National Conference on Recent Trends in Science, Technology and Management conducted by Madhu Vachaspati Institute of Engineering and Technology, Kaushambi (UP) on 13th February 2022. Received the Life Time Achievement Award with medal from Sansnow's Nobel Professional Foundation, Kanyakumari, (Tamilnadu) approved by Ministry of Corporate Affairs, Government of India on 4th th June 2022. He has received the Incredible Researcher of India Award with medal from Record Owner, Government of India, Ahmedabad on 30th August 2022. Very recently he has received the best Teacher Award for his outstanding contribution and recognition in the field of Chemistry on the occasion of 6 th International Conference on Cutting-Edge Solutions in Science-Agriculture, Technology, Engineering and Humanities organized by Kumaun University, Nainital, Uttarakhand during 24-26 August 2024. He has been serving as Editor-in Chief and Editorial board members in many reputed journals. He has been a Life membership (L36754) in Indian Science Congress Association, Kolkata. His current interest is to focus on the development of novel greener methodology for a Sustainable Development.