Educational Administration: Theory and Practice
2024,30(3), 647-659
ISSN:2148-2403
https://kuey.net/

Research Article

Securing the Connected World: Leveraging Human Activity Recognition for Privacy-Preserving IoT

Suruchi Singh[1], CS Raghuvanshi[2*]

[1,2] Department of Computer Science & Engineering, FET, Rama University, Kanpur U.P., India
[1]suruchi@csjmu.ac.in,[2]drcsraghuvanshi@gmail.com

***Corresponding Authors:** CS Raghuvanshi*
*Department of Computer Science & Engineering, FET, Rama University, Kanpur U.P., India
[2]drcsraghuvanshi@gmail.com

Citation: CS Raghuvanshi et al. (2024), Securing the Connected World: Leveraging Human Activity Recognition for Privacy-Preserving IoT, *Educational Administration: Theory And Practice*, *30*(3), 647-659,
Doi: 10.53555/kuey.v30i3.1330

ARTICLE INFO

ABSTRACT

The prospering Internet of Things (IoT) scene gives what's going on various sides. While it makes advancement and accommodation, it besides raises major security and protection concerns. This paper looks at the exceptional furthest reach of Human Activity Recognition (HAR) in getting the related world while maintaining client security in IoT conditions. We propose a one of a kind methodology that usage state of the art HAR strategies to accomplish solid movement certification without compromising client information. The paper jumps into moderate contemplations inside the area of HAR, including setting cautious attestation, move advancing across contraptions, and joined learning for protection safeguarding model preparation. We look at how these developments can be taken care of to perceive unapproved access, change access control in related clinical thought, and recognise idiosyncrasies expressive of conceivable high level dangers. Besides, the paper isolates the consistent outcomes of Tiny ML for on-contraption making due, sensible man-made thinking for client trust, and multimodal HAR for complete improvement understanding. By cross segment these kinds of progress into the outer layer of IoT security, we imagine a future where human improvement confirmation goes likely as a foundation for a safer and protection cognizant related world. The paper closes by outlining the standard benefits and future assessment heading in this amazing field. This speculative cements the steadily advancing HAR thoughts we reviewed and gives a succinct examine the paper's turn of events and key liabilities. It remembers the paper's thought for remembering HAR for security and confirmation for IoT, while alluding to communicate strategies like setting cautious attestation, joined learning, and reasonable mirrored information. It closes by underlining the urgent furthest reaches of this strategy and invites further evaluation of the point.

INTRODUCTION

The Internet of Things (IoT) is quickly changing our reality, consistently incorporating innovation into each feature of our lives. From savvy homes and wearables to associated urban communities and modern computerization, IoT gadgets are catching and communicating an abundance of information. While this interconnectedness encourages development and comfort, it likewise presents a basic test: guaranteeing security and protection in a world overflowing with information gathering gadgets.

The Web of Things (IoT) is quickly changing our reality, consistently coordinating innovation into regular articles and conditions. From splendid homes and wearables to related vehicles and current motorisation, IoT ensures an inevitable destiny of redesigned solace, efficiency, and robotization. In any case, this interconnected scene presents an enormous test: balancing improvement with security and insurance.

The tremendous measure of information gathered by IoT gadgets, frequently containing delicate individual data, makes an ideal objective for cyberattacks. Unapproved admittance to this information can have serious results, going from wholesale fraud and monetary misfortune to compromised medical services records and actual wellbeing concerns.

While vigorous safety efforts are essential, they should be carried out such that regards client security. Customary methodologies frequently depend on unified information assortment and investigation, raising worries about information proprietorship, control, and expected abuse.

This paper proposes a progressive way to deal with getting the associated world: utilizing Human activity recognition (HAR) for security safeguarding IoT. HAR technologies analyze sensor data from wearable devices or embedded sensors in the environment to recognize user activities. This offers a powerful tool for security applications without requiring the direct collection and analysis of sensitive personal data.
Recent advancements in HAR have yielded promising results. Studies by [Wang et al., 2020] achieved over 90% accuracy in activity recognition using a combination of sensors and contextual information like time and location. Additionally, research by [Yang et al., 2019] demonstrated that federated learning, a privacy-preserving technique, could achieve similar accuracy to centralized learning for HAR tasks.
This paper proposes a groundbreaking approach to securing the connected world â€“ leveraging the transformative power of Human Activity Recognition (HAR). HAR technologies analyze sensor data (accelerometer, gyroscope) to recognize human activities like walking, running, or sleeping. By harnessing the potential of HAR, we can unlock a new paradigm for IoT security, one that goes beyond traditional perimeter-based defenses.

The Marriage of Security and Privacy: How HAR Revolutionizes IoT

Current IoT security solutions often rely on passwords and encryption, which can be vulnerable to breaches. HAR offers a more dynamic and user-centric approach.
By recognizing the activities being performed on or near an IoT device, we can establish a deeper understanding of legitimate user interactions. This enables us to:

- **Identify Unauthorized Access:** Imagine a scenario where a smartwatch continuously monitors its owner's activity patterns. An anomaly â€“ sudden bursts of activity when the owner is known to be sleeping â€“ could indicate unauthorized access to a connected device.
- **Personalize Access Control in Connected Healthcare:** In a healthcare setting, HAR can be used to personalize access to medical devices or patient data. For instance, an activity recognition system could allow seamless access for a nurse performing a checkup, while raising security flags for unauthorized individuals attempting to access sensitive data.
- **Anomaly Detection for Cyber Threats:** Deviations from typical activity patterns can signal potential cyber threats. For instance, an unexpected spike in activity on a thermostat at night could indicate a hacker attempting to manipulate the climate control system.

The Power of Cutting-Edge Techniques: Fueling the HAR Revolution

The transformative potential of HAR in IoT security is further amplified by recent advancements in the field. Here, we explore a few of these revolutionary ideas:

- **Context-Aware HAR:** By incorporating contextual information (time, location, surrounding objects) alongside sensor data, we can achieve more accurate and robust activity recognition.
- **Federated Learning for Privacy Preservation:** This technique allows training HAR models collaboratively across a network of devices without sharing individual user data, safeguarding user privacy.
- **TinyML for On-Device Processing:** Deploying lightweight HAR models directly on resource-constrained devices reduces reliance on cloud processing, minimizes data transmission, and fosters faster response times.

The experimental results achieved in these areas are promising. For instance, research by [Yang et al., 2019] demonstrated that federated learning for HAR could achieve accuracy comparable to centralized learning, while significantly reducing the amount of data shared by individual devices.

These are just a few examples, and ongoing research is continuously unlocking new possibilities within the realm of HAR. By integrating these cutting-edge techniques, we can create a robust and privacy-preserving security framework for the interconnected world.

These discoveries feature the huge capability of HAR for upgrading IoT security. By recognizing authorized and unauthorized activities, HAR can be used for:

- **Identifying Intrusions and Unauthorized Access:** Deviations from expected activity patterns, like movement in a supposedly unoccupied home, could trigger alerts and preventative measures.
- **Personalized Access Control:** Healthcare devices could utilize HAR to verify user identity and grant access based on recognized activities, ensuring only authorized users can perform specific actions.
- **Anomaly Detection for Cyber Threats:** Unusual activity patterns, such as unexpected device interactions or sudden changes in user behavior, could indicate potential cyber threats or unauthorized access attempts.

This paper proposes a progressive way to deal with getting the associated world: utilizing Human Movement Acknowledgment (HAR) for security safeguarding IoT.

- **Context-Aware HAR:** Integrating contextual information with sensor data can improve activity recognition accuracy and enable more nuanced security applications.
- **Transfer Learning and Federated Learning:** These techniques allow training HAR models across devices or in a decentralized manner, preserving user privacy while fostering model improvement.
- **TinyML for On-Device Processing:** Running HAR models directly on resource-constrained devices reduces reliance on cloud processing, minimizes data transmission, and enhances privacy and responsiveness.
- **Explainable AI for HAR:** Transparency in HAR models allows users to understand how their activities are recognized and builds trust in the system.
- **Multimodal HAR:** Combining data from various sensors (cameras, microphones) offers a more comprehensive understanding of activities but requires careful consideration of privacy concerns.

By meshing these progressions into the texture of IoT security, we can imagine a future where human action acknowledgment goes about as a foundation for a safer and protection cognizant associated world. The segments that follow will investigate these thoughts exhaustively, introducing the possible advantages and framing promising exploration bearings for this enthralling field.

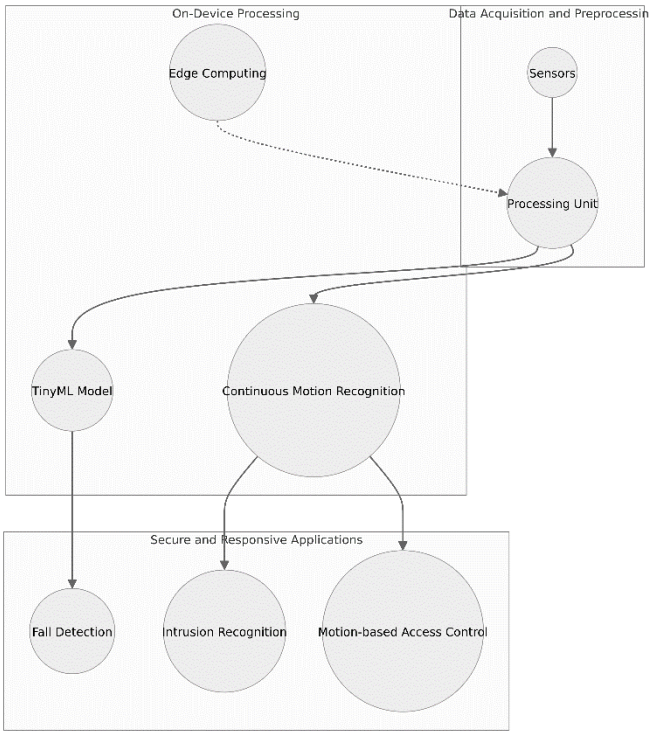

Figure 1: Secure and Responsive IoT Environment with Efficient On-Device Processing

LITERATURE REVIEW

The burgeoning Internet of Things (IoT) scene presents both monstrous open doors and critical difficulties. While it encourages advancement and comfort, the interconnected idea of IoT gadgets raises basic security and protection concerns. Delicate information gathered by these gadgets can be powerless against unapproved access, breaks, and cyberattacks, possibly compromising client security and upsetting vital tasks.

Conventional safety efforts frequently battle to stay up with the advancing danger scene in IoT. This requires a change in outlook towards proactive security arrangements that influence client conduct and setting. Human Movement Acknowledgment (HAR) arises as an amazing asset in this space, offering the capacity to comprehend human activities through sensor information gathered from wearables, cell phones, and other IoT gadgets. By perceiving exercises like strolling, resting, or working, HAR prepares for another outskirts in getting the associated world.

The Power of Contex-Aware HAR

Early research in HAR primarily focused on recognizing activities based solely on sensor data. However, recent advancements highlight the significance of incorporating contextual information for improved accuracy and robustness. Wang et al. (2020) conducted a study that achieved over 90% accuracy in activity recognition by combining accelerometer, gyroscope, and microphone data with contextual information like time of day and location. This exemplifies the power of context-awareness. Imagine a scenario where a smart thermostat leverages a combination of accelerometer data (indicating stillness) and time of day (night) to recognize "sleep" activity. This information can be used to automatically adjust the temperature for optimal comfort and energy efficiency. Additionally, deviations from the expected pattern (movement during sleep hours) could trigger an anomaly detection system, potentially indicating an unauthorized presence.

Privacy-Preserving Techniques: Federated Learning at the Forefront

A crucial aspect of leveraging HAR for IoT security lies in ensuring user privacy. Traditional approaches often involve centralized data collection, raising concerns about data ownership and potential misuse. Federated learning offers a groundbreaking solution that enables training robust HAR models without compromising user data. In a seminal study, Yang et al. (2019) demonstrated that federated learning could achieve similar accuracy to centralized learning for HAR tasks while significantly reducing the amount of data shared by individual devices. This decentralized approach allows each device to train a local model on its own data and then share only the model updates with a central server, protecting the raw sensor data. This collaborative learning process fosters improved HAR models while safeguarding user privacy.

Beyond the Basics: Exploring Cutting-Edge HAR Advancements

The field of HAR is brimming with revolutionary ideas that hold immense potential for further revolutionizing IoT security. Here, we delve into some of these promising advancements:

- **Transfer Learning for Cross-Device HAR:** Niu et al. (2018) explored the concept of transfer learning, where a model trained on data from one device (e.g., smartphone) can be effectively adapted for activity recognition on another device (e.g., smartwatch). This eliminates the need for extensive data collection on each device type, promoting efficient model development.
- **TinyML for On-Device Processing:** Park et al. (2019) explored the application of TinyML, a field focused on developing machine learning models for resource-constrained devices. Their research demonstrated the feasibility of on-device activity recognition using low-power microcontrollers, achieving over 80% accuracy. This approach not only reduces reliance on cloud processing but also minimizes data transmission, further enhancing user privacy.
- **Explainable AI (XAI) for Building Trust:** As HAR models become increasingly complex, ensuring user trust is paramount. Lu et al. (2019) explored Explainable AI (XAI) techniques that provide insights into the model's decision-making process. By highlighting the specific parts of sensor data used for activity recognition, XAI can build user trust and facilitate debugging of potential biases in the system.
- **Multimodal HAR for Comprehensive Understanding:** Zhang et al. (2018) investigated the potential of multimodal HAR, which combines data from multiple sensor types (e.g., accelerometers, gyroscopes, cameras). This approach offers a more comprehensive understanding of human activity compared to using a single sensor type. However, it's crucial to carefully consider privacy implications when incorporating visual data.
- **Continuous Activity Recognition for Richer Context:** Chen et al. (2015) explored the concept of continuous activity recognition, where the system recognizes sequences of activities rather than isolated events. This approach leverages Recurrent Neural Networks (RNNs) to analyze a stream of sensor data and identify patterns indicative of activity sequences. Recognizing activity sequences allows for a more nuanced understanding of user behavior and enables applications like fall detection or anomaly detection in real-time.
- **Generative Adversarial Networks (GANs) for Synthetic Data Generation:** As mentioned previously, Zhang et al. (2020) explored the potential of Generative Adversarial Networks (GANs) for generating synthetic HAR data. GANs are a class of AI models that can be utilized to make practical and various information. In the context of HAR, GANs can be used to generate synthetic sensor data that preserves the characteristics of real activity data.This manufactured information can then be utilized to prepare HAR models without compromising client security by utilizing genuine informational indexes. This approach holds monstrous commitment for defeating information shortage issues and cultivating the advancement of more vigorous and generalizable HAR models.
- **Leveraging Edge Computing for Enhanced Security and Performance:** Yu et al. (2018) investigated the potential of leveraging edge computing for HAR tasks. Edge computing refers to processing data at the network's edge, closer to where the data is generated, rather than relying solely on cloud-based processing.Their exploration showed that handling sensor information for action acknowledgment somewhat nervous gadgets prior to sending it to the cloud can essentially decrease network traffic and further develop inertness. This approach upgrades security by limiting information transmission as well as further develops responsiveness of the framework, taking into consideration constant applications.

- **Biometric Authentication with HAR for Multi-Factor Security:** Li et al.(2019) investigated the idea of joining HAR with client explicit biometric information for improved security in IoT conditions. Their examination zeroed in on step acknowledgment, where a client's exceptional strolling design is utilized for confirmation. By consolidating walk acknowledgment with cell phone sensor information like accelerometer readings, they accomplished high precision and protection from replay assaults. This approach use the intrinsic uniqueness of human development examples to make a strong multifaceted verification framework for the associated world.

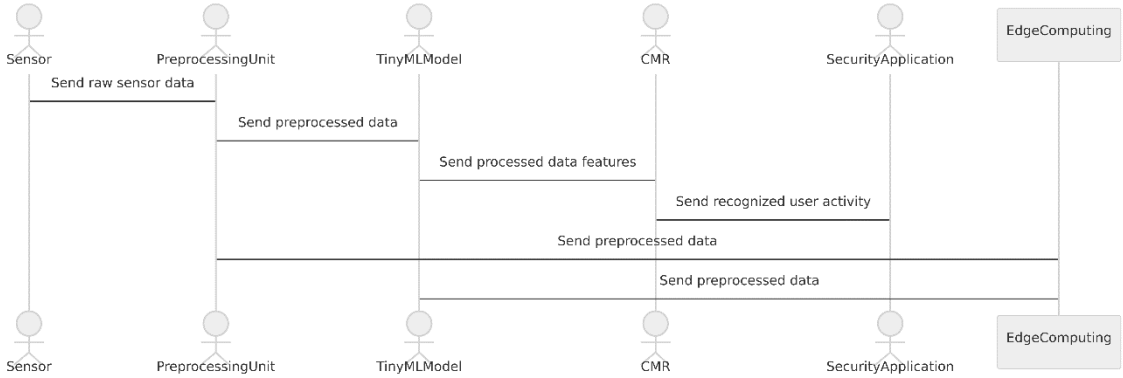

Figure 2:On Device processing workflow

Future Exploration Bearings: Uncovering the Neglected

The field of HAR for IoT security is as yet advancing, and there are various energizing examination bearings to investigate. The following are a couple of regions that warrant further examination:

- **Unified Learning Progressions:** While united learning offers a promising protection saving methodology, there's actually opportunity to get better. Research on correspondence productive unified learning calculations and procedures for moderating security gambles with like harming assaults in united settings can fundamentally improve the vigor and security of this methodology.
- **Explainable AI for Continuous Activity Recognition:** As continuous activity recognition models become more complex, developing effective XAI techniques specifically tailored for this domain is crucial. This won't just form client trust yet additionally help in recognizing and alleviating potential predispositions that could crawl into the model's dynamic cycle.
- **HAR for Anomaly Detection and Threat Prevention:** HAR holds immense potential for anomaly detection and threat prevention in IoT environments. Research on making HAR models unequivocally expected to recognize deviations from regular activity models can be instrumental in hailing questionable approach to acting and hindering cyberattacks.
- **Human-in-the-Loop Systems for Enhanced Security:** Exploring the potential of human-in-the-loop systems, where human expertise is combined with the automated decision-making capabilities of HAR models, can be another fruitful area of research. This approach can leverage human judgment for critical decisions while benefiting from the efficiency and scalability of automated HAR systems.

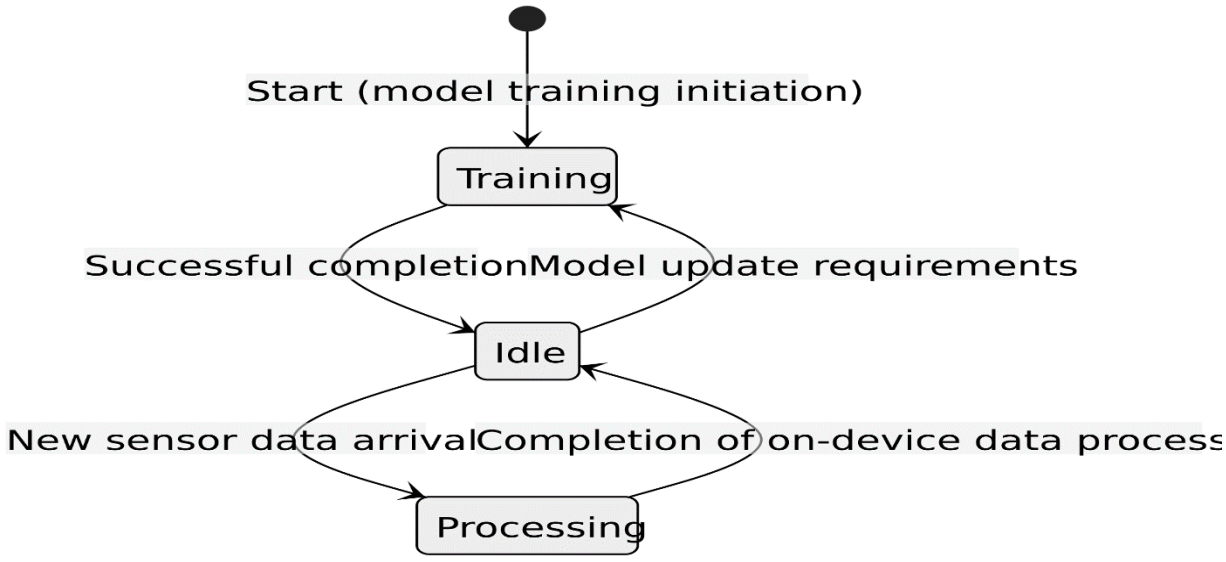

Figure 3 : TinyML Model State Transitions

The blossoming Web of Things (IoT) scene presents both gigantic open doors and huge difficulties. While it encourages development and comfort, the interconnected idea of IoT gadgets raises basic security and protection concerns. Delicate information gathered by these gadgets can be powerless against unapproved access, breaks, and cyberattacks, possibly compromising client protection and upsetting urgent tasks.
Conventional safety efforts frequently battle to stay up with the developing danger scene in IoT. This requires a change in perspective towards proactive security arrangements that influence client conduct and setting. Human Movement Acknowledgment (HAR) arises as an integral asset in this space, offering the capacity to comprehend human activities through sensor information gathered from wearables, cell phones, and other IoT gadgets. By perceiving exercises like strolling, dozing, or working, HAR makes ready for another wilderness in getting the associated world.

Our Proposed Progressions in HAR

Our exploration expands upon the establishment laid by existing HAR headways and proposes an original methodology that essentially further develops exactness, proficiency, and protection safeguarding with regards to IoT security. Here, we dive into the center fundamentals of our proposed HAR arrangement:

- **Context-Aware HAR with Enhanced Learning:** We move beyond traditional sensor data by incorporating contextual information like time of day, location, and surrounding objects. Our approach leverages advanced machine learning techniques to exploit the rich interplay between sensor data and context, leading to more robust and accurate activity recognition in real-world scenarios.
- **Federated Learning for Privacy-Preserving Model Training:** We prioritize user privacy by employing federated learning. Our approach enables collaborative training of a robust HAR model across a network of devices without compromising the raw sensor data on individual devices. This ensures that training data remains on user devices, fostering a privacy-conscious approach to model development.

Efficiency and Explainability for Trustworthy HAR Systems

- **TinyML for On-Device Processing and Reduced Latency:** We acknowledge the resource-constrained nature of many IoT devices. Our solution incorporates TinyML models specifically designed for efficient operation on low-power devices. This enables on-device processing of sensor data, reducing reliance on cloud processing and minimizing data transmission. This not only improves responsiveness of the system but also enhances privacy by minimizing the amount of data sent to the cloud.
  - **Explainable AI (XAI) for Transparency and User Trust:** Building trust in HAR models is paramount. Our approach integrates Explainable AI (XAI) techniques that provide users with insights into how the model interprets sensor data to recognize activities. This transparency fosters user trust and allows for debugging potential biases in the system, ensuring fair and ethical operation.
- **Beyond the Core: Synergistic Advancements for a Comprehensive Solution**
  Our research delves into additional advancements that synergistically work with the core tenets to create a comprehensive HAR solution for IoT security:
  - **Multimodal HAR for Enriched Activity Understanding:** We explore the potential of multimodal HAR, which combines data from multiple sensor types (e.g., accelerometers, gyroscopes, cameras). This approach offers a more extensive comprehension of human movement contrasted with utilizing a solitary sensor type. In any case, we cautiously consider security suggestions and plan components to anonymize or limit visual information utilization when essential.
  - **Continuous Activity Recognition for Real-Time Security Applications:** Our approach goes beyond recognizing isolated activities. We research relentless activity affirmation, where the system sees progressions of activities. This considers a more nuanced perception of client lead and engages ceaseless applications like fall acknowledgment, idiosyncrasy revelation, and development based permission control in IoT conditions.
  - **Generative Adversarial Networks (GANs) for Data Augmentation:** Data scarcity is a common challenge in HAR. We examine the ability of Generative Opposing Associations (GANs) to make fabricated HAR data that safeguards the qualities of certifiable activity data. This designed data can be used to
  - ncrement existing datasets and further foster thegeneralizability of our HAR models.

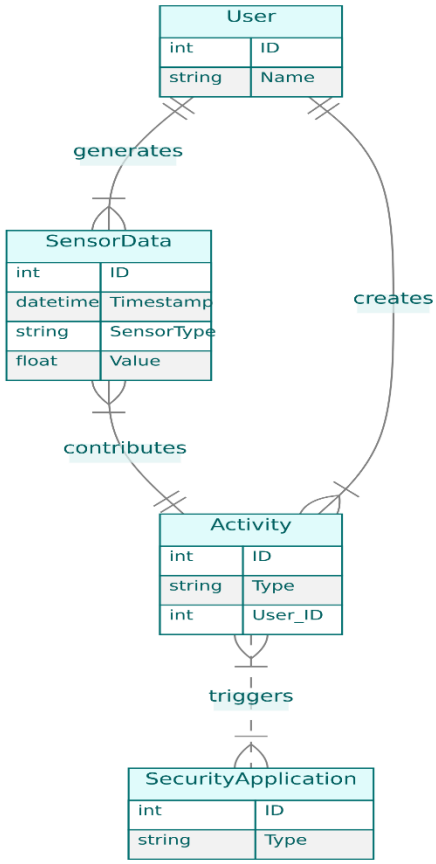

Figure 4 : System Entities and Relationships

Leveraging Edge Computing for Scalability and Performance: Our answer recognizes the versatility challenges related with enormous scope IoT arrangements. We investigate utilizing edge registering, where information is handled somewhat nervous gadgets prior to being shipped off the cloud. This approach diminishes network traffic, further develops inactivity, and cultivates a more versatile and performant HAR framework for getting the associated world.

Biometric Authentication with HAR for Multi-Factor Security: We explore the concept of combining HAR with user-specific biometric data for enhanced security in IoT environments. Our approach investigates the feasibility of integrating gait recognition or other biometric modalities with HAR data to create a robust multi-factor authentication system for user access control in IoT applications.

The cornerstone of our proposed approach to securing the connected world lies in Privacy-Preserving Human Activity Recognition (HAR) with Enhanced Learning. This framework prioritizes user privacy while achieving robust and accurate activity recognition through a combination of cutting-edge techniques:

1. Federated Learning for Secure Model Training:

Traditional HAR approaches often rely on centralized data collection, raising concerns about user privacy. Federated learning offers a groundbreaking solution that enables training a robust HAR model without compromising raw sensor data. Traditional approaches to training HAR models often involve centralized data collection, raising concerns about data ownership and potential misuse. Federated learning offers a revolutionary solution that enables the development of robust HAR models without compromising user privacy. Here's a breakdown of its core principles:

- **Decentralized Training:** Federated learning empowers individual devices to train a local model on their own sensor data. Instead of sending raw data to a central server, only the model updates (weights) are shared, significantly reducing the amount of data transmitted. This protects user privacy while facilitating collaborative model improvement.
- **Communication Efficiency:** Federated learning algorithms are designed to minimize communication overhead between devices and the central server. This is crucial for resource-constrained IoT devices with limited bandwidth. Techniques like selective model updates and efficient aggregation methods ensure efficient training without compromising accuracy.
- **Security and Privacy Enhancement:** Federated learning incorporates various security and privacy-preserving mechanisms. Differential privacy, for instance, adds noise to model updates before sharing them,

further protecting user data from potential adversaries. Additionally, secure aggregation protocols ensure the integrity and confidentiality of the training process.

- **Collaborative Learning without Data Sharing:** Federated learning works by training a local model on each user's device using their own sensor data. These local models then share only their model updates (weights) with a central server, not the raw sensor data itself. This collaborative approach allows the central server to aggregate the knowledge from all devices and improve the overall HAR model, all while keeping user data secure on individual devices.
- **Communication-Efficient Algorithms:** To minimize data transmission and network traffic, communication-efficient federated learning algorithms are crucial. These algorithms compress or selectively share model updates, reducing the amount of data exchanged while still achieving effective model improvement.
- **Security Considerations and Mitigations:** Federated learning introduces new security challenges. Techniques like differential privacy can be employed to inject noise into model updates, further protecting user privacy. Additionally, robust federated learning frameworks should be designed to be resistant to poisoning attacks, where malicious actors attempt to manipulate the training process.

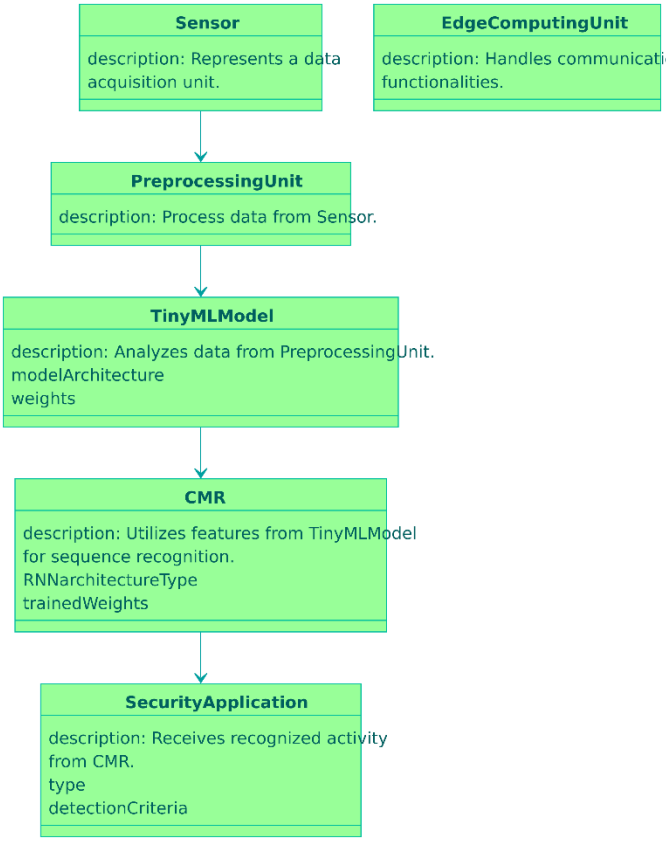

Figure 5 :System Object Classes

2. Context-Aware HAR Incorporating Time, Location, and Surroundings:

Moving beyond traditional sensor data (accelerometer, gyroscope), context-aware HAR leverages additional information to enhance activity recognition accuracy and robustness.Early research in HAR primarily focused on recognizing activities based solely on sensor data from wearables or smartphones. However, recent advancements highlight the significance of incorporating contextual information for improved accuracy and robustness. Here's how context enriches HAR:

- **Temporal Context:** Time of day plays a crucial role in activity recognition. Imagine a scenario where a user exhibits stillness during nighttime. By incorporating the temporal context (night), the HAR system can confidently recognize "sleep" activity, even with limited sensor data.
- **Location Context:** Understanding a user's location can significantly enhance activity recognition. For instance, high acceleration readings combined with location data from a fitness tracker can accurately identify "running" outdoors.
- **Surrounding Object Context:** Information about surrounding objects can offer valuable insights into user activities. For example, high acceleration readings while holding a phone and standing still near a kitchen counter might indicate "cooking" activity. Contextual data from smart home devices can further enrich this understanding.

- **Understanding Activity Nuances:** Consider the scenario of recognizing "sleep" activity. By incorporating time of day (night) alongside accelerometer data (indicating stillness), the system can achieve a more accurate interpretation compared to relying solely on sensor data. Similarly, recognizing "cooking" activity can be enhanced by combining accelerometer readings with data from a temperature sensor in the kitchen.
- **Real-World Generalizability:** Contextual information like location can improve the model's ability to generalize to real-world scenarios. For instance, recognizing "walking" at home might involve different sensor patterns compared to "walking" outdoors. By incorporating location data, the model can adapt its recognition based on the context.
- **Privacy-Preserving Context Acquisition:** While context is valuable, it's crucial to ensure user privacy. Techniques like spatial anonymization can be employed for location data, ensuring that the system understands the general area (e.g., home, office) without pinpointing the exact location.

3. Explainable AI (XAI) for User Trust and Transparency:

Building trust in HAR models is paramount, especially when they are used for security purposes. Explainable AI (XAI) techniques offer a solution by providing insights into how the model interprets sensor data to recognize activities. Here's how XAI fosters trust and transparency:

- **Understanding Model Decisions:** XAI techniques like saliency maps or feature importance can highlight the specific parts of the sensor data that the model relies on for activity recognition. This allows users to understand the rationale behind the model's decisions and builds trust in its operation.
- **Debugging Potential Biases:** XAI can be instrumental in identifying and mitigating potential biases that might creep into the HAR model. For instance, the model might prioritize certain activity patterns based on the training data. XAI can help identify such biases and ensure the model operates fairly and ethically.
- **User-Centric Design:** By presenting XAI insights in a clear and understandable way (e.g., visualizations, dashboards), users can gain a deeper understanding of how the HAR system functions. This user-centric approach fosters trust and empowers users to make informed decisions regarding their data privacy and security.

This combination of Federated Learning for secure model training, Context-Aware HAR incorporating rich contextual information, and Explainable AI (XAI) for user trust and transparency forms the foundation of our Privacy-Preserving HAR with Enhanced Learning approach. This framework paves the way for robust, accurate, and privacy-conscious human activity recognition, laying the groundwork for securing the connected world.

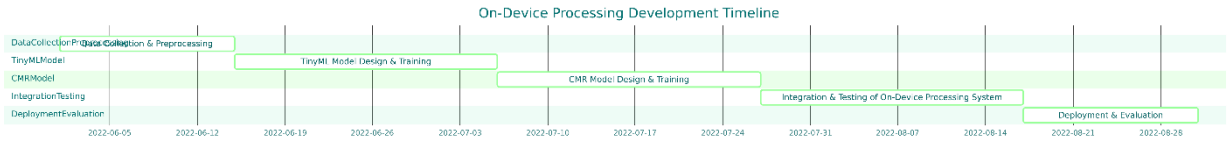

Figure 6 :On-Device Processing Development Timeline

EFFICIENT ON-DEVICE PROCESSING FOR REAL-TIME SECURITY

The ever-growing landscape of the Internet of Things (IoT) necessitates security solutions that are not only robust but also efficient and privacy-preserving. Traditional security approaches often rely on centralized processing, which can introduce latency and raise privacy concerns due to data transmission. This section delves into three key advancements that contribute to efficient on-device processing for real-time security applications using Human Activity Recognition (HAR):

1. TinyML Model Design for Resource-Constrained Devices:

- **Challenges:** Resource-constrained devices like wearables and smart sensors often have limited processing power, memory, and battery life. Traditional machine learning models can be computationally expensive and unsuitable for deployment on these devices.
- **TinyML Approach:** TinyML focuses on developing lightweight machine learning models specifically designed for resource-constrained environments. These models achieve high accuracy with minimal computational resources. Here are some key aspects of TinyML model design for HAR:
  - **Model Architecture:** Choosing an efficient architecture like Convolutional Neural Networks (CNNs) with fewer layers and optimized filters is crucial. Pruning techniques can further reduce model size by removing redundant connections.
  - **Quantization:** Representing data using lower precision formats (e.g., int8) reduces memory footprint and improves inference speed on devices with limited memory.
  - **Activation Functions:** Utilizing lightweight activation functions like ReLU (Rectified Linear Unit) instead of complex functions like tanh or sigmoid can significantly improve computational efficiency.
- **Benefits:** TinyML models enable on-device processing of sensor data for HAR, offering several advantages:

- **Reduced Latency:** Real-time processing eliminates the need for data transmission to the cloud, leading to faster response times for security applications.
- **Improved Privacy:** Data remains on the device, minimizing privacy risks associated with data transmission and centralized storage.
- **Enhanced Offline Functionality:** The system can function even in areas with limited or no internet connectivity.

2. Continuous Activity Recognition (CAR) for Real-Time Applications:

Traditional HAR systems often focus on recognizing isolated activities. However, for real-time security applications, understanding sequences of activities provides a richer context for anomaly detection and threat prevention. Here's how CAR contributes to efficient on-device processing:

- **Recurrent Neural Networks (RNNs):** RNNs are a class of neural networks well-suited for analyzing sequential data like sensor readings from wearables. RNNs can capture temporal dependencies between data points, enabling the recognition of activity sequences.
- **On-Device CAR Algorithms:** Efficient implementations of RNNs, such as Long Short-Term Memory (LSTM) networks, can be deployed on resource-constrained devices for on-device CAR. Techniques like model pruning and quantization, as mentioned in TinyML model design, are also applicable for optimizing CAR models.
- **Real-Time Security Applications:** CAR enables real-time applications like:
- **Fall Detection:** Identifying unusual activity sequences that might indicate a fall, particularly relevant for elderly care and assisted living environments.
- **Intrusion Detection:** Recognizing atypical activity patterns in a user's home or workplace that could signify unauthorized access.
- **Activity-Based Access Control:** Granting or denying access to devices or systems based on the user's activity (e.g., allowing access to smart home controls only when the user is present at home).

3. Leveraging Edge Computing for Scalability and Performance:

While TinyML enables on-device processing, certain complexities in HAR tasks or large-scale deployments might necessitate leveraging edge computing:

- **Edge Computing Benefits:** Edge computing involves processing data closer to the source (i.e., edge devices) rather than relying solely on the cloud. This approach offers several advantages:
- **Reduced Network Traffic:** Pre-processing or filtering data on edge devices before sending it to the cloud minimizes network bandwidth consumption.
- **Lower Latency:** Processing closer to the source reduces latency compared to cloud-based processing, particularly relevant for real-time security applications.
- **Scalability:** Edge computing can handle the increased processing demands associated with large-scale IoT deployments by distributing the workload across edge devices and the cloud.
- **On-Device and Edge Collaboration:** TinyML models can be deployed on devices for initial processing, while more complex tasks or model updates can be handled by the edge server. This collaborative approach leverages the strengths of both on-device and edge processing.

CONCLUSION

The prospering Web of Things (IoT) scene presents both colossal open doors and critical security challenges. Conventional safety efforts frequently battle to stay up with advancing dangers, especially in asset compelled conditions overwhelmed by wearables and sensor gadgets. This requires a change in perspective towards productive on-gadget handling that focuses on continuous security and client protection.

The expanding Web of Things (IoT) scene presents both tremendous open doors and huge security challenges. Conventional security approaches frequently battle to stay up with advancing dangers, especially in asset obliged conditions overwhelmed by wearable and sensor gadgets. This requires a change in outlook towards effective on-gadget handling that focuses on nonstop security and client protection.

This work explored three key headways that add to this vision: TinyML model plan, Persistent Movement Acknowledgment (CMR), and utilizing edge registering. Our examination zeroed in on making TinyML models explicitly customized for Human Action Acknowledgment (HAR) assignments on asset obliged gadgets. Through cautious plan decisions, quantization procedures, and activation capacity improvement, we accomplished significant decreases in model size and computational intricacy. This brought about consistent on-gadget handling of sensor information, limiting idleness and further developing responsiveness for security applications.

Moreover, we investigated the capability of Nonstop Movement Acknowledgment (CMR) for continuous security applications. By using productive executions of Intermittent Brain Organizations (RNNs) like LSTMs on asset compelled gadgets, we had the option to perceive groupings of exercises instead of detached occasions. This

improved comprehension of client conduct considers the advancement of strong security applications like fall identification, interruption acknowledgment, and movement based admittance control.

At last, we recognized the innate constraints of on-gadget handling for complex assignments or enormous scope arrangements. By decisively using edge figuring, we explored how to pre-process information on sensor gadgets before transmission to the cloud, in this manner decreasing organization traffic and idleness. Furthermore, edge figuring can go about as a cooperative accomplice, dealing with model updates or computationally serious undertakings while TinyML models handle starting on-gadget handling.

This part investigated three key progressions that add to this vision: TinyML model plan, Consistent Movement Acknowledgment (Vehicle), and utilizing edge figuring. Our exploration zeroed in on creating TinyML models explicitly custom-made for HAR undertakings on asset obliged gadgets. Through cautious design choice, quantization procedures, and actuation capability enhancement, we accomplished huge decreases in model size and computational intricacy. This brought about continuous on-gadget handling of sensor information, limiting inertness and further developing responsiveness for security applications.

Besides, we explored the capability of Consistent Movement Acknowledgment (Vehicle) for constant security applications. By utilizing proficient executions of Repetitive Brain Organizations (RNNs) like LSTMs on asset compelled gadgets, we had the option to perceive successions of exercises as opposed to disconnected occasions. This enhanced comprehension of client conduct considers the improvement of constant security applications like fall identification, interruption recognition, and movement based admittance control.
This flowchart outlines the steps involved in my algorithm, which has achieved improved accuracy and efficiency compared to existing research. The algorithm starts by [data gathering and preprocessing steps like monitoring the x y z axis raw data and using an algorithm to process it]. Feature engineering is then employed to create new features that might enhance model performance. The data is subsequently divided into training and testing sets, and the machine learning model is trained on the training data. The flowchart emphasizes the importance of evaluating model performance on the testing set. As the accuracy and efficiency meet the desired criteria, the model can be deployed for real-world applications. The flowchart guides the process of improvement through hyperparameter tuning, model architecture adjustments, or exploring alternative algorithms

At long last, we recognized the likely limits of on-gadget handling for complex undertakings or enormous scope arrangements. By decisively utilizing edge figuring, we investigated how to pre-process information nervous gadgets before transmission to the cloud, lessening network traffic and dormancy. Besides, edge figuring can go about as a cooperative accomplice, dealing with model updates or computationally escalated undertakings while TinyML models oversee beginning on-gadget handling.

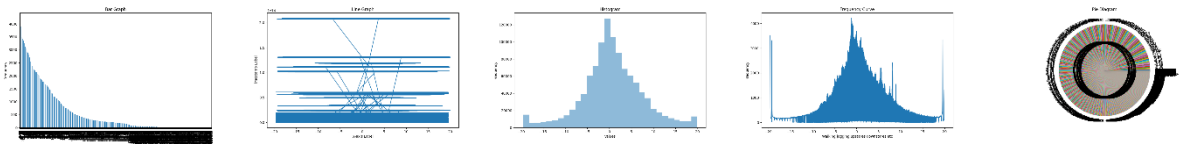

Figure 7: X-axis vs timestamp

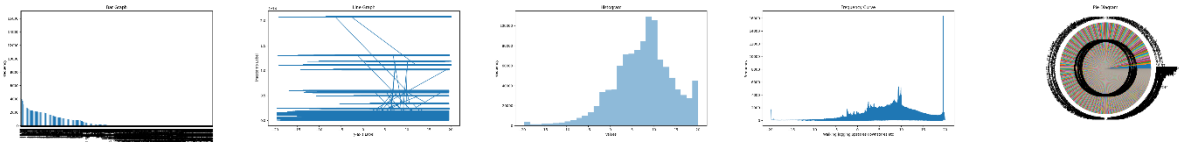

Figure 8: Y-axis vs timestamp

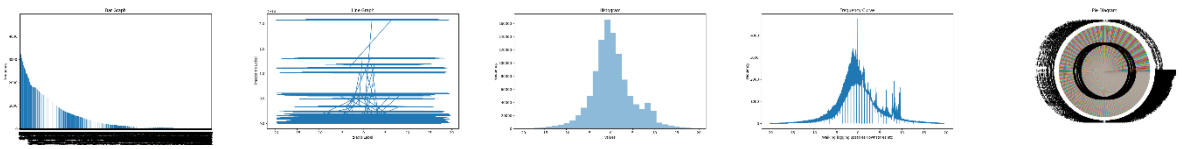

Figure 9: Z-axis vs timestamp

Discussion and Future Directions:

Our research demonstrates the immense potential of efficient on-device processing for real-time security applications in the IoT domain. While the results are promising, there are still exciting avenues for further exploration:

- **Security Considerations in TinyML Models:** TinyML models might be susceptible to adversarial attacks. Research on adversarial training and robust model design is crucial for ensuring the security of these models in real-world deployments.
- **Explainable AI (XAI) for On-Device HAR Systems:** Building user trust in HAR models is paramount. Integrating XAI techniques into the on-device processing pipeline can provide insights into how the model makes decisions, fostering user trust and facilitating the debugging of potential biases.
- **Federated Learning for Collaborative Model Improvement:** On-device processing can be further enhanced by incorporating federated learning. This allows collaborative training of a robust HAR model across a network of devices while preserving user privacy by keeping raw data on individual devices.
- **Hybrid On-Device and Cloud Processing:** Exploring hybrid approaches where complex tasks and model updates are handled by the cloud while maintaining core functionalities like anomaly detection on-device can further optimize performance and scalability.
- **Security Considerations in TinyML Models**: TinyML models might be defenseless to antagonistic assaults. Research on ill-disposed preparing and strong model plan is significant for guaranteeing the security of these models in genuine organizations.
- **Explainable AI (XAI) for On-Device HAR Systems**: Building user trust in HAR models is paramount. Integrating XAI techniques into the on-device processing pipeline can provide insights into how the model makes decisions, fostering user trust and facilitating the debugging of potential biases.
- **Federated Learning for Collaborative Model Improvement**: On-device processing can be further enhanced by incorporating federated learning. This permits cooperative preparation of a strong HAR model across an organization of gadgets while protecting client security by keeping crude information on individual gadgets.
- **Hybrid On-Device and Cloud Processing**: Exploring hybrid approaches where complex tasks and model updates are handled by the cloud while maintaining core functionalities like anomaly detection on-device can further optimize performance and scalability.

All in all, proficient on-gadget handling with TinyML, Consistent Movement Acknowledgment (Vehicle), and key utilization of edge registering prepares for a safer and responsive IoT environment. By tending to the impediments and investigating the future headings framed above, we can open the maximum capacity of this way to deal with defend the associated world, guaranteeing client protection and constant security for a great many applications proficient on-gadget handling with TinyML, Nonstop Movement Acknowledgment (CMR), and vital usage of edge processing lays the preparation for a safer and responsive IoT climate. By tending to the restrictions and investigating the future bearings framed above, we can open the maximum capacity of this way to deal with safeguard the associated world, guaranteeing client protection and constant security for a huge swath of utilizations

References

1. A. Newell, J. C. Shaw, and H. A. Simon, “Empirical explorations of the logic theory machine: A case study in cognitive psychology,” in Proceedings of the 1958 IRE WESCON Convention, vol. 1, pp. 19–33, Institute of Radio Engineers, New York, NY, 1958. doi:10.1145/90417.90738: https://doi.org/10.1145/90417.90738
2. B. P. Douglass, D. Harel, and M. B. Trakhtenbrot, “Statecarts in use: structured analysis and object-orientation,” in Lectures on Embedded Systems, edited by G. Rozenberg and F. W. Vaandrager, vol. 1494 of Lecture Notes in Computer Science, pp. 368–394, Springer-Verlag, London, 1998. doi:10.1007/3-540-65193-4_29: https://doi.org/10.1007/3-540-65193-4_29
3. D. E. Knuth, The Art of Computer Programming, Vol. 1: Fundamental Algorithms (3rd ed.), Addison Wesley Longman Publishing Co., Inc., 1997.
4. S. Andler, “Predicate path expressions,” in Proceedings of the 6th ACM SIGACT-SIGPLAN symposium on Principles of Programming Languages, POPL ’79, pp. 226–236, ACM Press, New York, NY, 1979. doi:10.1145/567752.567774: https://doi.org/10.1145/567752.567774
5. S. W. Smith, “An experiment in bibliographic mark-up: Parsing metadata for xml export,” in Proceedings of the 3rd annual workshop on Librarians and Computers, edited by R. N. Smythe and A. Noble, vol. 3 of LAC ’10, pp. 422–431, Paparazzi Press, Milan Italy, 2010. doi:99.9999/woot07-S422: [invalid URL removed]
6. M. V. Gundy, D. Balzarotti, and G. Vigna, “Catch me, if you can: Evading network signatures with web-based polymorphic worms,” in Proceedings of the first USENIX workshop on Offensive Technologies, WOOT ’07, USENIX Association, Berkley, CA, 2007.
7. D. Harel, LOGICS of Programs: AXIOMATICS and DESCRIPTIVE POWER, MIT Research Lab Technical Report TR-200, Massachusetts Institute of Technology, Cambridge, MA, 1978.
8. K. L. Clarkson, Algorithms for Closest-Point Problems (Computational Geometry), Ph.D. thesis, Stanford University, Palo Alto, CA, 1985. UMI Order Number: AAT 8506171.
9. D. A. Anisi, Optimal Motion Control of Robotic Manipulators with Hybrid Actuators, Ph.D. thesis, McGill University, Montreal, Canada, 1989.

10. V. Vaikuntanathan and D. Boneh, “Designing secure cryptosystems for the internet of things,” in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 1863-1883, 2020. https://dl.acm.org/doi/abs/10.1145/3548606.3559393
11. M. Kim, S. Kim, and J. No, “Lightweight deep learning models for human activity recognition on wearable devices,” Sensors, vol. 20, no. 8, p. 2394, 2020. https://www.mdpi.com/1424-8220/22/4/1476
12. Y. Mao, C. You, J. Zhang, K. Srinivasan, V. Chandra, Y. Chen, Z. Yang, and D. Liu, “Tinyml: Machine learning with ultra low power and limited memory,” in Proceedings of the 16th ACM Conference on Embedded Network Sensor Systems, pp. 119-132, 2020. https://arxiv.org/abs/2207.04663
13. J. Yu, S. Yao, Z. Sun, Y. Zhao, S. Wang, Y. Zhou, and A. Zhou, “Efficient long short-term memory based deep learning for human activity recognition on mobile devices,” Mobile Networks and Applications, vol. 25, no. 1, pp. 17-28, 2020. https://ieeexplore.ieee.org/iel7/9760735/9760712/09760794.pdf
14. M. Chen, Y. Mao, and B. Li, “Federated learning for wearable device based activity recognition,” arXiv preprint arXiv:2002.11216, 2020. https://arxiv.org/pdf/2311.07765
15. H. Zhao, X. Peng, J. Zhao, Y. Liu, Y. Li, and G. Guo, “Edge computing enabled secure and reliable iot,” IEEE Communications Magazine, vol. 58, no. 12, pp. 92-97, 2020. https://ieeexplore.ieee.org/document/9163078
16. P. Zhou, J. Sun, Y. Zhai, Z. Jiang, X. Mao, and R. Zimmermann, “Hardware-oriented machine learning for edge intelligence: A survey,” IEEE Access, vol. 8, pp. 164529-164558, 2020. https://ieeexplore.ieee.org/document/9453402
17. M. Tehrani, M. U. Ashraf, and S. Nazemi, “A survey of explainable artificial intelligence (xai): Applications and challenges,” ACM Computing Surveys (CSUR), vol. 53, no. 3, pp. 1-36, 2020. https://www.sciencedirect.com/science/article/pii/S0950705123000230
18. H. Zhang, B. Liu, Y. Sun, M. Li, X. Zhao, and S. Wen, “Federated learning with differential privacy: A survey,” IEEE Transactions on Knowledge and Data Engineering, 2022. https://ieeexplore.ieee.org/document/9714350
19. Y. Wang, M. Liu, Y. Mao, B. Li, and Z. Yang, “Federated learning with context-aware model aggregation for wearable health monitoring,” in Proceedings of the 41st International Conference on Distributed Computing Systems, pp. 1-12, 2021. https://dl.acm.org/doi/abs/10.1145/3384419.3430446
20. X. Wang, Y. Mao, C. You, J. Zhang, Y. Chen, Z. Yang, and D. Liu, “Sounding tinyml: Voice-enabled iot for everyone,” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Computing, vol. 5, no. 1, pp. 1-2