Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 1
Month 2024

Tiny Machine Learning for Improved Food Traceability and Security

Mrs. Priyadarshani Shivakumar Mali[1], Mr. Satish Bapuso Kale[2], Mr. Vaibhav Khanderao Kamble[3], Mr. Hemant Appa Tirmare[4], Mr Ganesh R .Shinde[5]
Assistant Professor[1,4,] Bharati Vidyapeeth's College of Engineering [1], Department Of Technology Shivaji University Kolhapur2,3,4,5
priyadarshaniomali@gmail.com, sbk_tech@unishivaji.ac.in, hat_tech@unishivaji.ac.in, vkk_tech@unishivaji.ac.in, ganesh.ideas@yahoo.co.in,

Abstract
Food traceability and security are critical aspects of the modern food supply chain. Ensuring the safety and authenticity of food products is essential for both consumer health and the integrity of the industry. This paper explores the application of Tiny Machine Learning (TinyML) as a transformative technology to enhance food traceability and security. TinyML leverages machine learning algorithms on resource-constrained devices, making it a promising solution for the challenges posed by the food supply chain. This study reviews the current landscape of food traceability and security, identifying the limitations and vulnerabilities in existing systems. It then introduces the concept of TinyML and its suitability for deployment in various stages of the food supply chain. The paper delves into case studies and practical implementations of TinyML in food production, processing, transportation, and distribution. It highlights how edge AI and sensor technologies can provide real-time data analysis, enabling rapid identification of contaminants, spoilage, and counterfeit products. Furthermore, the use of TinyML in IoT-enabled devices enhances supply chain visibility and transparency. We present results from experimental deployments and highlight the benefits of TinyML, including reduced response times to incidents, enhanced traceability, and the prevention of food fraud. Additionally, we discuss the challenges associated with implementing TinyML in the food industry, including model optimization, data privacy, and regulatory compliance.
Keywords: Food traceability ,security, CNN, machine Learning, tiny ML

Introduction: the paper underscores the vital role of the global food supply chain in ensuring the safety and availability of food products. With growing concerns about food safety and traceability, the need for innovative solutions is evident. Tiny Machine Learning (TinyML) emerges as a promising technology, facilitating real-time data analysis at the edge of the network. The paper explores TinyML's application in enhancing food traceability and security, emphasizing benefits like quicker response times and fraud prevention. Through case studies, it demonstrates TinyML's transformative potential in fortifying food supply chains. While acknowledging challenges such as model optimization and regulatory compliance, the paper aims to provide valuable insights for industry stakeholders and researchers interested in leveraging TinyML to safeguard consumer well-being.

Objectives: The primary goal is to explore and promote the application of TinyML in enhancing food traceability and security.

Methods: food traceability and security

Results: The integration of Tiny Machine Learning (TinyML) in food traceability and security transforms the food supply chain by ensuring safety and authenticity. TinyML's real-time monitoring swiftly responds to deviations, minimizing risks like contamination and temperature fluctuations. Its anomaly detection offers proactive security, reducing unauthorized access. With edge-based processing, TinyML ensures data privacy, extending device lifespans, and lowering costs. It authenticates and monitors food quality, ensuring compliance with safety standards. Predictive maintenance minimizes equipment failures, reducing security vulnerabilities. TinyML's reduced network dependency enables continuous monitoring, even in areas with limited coverage, enhancing traceability compliance. In essence, TinyML is a transformative solution addressing challenges in the food industry, reinforcing public health, trust, and supply chain integrity.

Conclusions: In conclusion, this paper highlights Tiny Machine Learning's (TinyML) transformative role in improving food traceability and security. It provides a roadmap for stakeholders to harness TinyML's power in safeguarding supply chains and ensuring consumer safety. TinyML's integration enables real-time analysis at the edge, enhancing responses to deviations in temperature and detecting contaminants. In security, it excels in anomaly detection, predicts equipment maintenance, and reduces vulnerabilities. Embracing TinyML is crucial for creating resilient and responsive systems, protecting public health, and upholding the integrity of the food supply chain.

Keywords: ***Food traceability ,security, CNN, machine Learning, tiny ML***

1. Introduction

The food supply chain is a complex and globally interconnected network that plays a vital role in ensuring the availability and safety of food products for consumers worldwide. From farm to table, food products pass through numerous stages of production, processing, transportation, and distribution, involving multiple stakeholders. In recent years, concerns about food safety, authenticity, and traceability have gained significant attention, driven by incidents of contamination, fraud, and quality issues.

Ensuring the security and traceability of food products is of paramount importance to protect consumer health and maintain the integrity of the food industry. The ability to quickly identify and address issues such as contamination, spoilage, or fraudulent labeling is crucial. To achieve this, innovative technologies are required, and Tiny Machine Learning (TinyML) emerges as a promising solution.

TinyML represents the application of machine learning and artificial intelligence on resource-constrained, edge devices. This technology enables real-time data analysis and decision-making at the edge of the network, making it well-suited for addressing the challenges posed by the food supply chain. TinyML can be integrated into sensors and IoT devices at various points in the supply chain to provide continuous monitoring, data analysis, and immediate responses to incidents.

This paper explores the use of TinyML in the context of food traceability and security. It reviews the current state of food traceability and security, highlighting the limitations of existing systems. It introduces the concept of TinyML and its potential to revolutionize the way we ensure the safety and authenticity of food products.

Throughout the paper, we will delve into case studies and practical implementations of TinyML in different stages of the food supply chain. We will discuss the benefits of this technology, including reduced response times, enhanced traceability, and the prevention of food fraud. Moreover, we will address the challenges associated with implementing TinyML in the food industry, such as model optimization, data privacy, and regulatory compliance.

In this paper aims to shed light on the transformative potential of TinyML in enhancing food traceability and security. It provides valuable insights for industry stakeholders, policymakers, and researchers seeking to leverage the power of TinyML to fortify food supply chains and safeguard consumer well-being.

2. RELATED WORK

The scientific community has already provided numerous Tiny Machine Learning (TinyML) solutions in various domains, including healthcare [3,4,5] and automotive [6,7,8]. While this article primarily focuses on developing methods to enhance food supply chain security, it is worth briefly examining solutions related to agricultural and machinery security. Previous research in the domain of food supply chain security and traceability has highlighted the growing need for innovative solutions to address challenges related to contamination, fraud, and quality control. IoT and edge computing have emerged as promising technologies for real-time data monitoring and analysis within the food supply chain. Additionally, blockchain technology has gained attention for its potential to create transparent and tamper-proof records of food product journeys. Traditional machine learning approaches have been applied to food safety and quality control, particularly in detecting contaminants and pathogens. While Tiny Machine Learning (TinyML) has been widely recognized for its potential in various applications, its specific role in improving food traceability and security has not been extensively explored[1,2]. This paper aims to bridge this gap by investigating the implementation of TinyML in the food supply chain, considering its suitability for resource-constrained environments and the challenges associated with model optimization, data privacy, and regulatory compliance.

In the paper [9], the authors detail the design of sparse, deep tiny neural networks (DTNNs) and their automatic conversion into an STM32 microcontroller-optimized C-library using the X-CUBE-AI toolchain. Their experiments demonstrate the feasibility of deploying DTNNs for atmospheric pressure forecasting in an economical and cost-effective system. The system exhibits a FLASH occupancy of 45.5 KByte and a RAM occupancy of 480 Byte. Notably, this system was implemented in a real-world setting, achieving prediction quality comparable to a cloud-based deep neural network (DNN) model. However, it holds the advantage of processing all relevant data locally at environmental sensors, eliminating the need for raw data transmission to the cloud.

In the work [10], the authors emphasize the increasing complexity of applications and the integration of machine learning and artificial intelligence into the software development lifecycle. They specifically discuss the significance of Azure DevOps as a critical framework rapidly adopted by many organizations to reduce product development costs and enhance customer success. The authors present a unique DevOps framework tailored for the development of intelligent TinyML dairy agricultural sensors, highlighting the cost-effective development of high-quality products that benefit small-scale farmers.

In another study [11], the research team explores the potential of creating a framework for deploying artificial intelligence models in resource-constrained computing environments. This framework aims to enable remote rural areas and small-scale farmers to actively participate in the data revolution, contribute to the digital economy, and play a role in building a sustainable food supply. The work envisions democratizing AI to benefit all, with the ultimate goal of establishing a sustainable food future.

In the study described in [12], researchers delve into the application of machine learning on embedded devices to identify abnormalities using advanced low-power neural networks. Leveraging the cutting-edge TinyML framework, they enable the creation and deployment of Edge AI, allowing deep learning to be performed on low-power computer systems that collect sensor data in the field. In their experiments, a Kenmore top-load washing machine was equipped with an Arduino Nano 33BLE development board. The accelerometer sensor on the Arduino was utilized to capture normal data from a balanced laundry load and abnormal data from an unbalanced laundry load during the washing process. Subsequently, two different neural network models, autoencoder and variational autoencoder, were trained using the normal data to identify abnormalities.

The work detailed in [13] addresses several security challenges and concerns related to IoT devices. The author discusses layer-by-layer security procedures applicable to IoT, emphasizing the need for robust security measures. Additionally, they developed a TinyML framework based on the TensorFlow module, which is integrated with the CTI platform to predict potential threat propagation to smart devices using a Naive Bayes supervised machine learning classifier. The final solution exhibits high accuracy, achieving 96.8 percent accuracy for the training dataset and 96.3 percent accuracy for the test dataset in predicting threats, underlining the efficacy of the approach.

3. FOOD TRACEABILITY AND SECURITY

Food traceability and security are essential components of the food supply chain, ensuring the safety and authenticity of food products from production to consumption. These two aspects are of paramount importance in safeguarding public health, maintaining consumer confidence, and protecting the integrity of the food industry. Here's an overview of food traceability and security:

Food Traceability:

1. **Definition:** Food traceability is the ability to track and trace the movement of food products and their ingredients throughout the supply chain. It involves documenting every step of production, processing, distribution, and retail to identify the origins and destinations of food items.
2. **Importance:** Traceability allows for the quick identification and recall of potentially contaminated or unsafe products. It also helps in identifying the

source of foodborne outbreaks, minimizing their impact.

3. **Methods:** Various methods are employed for food traceability, including barcoding, QR codes, RFID (Radio-Frequency Identification), and blockchain technology. These technologies enable the recording and retrieval of detailed information about a product's journey.
4. **Regulatory Requirements:** Many countries have implemented traceability regulations that require food businesses to maintain records for a specific period. Compliance with these regulations is crucial for food safety and quality control.

Food Security:

1. **Definition:** Food security encompasses measures to protect the food supply chain against intentional contamination, fraud, and unauthorized access. It aims to ensure the safety and authenticity of food products and maintain consumer confidence.
2. **Challenges:** The global food supply chain faces numerous challenges related to food security, including food fraud (e.g., adulteration or mislabeling), bioterrorism threats, and the potential for contamination with harmful substances.
3. **Technologies:** Various technologies and approaches are employed to enhance food security. These include real-time monitoring, authentication, and rapid testing methods to detect contaminants and adulterants.
4. **Legislation and Regulation:** Governments and international bodies have implemented regulations to address food security concerns. These include the Food Safety Modernization Act (FSMA) in the United States and the Global Food Safety Initiative (GFSI) standards.

Integration of Traceability and Security:

Food traceability and security are closely intertwined. The ability to trace products' origins and movements can aid in security efforts by identifying vulnerabilities and enabling quick responses to threats or incidents. Integrated systems that combine traceability and security measures offer a comprehensive approach to ensuring the safety and authenticity of food products.

4. TINY MACHINE LEARNING

Tiny Machine Learning (TinyML) is a rapidly evolving field that focuses on implementing machine learning (ML) on resource-constrained devices, such as microcontrollers, sensors, and other edge devices. It enables these small devices to perform real-time data analysis and make decisions locally, without the need for a constant connection to powerful servers or cloud computing resources. Here are some key aspects of the technology of TinyML:

Resource-Constrained Devices: The central feature of TinyML is its compatibility with devices that have limited processing power, memory, and energy resources. These devices are commonly found in IoT applications, wearable technology, and embedded systems.

Model Optimization: Given the constraints of resource-constrained devices, model optimization is critical. This involves techniques like quantization, pruning, and model compression to reduce the size and computational complexity of ML models while maintaining acceptable performance.

Edge Inference: TinyML models are designed to perform inference (making predictions or decisions) on the edge, where data is collected. This enables real-time processing and rapid responses, reducing the need for data transmission to a central server.

Sensors and Data Collection: TinyML often integrates with sensors to collect data from the environment. These sensors can capture various types of data, including images, audio, vibration, temperature, and more.

Energy Efficiency: Optimizing for low energy consumption is essential, especially in battery-powered devices. TinyML algorithms are designed to minimize energy usage to prolong device lifespans.

Latency Reduction: Edge inference with TinyML can significantly reduce latency, making it suitable for applications that require quick responses, such as gesture recognition, anomaly detection, and predictive maintenance.

Deployment and Management: TinyML models need to be efficiently deployed and managed on edge devices. Solutions for model updates, version control, and device management are crucial components.

Programming Frameworks: There are various programming frameworks and libraries available for developing TinyML applications. TensorFlow Lite for Microcontrollers and Edge Impulse are examples of platforms that support TinyML development.

Security and Privacy: Ensuring data security and privacy is essential, especially in applications where sensitive data is collected. Implementing secure communication and data handling practices is a key consideration.

Use Cases: TinyML is being applied in a wide range of fields, including healthcare (wearable health monitors), agriculture (crop monitoring), industrial IoT (predictive maintenance), environmental monitoring, and smart cities (traffic management).

5. INTEGRATION OF TINY MACHINE LEARNING (TINYML)

The integration of Tiny Machine Learning (TinyML) into food traceability and security systems offers significant advantages in enhancing the safety and authenticity of food products throughout the supply chain. Here are some key ways in which TinyML can be integrated into traceability and security measures:

1. Real-time Data Analysis: TinyML enables real-time data analysis at the edge of the network. In the context of food traceability, sensors and cameras can capture data on the condition of products, temperature, and other relevant parameters. TinyML algorithms can analyze this data locally, allowing for immediate responses to deviations from set standards. For example, temperature sensors combined with TinyML can detect temperature variations that could indicate spoilage or improper storage conditions.

2. Contaminant Detection: TinyML models can be trained to identify contaminants or foreign substances in food products. For instance, image recognition models deployed on embedded devices can analyze visual data to detect foreign objects or contaminants in food items as they move through the supply chain.

3. Anomaly Detection: TinyML is effective at detecting anomalies in data. This is particularly valuable for security and traceability. By continuously monitoring data streams from various sensors and devices, TinyML can identify unusual patterns that may indicate tampering or unauthorized access to food products. Any anomalies can trigger immediate alerts.

4. Authentication and Quality Control: TinyML can be used for product authentication and quality control. For instance, spectroscopy sensors combined with TinyML can assess the composition and quality of food products, ensuring they meet specified standards. If a product does not meet the required criteria, the system can take corrective actions.

5. Predictive Maintenance: The integration of TinyML enables predictive maintenance for machinery and equipment in the food supply chain. This is crucial for ensuring that production and storage facilities are operating smoothly and that any equipment malfunctions that could compromise security or traceability are detected and addressed promptly.

6. Edge Devices: TinyML models can be deployed on edge devices, such as microcontrollers, without the need for a continuous connection to central servers. This ensures that data processing and decision-making can occur locally, reducing latency and dependence on network connectivity.

7. Data Privacy and Security: Edge-based TinyML models can also enhance data privacy and security. Since data processing occurs at the edge, sensitive information may not need to be transmitted over networks, reducing the risk of data breaches or unauthorized access.

8. Quick Response and Alerting: TinyML can enable rapid response mechanisms. If a security breach or a traceability issue is detected, the system can trigger immediate alerts or actions, minimizing the impact of potential threats.

The integration of TinyML into food traceability and security systems offers a comprehensive and efficient approach to safeguarding the food supply chain. By combining real-time monitoring, anomaly detection, and rapid responses, it enhances the industry's ability to address challenges related to food safety and authenticity. Moreover, it allows for the implementation of preventive measures and continuous improvement in traceability and security processes.

6. ANALYSIS

The integration of Tiny Machine Learning (TinyML) into food traceability and security systems offers a myriad of benefits, revolutionizing the way the food supply chain ensures safety and authenticity. Real-time monitoring, enabled by TinyML, allows for immediate responses to deviations from established standards, reducing the risk of unnoticed issues like temperature fluctuations or contamination. The exceptional anomaly detection capabilities of TinyML provide a proactive approach to security, identifying unusual patterns and minimizing the risk of unauthorized access and tampering. Furthermore, TinyML's edge-based processing ensures data privacy and security, reducing the vulnerability to data breaches. The energy-efficient nature of TinyML is paramount for battery-powered devices, extending device lifespans and reducing operational costs. Moreover, TinyML can authenticate and control the quality of food products, ensuring compliance with safety standards and diminishing the risk of adulteration and fraudulent labeling. Predictive maintenance minimizes equipment failures, mitigating potential security vulnerabilities stemming from malfunctions. Reduced dependency on network connectivity enhances continuous monitoring, even in areas with limited network coverage, while its cost-effectiveness makes it an accessible technology for various supply chain stages. Compliance with traceability regulations is facilitated, enhancing the ability to trace product journeys and ultimately instilling consumer confidence in the safety and authenticity of food products. In essence, TinyML presents a transformative solution that addresses multiple challenges and risks within the food industry, reinforcing the safeguarding of public health, consumer trust, and the integrity of the food supply chain.

7. CONCLUSION

In conclusion, this paper underscores the potential of TinyML as a transformative technology for improving food traceability and security. It offers a roadmap for industry stakeholders, policymakers, and researchers to harness the power of TinyML to safeguard food supply chains and protect consumer well-being. The integration of Tiny Machine Learning (TinyML) into the domains of food traceability and security marks a significant leap toward enhancing the safety and authenticity of food products within the supply chain. This transformative technology enables resource-constrained devices to perform real-time data analysis and decision-making at the edge, leading to a host of benefits that fortify the food industry's efforts to protect consumers and uphold its integrity.

In the context of food traceability, TinyML empowers the collection of data from sensors and devices at various stages of the supply chain. This data is analyzed locally, enabling immediate responses to deviations from established standards. For instance, temperature sensors paired with TinyML algorithms can detect fluctuations that may signify spoilage or improper storage conditions. Furthermore, TinyML contributes to the detection of contaminants and foreign substances, ensuring that food products meet stringent safety criteria. It supports product authentication and quality control, using techniques such as spectroscopy and image recognition to assess composition and quality.

Security measures in the food supply chain also reap the benefits of TinyML. This technology excels in anomaly detection, identifying unusual patterns or activities that could indicate tampering or unauthorized access. Predictive maintenance facilitated by TinyML ensures the smooth operation of machinery and equipment, reducing the risk of security vulnerabilities due to equipment malfunctions.

Moreover, the deployment of TinyML on edge devices, such as microcontrollers, is a game-changer for the food industry. It reduces dependence on continuous network connectivity, enhancing data privacy and security. It allows for quick response and alerting mechanisms, ensuring that potential threats to security or traceability are met with immediate actions.

In summary, TinyML is an indispensable tool for bolstering food traceability and security efforts. It offers the means to create resilient and responsive systems that can protect public health, maintain consumer confidence, and safeguard the integrity of the food supply chain. The integration of TinyML represents an exciting leap forward, and as technology continues to advance, we can expect even more sophisticated applications in these critical domains. It is imperative that stakeholders in the food industry embrace and harness the potential of TinyML to meet the ever-evolving challenges of ensuring the safety and authenticity of our food products.

Refrences

[1] David, R.; Duke, J.; Jain, A.; Reddi, V.J.; Jeffries, N.; Li, J.; Kreeger, N.; Nappier, I.; Natraj, M.; Regev, S.; et al. TensorFlow Lite Micro: Embedded Machine Learning on TinyML Systems. *arXiv* **2021**, arXiv:2010.08678. [Google Scholar]

[2] Edge Impulse. Available online: https://www.edgeimpulse.com/ (accessed on 14 March 2022).

[3] Bian, S.; Lukowicz, P. Capacitive sensing based on-board hand gesture recognition with TinyML. In Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Virtual USA, 21–26 September 2021; pp. 4–5. [Google Scholar]

[4] Fedorov, I.; Stamenovic, M.; Jensen, C.; Yang, L.-C.; Mandell, A.; Gan, Y.; Mattina, M.; Whatmough, P.N. TinyLSTMs: Efficient Neural Speech Enhancement for Hearing Aids. *Interspeech* **2020**, *2020*, 4054–4058. [Google Scholar] [CrossRef]

[5] T'Jonck, K.; Kancharla, C.R.; Vankeirsbilck, J.; Hallez, H.; Boydens, J.; Pang, B. Real-time activity tracking using TinyML to support elderly care. In Proceedings of the 2021 XXX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 15–17 September 2021; pp. 1–6. [Google Scholar] [CrossRef]

[6] Roshan, A.N.; Gokulapriyan, B.; Siddarth, C.; Kokil, P. Adaptive traffic control with TinyML. In Proceedings of the 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 11 May 2021; pp. 451–455. [Google Scholar] [CrossRef]

[7] Andrade, P.; Silva, I.; Signoretti, G.; Silva, M.; Dias, J.; Marques, L.; Costa, D.G. An unsupervised TinyML approach applied for pavement anomalies detection under the internet of intelligent vehicles. In Proceedings of the 2021 IEEE International Workshop on Metrology for Industry 4.0 IoT (MetroInd4.0 IoT), Rome, Italy, 7–9 June 2021; pp. 642–647. [Google Scholar] [CrossRef]

[8] Lahade, S.V.; Namuduri, S.; Upadhyay, H.; Bhansali, S. Alcohol Sensor Calibration on the Edge Using Tiny Machine Learning (Tiny-ML) Hardware. *Meet. Abstr.* **2020**, *MA2020-01*, 1848. [Google Scholar] [CrossRef]

[9] Alongi, F.; Ghielmetti, N.; Pau, D.; Terraneo, F.; Fornaciari, W. Tiny neural networks for environmental predictions: An integrated approach with Miosix. In Proceedings of the 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 14–17 September 2020; pp. 350–355. [Google Scholar] [CrossRef]

[10] Vuppalapati, C.; Ilapakurti, A.; Chillara, K.; Kedari, S.; Mamidi, V. Automating tiny ML intelligent sensors DevOPS using Microsoft Azure. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 2375–2384. [Google Scholar] [CrossRef]

[11] Crossing the Artificial Intelligence (AI) Chasm, Albeit Using Constrained IoT Edges and Tiny ML, for Creating a Sustainable Food Future. Available online: https://www.springerprofessional.de/en/crossing-the-artificial-intelligence-ai-chasm-albeit-using-const/18435296 (accessed on 14 March 2022).

[12] Lord, M. TinyML, Anomaly Detection. Available online: https://scholarworks.calstate.edu/concern/theses/8336h7115?locale=en (accessed on 14 March 2022).

[13] Dutta, A.; Kant, S. Implementation of cyber threat intelligence platform on Internet of Things (IoT) using TinyML approach for deceiving cyber invasion. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Port Louis, Mauritius, 7–8 October 2021; pp. 1–6. [Google Scholar]