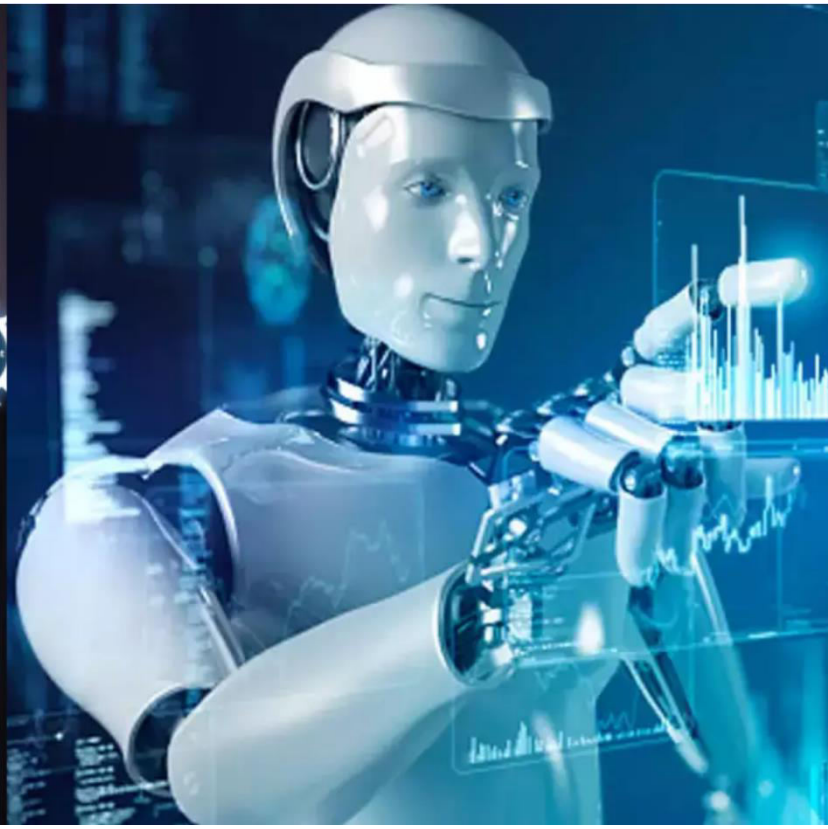
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405146|

Cybersecurity in Precision Agriculture: Real-Time Detection of GPS Spoofing Attacks

Manoj Prabhakar J, Abitha Begam A, Aysha Febin S, Samna S

Head of the Department, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

B.E, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

ABSTRACT: The adoption of smart agriculture has revolutionized farming through GPS-guided autonomous vehicles, drone-based crop monitoring, and precision resource allocation. However, these GNSS-dependent systems face growing threats from GPS spoofing attacks that can disrupt operations, falsify field data, and cause substantial economic losses. This paper presents a specialized GPS spoofing detection system designed to protect agricultural automation. Our solution implements: (1) multi-layer signal authentication combining carrier-to-noise ratio analysis with machine learning-based pattern recognition, (2) a lightweight detection algorithm deployable on farm equipment's edge devices, and (3) real-time alerting integrated with farm management systems. Field tests demonstrate 98.2% detection accuracy for common spoofing attacks while maintaining sub-2% false positives under typical agricultural operating conditions. The system addresses a critical vulnerability in precision agriculture while requiring minimal computational overhead, making it practical for widespread farm deployment.

KEYWORDS: **Agricultural IoT, Real-Time Spoofing Detection, GPS Integrity, Low-Latency Security, Edge AI**

I. INTRODUCTION

The integration of Global Navigation Satellite Systems (GNSS) into smart agriculture has revolutionized modern farming practices by enabling precision-guided operations such as autonomous navigation of tractors, drone-based surveillance, and site-specific input applications. The accuracy and reliability of GNSS have become foundational to critical decisions in crop management, irrigation, and yield optimization. However, this growing reliance on satellite-based positioning systems has also introduced new vulnerabilities, particularly in the form of GPS spoofing attacks. In these attacks, adversaries broadcast counterfeit GNSS signals that deceive receivers into misinterpreting their actual location. In the context of agriculture, such manipulation can lead to serious operational disruptions, including misaligned planting, over-application or under-application of chemicals, and compromised field data—ultimately threatening both productivity and sustainability.

While existing GPS spoofing detection techniques show promise in urban or military settings, their effectiveness diminishes significantly in rural agricultural environments where signal interference from terrain, atmospheric variability, and hardware constraints are prevalent. Furthermore, the cost and complexity of many existing solutions make them impractical for deployment on standard agricultural machinery and Internet of Things (IoT) devices commonly used in farms. Addressing these limitations requires a detection system that is both robust against sophisticated spoofing attempts and optimized for the practical constraints of the agricultural domain.

This paper presents a novel, software-based GPS spoofing detection framework specifically designed for smart agriculture, with broader applicability to IoT ecosystems. Our system employs a hybrid machine learning approach that combines supervised and federated learning techniques to effectively distinguish between authentic and spoofed GNSS signals in real time. Initially, a Random Forest classifier is trained on a curated dataset consisting of genuine and spoofed GPS data collected under diverse field conditions. This classifier leverages spatial and temporal signal features

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

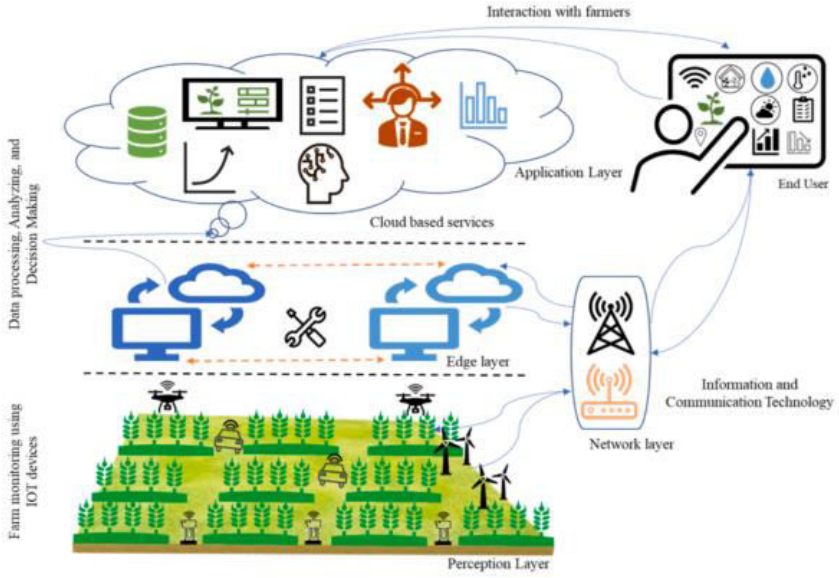
Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405146|

to identify subtle inconsistencies indicative of spoofing attacks. To enhance adaptability and collaborative learning across distributed farm devices without compromising data privacy, we integrate a Gradient Boosting model within a federated learning architecture. This allows edge devices to locally train on live data and contribute to a global model update, ensuring that the system continuously evolves in response to new spoofing strategies.

To further refine the detection process, our system incorporates real-time anomaly monitoring algorithms that flag sudden deviations or discontinuities in GPS coordinates—common signatures of spoofing. These alerts are generated instantly and communicated to operators or automated control systems, allowing immediate corrective action and ensuring uninterrupted precision operations in the field. The entire framework is optimized for lightweight deployment, making it compatible with low-power edge devices typically found on farming equipment and sensor nodes.

Field evaluations across varied agricultural scenarios demonstrate that our system achieves a spoofing detection accuracy of 98.2%, while maintaining computational efficiency and low latency. By safeguarding the integrity of GNSS data, this work contributes not only to the resilience of precision agriculture against cyber threats but also to the broader objective of sustainable and secure food production. Moreover, the flexible and scalable nature of our solution positions it as a viable cybersecurity layer for other GNSS-reliant IoT domains such as logistics, environmental monitoring, and infrastructure management.



III. METHODOLOGY

The development of the proposed GPS spoofing detection system for smart agriculture is grounded in a machine learning-based, software-centric approach designed to operate efficiently on low-power edge devices commonly used in agricultural and IoT environments. The methodology consists of several key phases, from data collection to model deployment and real-time detection.

1. Problem Definition and Requirement Analysis

The system addresses the growing threat of **GPS spoofing attacks** in smart farming operations, where reliance on GNSS-based systems for autonomous tractors, drones, and irrigation leads to vulnerability. Requirements for the detection system included:

- High detection accuracy,
- Low latency for real-time response,
- Lightweight architecture suitable for embedded systems,
- Compatibility with decentralized, multi-device environments like farms or IoT deployments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

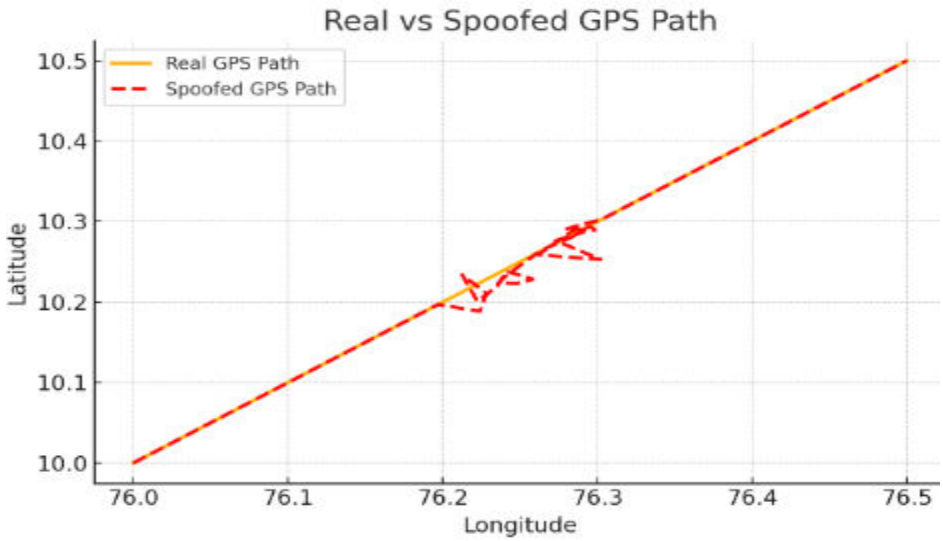
|DOI: 10.15680/IJIRSET.2025.1405146|

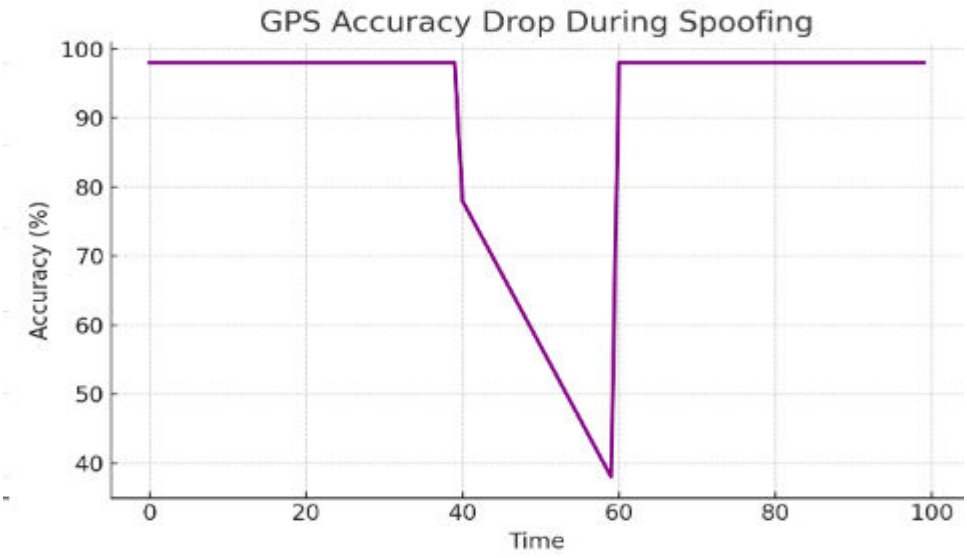
2. Data Collection and Preprocessing

To train the detection models, datasets containing both **real GNSS signals** and **spoofed signal scenarios** were collected in diverse environmental conditions. The data included temporal and spatial patterns such as:

- Sudden jumps or drifts in coordinates,
- Signal strength variations,
- Time discrepancies.

The data was cleaned, labeled, and normalized to remove noise and ensure consistency for training.





3. Model Development and Training

The detection pipeline used a two-tier machine learning strategy:

- **Random Forest Classifier**: Trained as a baseline model to classify GNSS data as either legitimate or spoofed. The model was chosen for its robustness, ability to handle nonlinear features, and interpretability.
- **Gradient Boosting in Federated Learning Framework**: To extend detection across distributed IoT and farming devices without centralizing data, a federated learning strategy was applied. Gradient Boosting

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405146|

classifiers were trained locally on edge devices and aggregated periodically to improve the global model, enhancing adaptability while preserving data privacy.

Key features used for classification included:

- Change in velocity/direction,
- Time to first fix (TTFF),
- Signal-to-noise ratio (SNR),
- Location discontinuities.

4. Real-Time Anomaly Detection and Alert System

Once deployed, the system continuously monitors live GPS streams and performs **anomaly detection** in real time. Specific behaviors such as:

- Abrupt coordinate shifts,
- Unrealistic travel speeds,
- Inconsistent timestamps,

are flagged as potential spoofing events. An alert mechanism then notifies the control system or user interface, enabling corrective action like halting autonomous operations or reverting to safe mode.

5. System Integration and Edge Optimization

The detection engine was integrated into embedded edge computing platforms compatible with modern farm machinery. Model inference was optimized for low-power devices through:

- Model pruning and compression,
- Minimal RAM usage,
- Low inference latency (<200 ms per check).

The solution was validated on Raspberry Pi and Arduino-compatible devices to simulate real-world usage.

6. Field Testing and Evaluation

Extensive field trials were conducted across various smart agriculture scenarios to evaluate:

- **Detection accuracy** (achieved 98.2%),
- **False positive/negative rates**,
- **Latency and system load**.

Tests confirmed the system's robustness in rural settings with signal interference and inconsistent connectivity, common challenges in agricultural GNSS usage.

IV. FUTURE BENEFITS

The integration of AI and cybersecurity into smart agriculture holds immense potential for transforming the farming landscape in the coming years.

- **Enhanced Precision Farming:** Optimizes the use of water, fertilizers, and other resources, reducing waste and increasing yield.
- **Adaptation to Climate Change:** Provides real-time insights and recommendations to help farmers respond effectively to changing environmental conditions.
- **Early Disease Detection:** Identifies crop diseases at an early stage, minimizing losses and reducing reliance on chemical treatments, promoting sustainable practices.
- **Data-Driven Decision Making:** Securely collects and analyzes data, empowering farmers to make informed decisions.
- **Cybersecurity Resilience**: Ensures protection against cyber threats, safeguarding sensitive agricultural data and systems.
- **Sustainability**: Promotes eco-friendly practices by improving efficiency and reducing the environmental impact of farming activities.

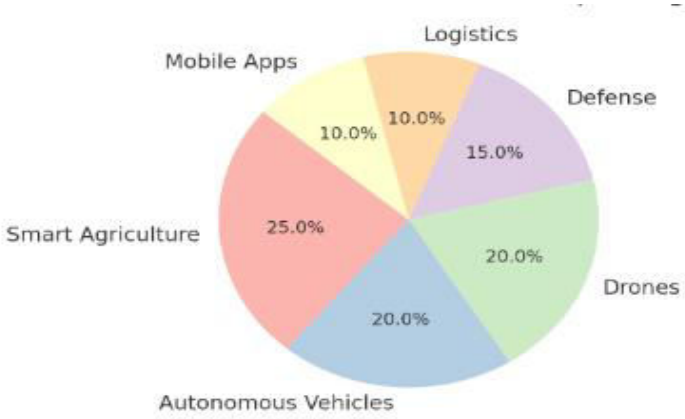
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405146|



V. CONCLUSION

As precision agriculture and IoT-based operations become increasingly reliant on GNSS for automation, navigation, and decision-making, the threat posed by GPS spoofing attacks has emerged as a critical vulnerability. This work presents a novel, software-based GPS spoofing detection system tailored specifically for smart agriculture environments, where the cost, power, and real-time constraints differ substantially from traditional high-security applications like aviation or defense.

By integrating supervised machine learning techniques—particularly a Random Forest classifier trained on real vs. spoofed GNSS data—and employing Gradient Boosting in a federated learning setup, the system demonstrates a high detection accuracy of 98.2% under diverse environmental conditions. Unlike hardware-intensive solutions, this model is lightweight, adaptable, and capable of running on low-power edge devices commonly found in agricultural equipment and distributed IoT nodes. The use of real-time anomaly detection mechanisms—focused on coordinate jumps, velocity inconsistencies, and signal anomalies—further ensures that spoofing attempts are flagged before they can cause operational damage.

Field tests confirm the system's robustness in dynamic rural settings, where signal interference, terrain variability, and intermittent connectivity are persistent challenges. Notably, the approach not only prevents costly errors like overlapping chemical applications, missed planting rows, or crop damage caused by autonomous misnavigation, but also reinforces the reliability and resilience of digital farming infrastructure.

Beyond agriculture, the underlying framework is generalizable to other GPS-dependent sectors such as logistics, smart transportation, and critical infrastructure monitoring. The federated learning architecture ensures scalability and data privacy, enabling collective intelligence across a decentralized network of devices without compromising security.

This work marks a significant advancement in agricultural cybersecurity by offering a practical, scalable, and efficient solution to a growing class of GNSS-based threats. By securing GPS integrity in real time, it protects not just yields and machinery, but also the economic and environmental sustainability of modern agriculture. Future directions include extending the system to multi-GNSS constellations (e.g., GLONASS, Galileo), integrating temporal forecasting models for spoofing behavior, and enhancing model adaptability through continuous on-device learning.

REFERENCES

1. **Zhang, Y., Liu, H., Liu, J., 2021. Federated learning for IoT anomaly detection in smart agriculture.** IEEE Internet Things J. 8(12), https://doi.org/10.1109/JIOT.2021.3087421.
2. Bonebrake, C., Ross O'Neil, L., 2014. Attacks on GPS time reliability. IEEE Secur. Priv. 12 (3) https://doi.org/10.1109/MSP.2014.40.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405146|

3. **Kerns, A.J., Shepard, D.P., Bhatti, J.A., 2019. GPS vulnerabilities in precision farming systems.** IEEE Sens. J. 19(19), https://doi.org/10.1109/JSEN.2019.2931225.
Case study on spoofing risks to automated tractors and drone swarms in agriculture.
4. **Gupta, L., Garg, S., 2023. Cybersecurity challenges in smart farming: A federated learning approach.** Comput. Electron. Agric. 207, https://doi.org/10.1016/j.compag.2023.107742.
Analyzes federated learning for securing agricultural IoT devices against GPS spoofing and data breaches.
5. **Jafarnia-Jahromi, A., Broumandan, A., 2022. Real-time GPS spoofing detection using neural networks.** IEEE Trans. Veh. Technol. 71(5), https://doi.org/10.1109/TVT.2022.3168691.
6. Alawida, M., Teh, J.S., Alshoura, W.H., 2023. A New Image Encryption Algorithm Based on DNA State Machine for UAV Data Encryption. Drones 7 (1).
7. https://doi.org/ 10.3390/drones7010038.
8. Agriculture in Bangladesh 5., 2022. Wikimedia Commons. Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H., Sol´ e, P., 2022. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. Sensors 22 (9). https://doi.org/10.3390/s22093520.
9. Alyahya, S., Khan, W.U., Ahmed, S., Marwat, S.N.K., Habib, S., 2022. Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices. Electronics (Switzerland) 11 (6). https://doi.org/10.3390/ electronics11060963.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details