ALBA: Novel Anomaly Location-Based Authentication in IoMT Environment Using Unsupervised ML

Presenter: Fawaz J. Alruwaili

Fawaz J. Alruwaili[1], S. P. Mohanty[2], E. Kougianos[3]

University of North Texas, Denton, TX, USA.[1,2,3].

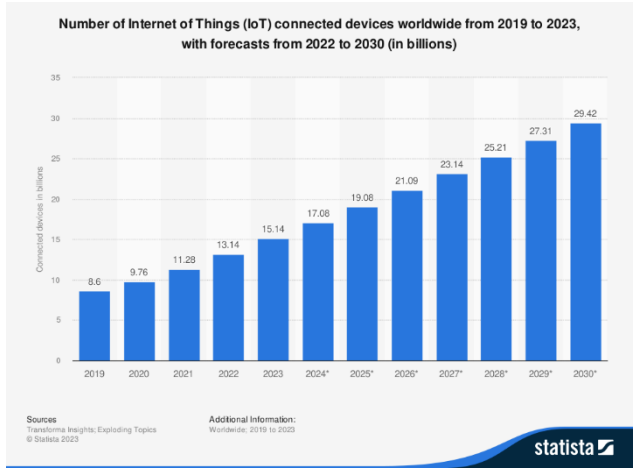
Email: **fawazalruwaili@unt.edu[1], saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3]**

Outline

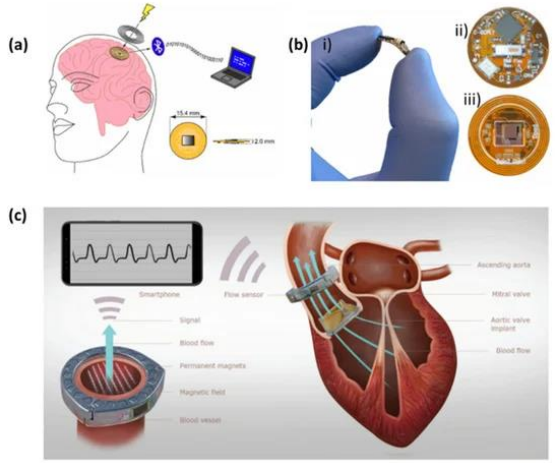
- Significance of Internet of Medical Things (IoMT)
- Smartphones Role in IoMT
- IoMT Security
- AI-Enhanced Cybersecurity
- Related Works on Behavioral Authentication
- Proposed Novel Solution (ALBA) & Novelty
- Implementation
- Experimental Results
- Conclusions & Future Work

Significance of Internet of Medical Things (IoMT)

- The growth of IoT embedded systems and biosensors introduced the IoMT.
- IoMT integrates medical devices, applications, and networks to enhance the efficiency of healthcare system.



(a) IoT device growth

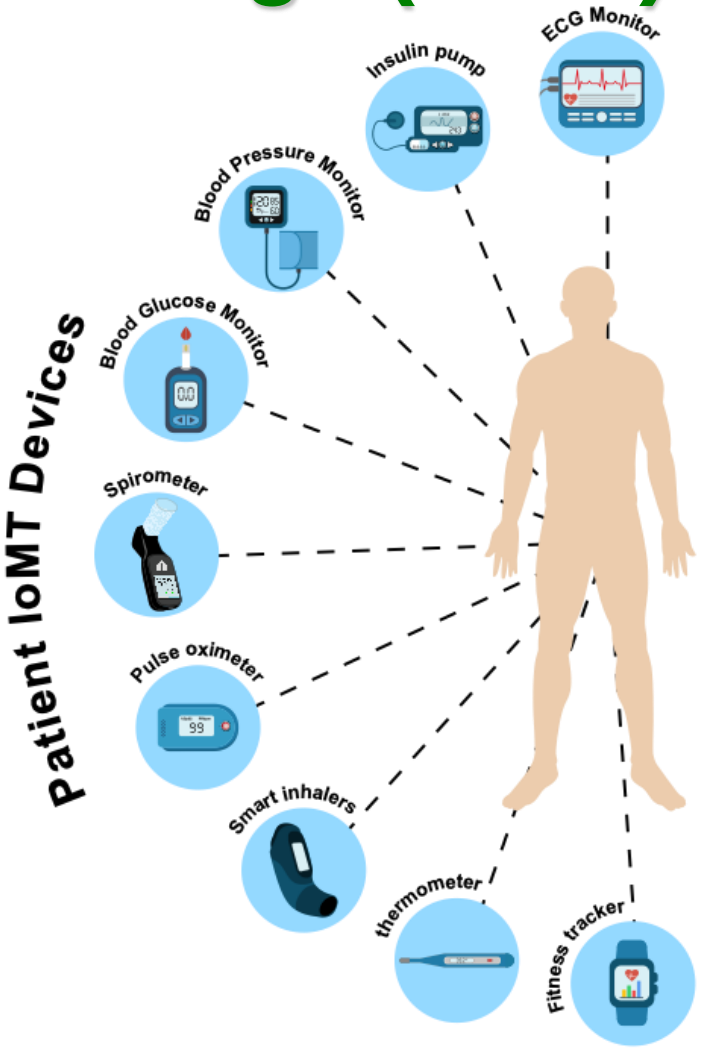


(b) implantable biosensors

(b) Image Source: https://www.mdpi.com/2079-6374/10/7/79

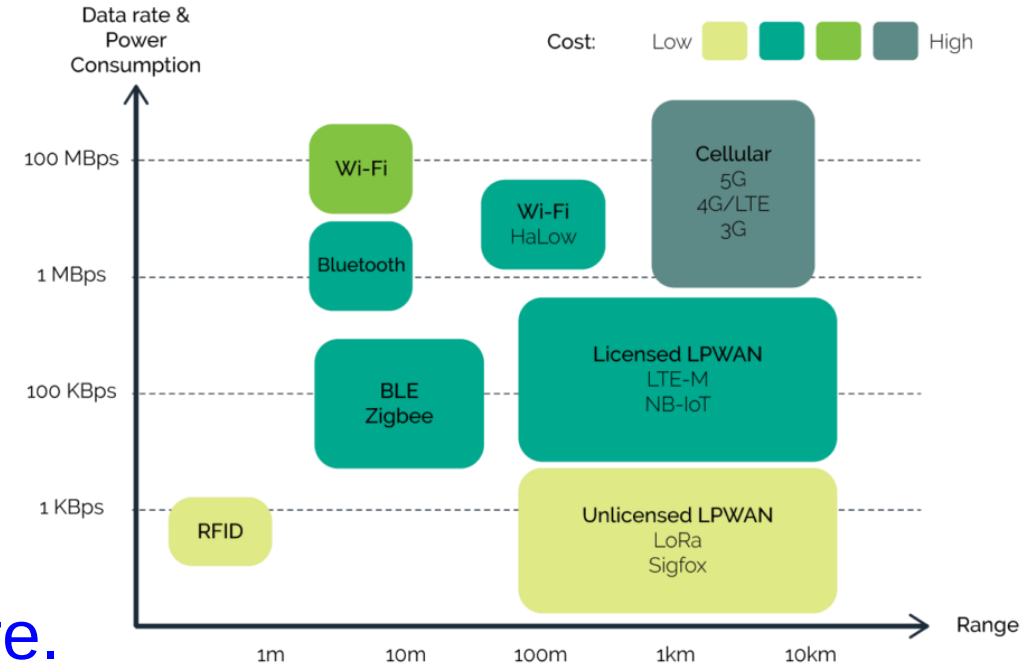
Significance of Internet of Medical Things (IoMT)

- **Enhancing Healthcare Efficiency**.
  - Real-time monitoring.
  - Improved patient outcomes.
  - Significant cost savings for healthcare systems.
  - Remote Patient Monitoring.
  - Enhanced Data Collection.
  - Improved Emergency Response



Significance of Internet of Medical Things (IoMT)

- **Limitations of IoMT devices.**
  - Limited Processing Power.
  - Limited Storage.
  - Battery Life.
  - Connectivity Issues.
  - User Interface Limitations (multiple).
  - Complexity of software and hardware.



The data rate & power consumption of IoT device connections compared to connection range.

EMBEDDED AMS

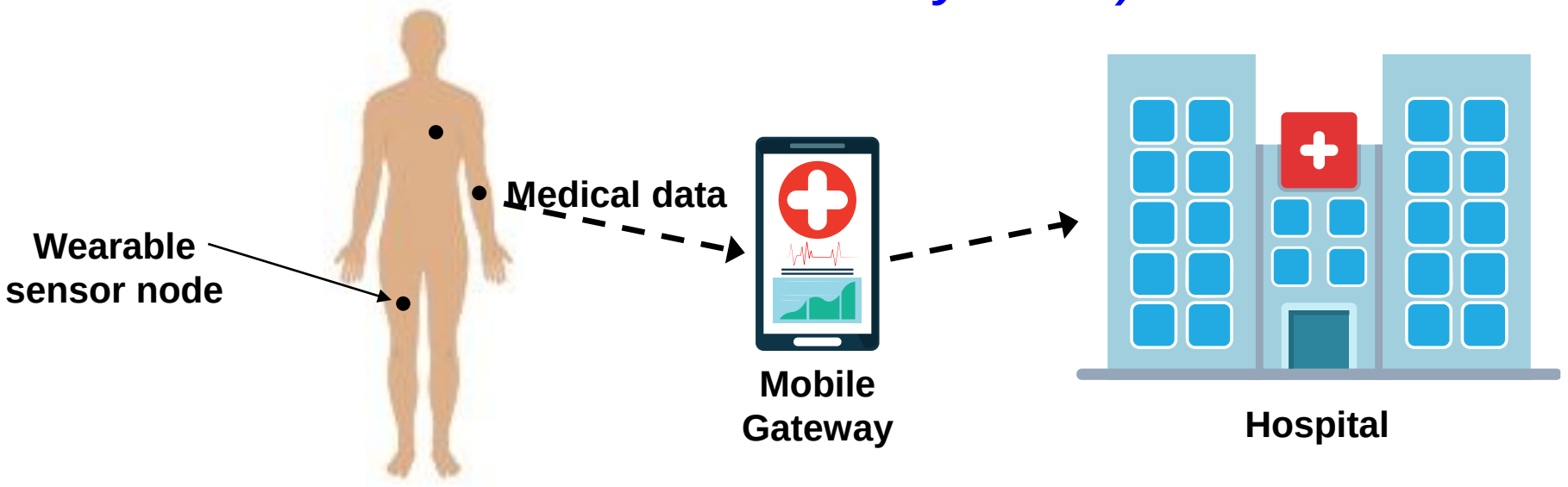
Image source: https://embeddedams.nl/different-ways-to-connect-iot-devices-to-transmit-and-receive-data/

The Role of Smartphones in IoMT

- Advancements in mobile technolog enable smartphones to become a main component of IoMT Network.
  - Ubiquity of Smartphones.
  - Computational capabilities.
  - Storage Capacity.
  - Adaptable Connectivity.
  - Comprehensive User Interface.

IoMT security

- Smartphones also introduce new security challenges due to the sensitive nature of medical data collected/processed/transmitted by smartphones.
- Multi-point Connectivity (a compromised smartphone can compromise the entire connected system)



AI-Enhanced Cybersecurity

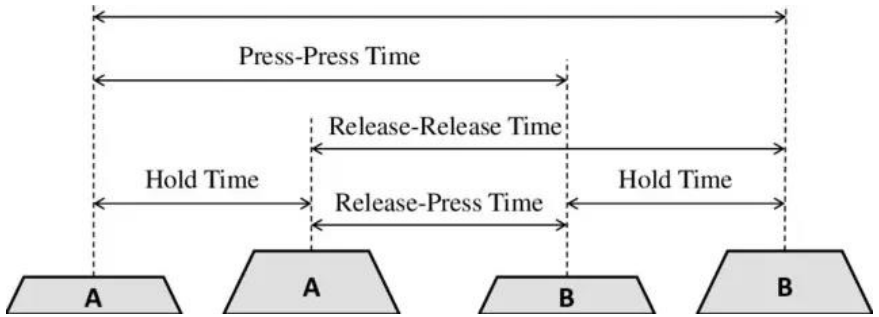
- **AI plays an important role in the security.**
  - **Enhanced Threat Detection**:
    - **Real-Time Monitoring**: large amounts of data can be analyzed in real-time.
    - **Predictive Analytics**: predicting future attacks based on historical data allowing for preventive measures.
  - **Efficient Response**:
    - **Automated Responses**: recognizing threats automatically.
    - **Prioritization**: allowing cybersecurity teams to focus on the most critical issues.
  - **Efficient Response**: AI algorithms can be improved over time by learning from new data.

AI-Enhanced Cybersecurity

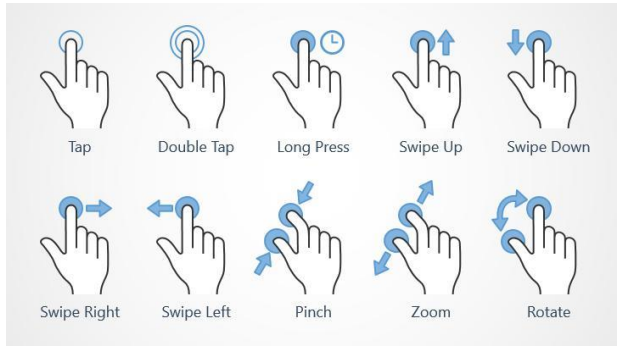
- **Data quality is crucial in machine learning (ML) for obtaining accurate results.**

Related Research on Behavioral Authentication

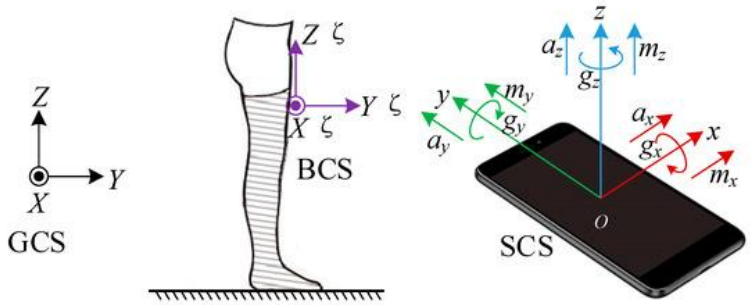
- **Existing research on behavioral authentication has provided valuable insights using various techniques and sensors, such as Keystroke Dynamics (KD), Touch Gestures (TG) [8, 9], and Gait Behavior.**



(a) Keystroke Dynamic Behavior



(b) Touch Gestures Behavior



(c) Gait Behavior

(a) Image Source: https://www.researchgate.net/publication/324536760_The_Wolf_of_SUTD_TWOS_A_dataset_of_malicious_insider_threat_behavior_based_on_a_gamified_competition

(c) Image Source: https://www.researchgate.net/publication/336688085_Smartphone-Based_3D_Indoor_Pedestrian_Positioning_through_Multi-Modal_Data_Fusion

Related Research on Behavioral Authentication

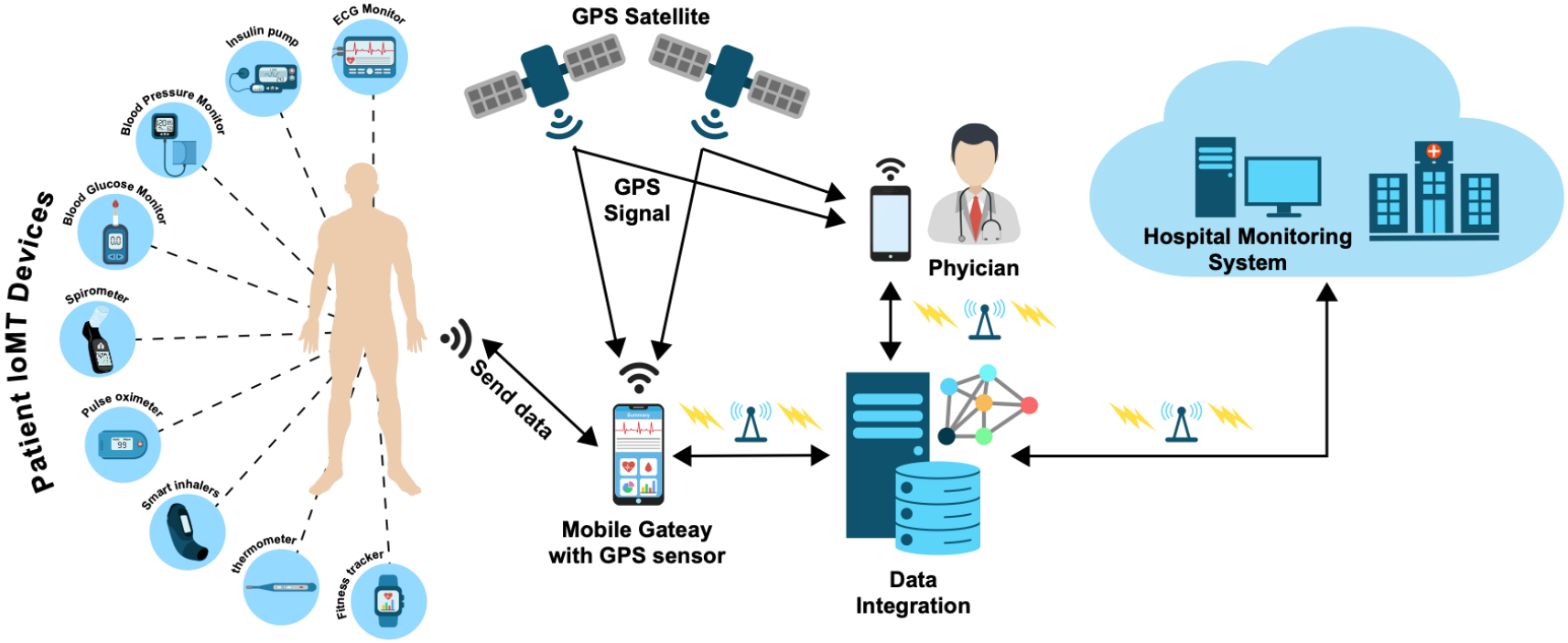
- **However, expectations in terms of (accuracy and stability) of authentication data are not met, nor considered the holistic security needs (environment, device, and user conditions).**

- **Limitations of related work:**
  - **Variety of devices:** No specific hardware - different shapes, layouts, and sizes.
  - **specific language: a**ffects the interval time between touches.
  - **Other factors:** environment, clothing, sickness, injuries, fatigue, emotional or mental status, and smartphone position.

Image soruce: https://en.zinggadget.com/there-is-now-more-smartphones-than-people-on-earth/

Proposed Solution (ALBA)

- **ALBA exploits GPS technology in smartphones to authenticate users based on the behavior of their locations utilizing ML technology for analyzing and detecting anomalous locations.**



Overview of the Proposed ALBA for IoMT.

Novelty of the Proposed Solution (ALBA)

- **ALBA method provides several contributions:**
  - **Less sensitive to internal/external factors.**
  - **Countering for GPS inaccuracies (model parameters)**
  - **Increasing efficiency:**
    - **GPS requires less features**
    - **Lightweight iForest algorithm that has low memory requirements, reducing computational demand and power consumption compared to existing behavioral methods.**

Novelty of the Proposed Solution (ALBA)

- **Scalability and applicability with GPS integration in various IoMT devices without specific hardware requirements.**
- **Enhancing user convenience as our method can be additional security layer along with existing authentication factors, reducing their constraints..**

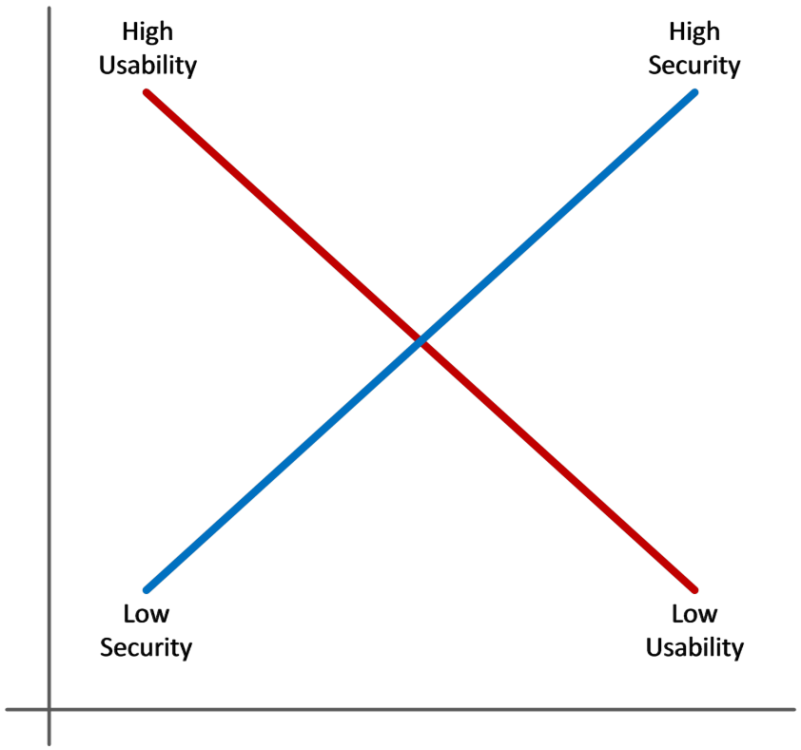
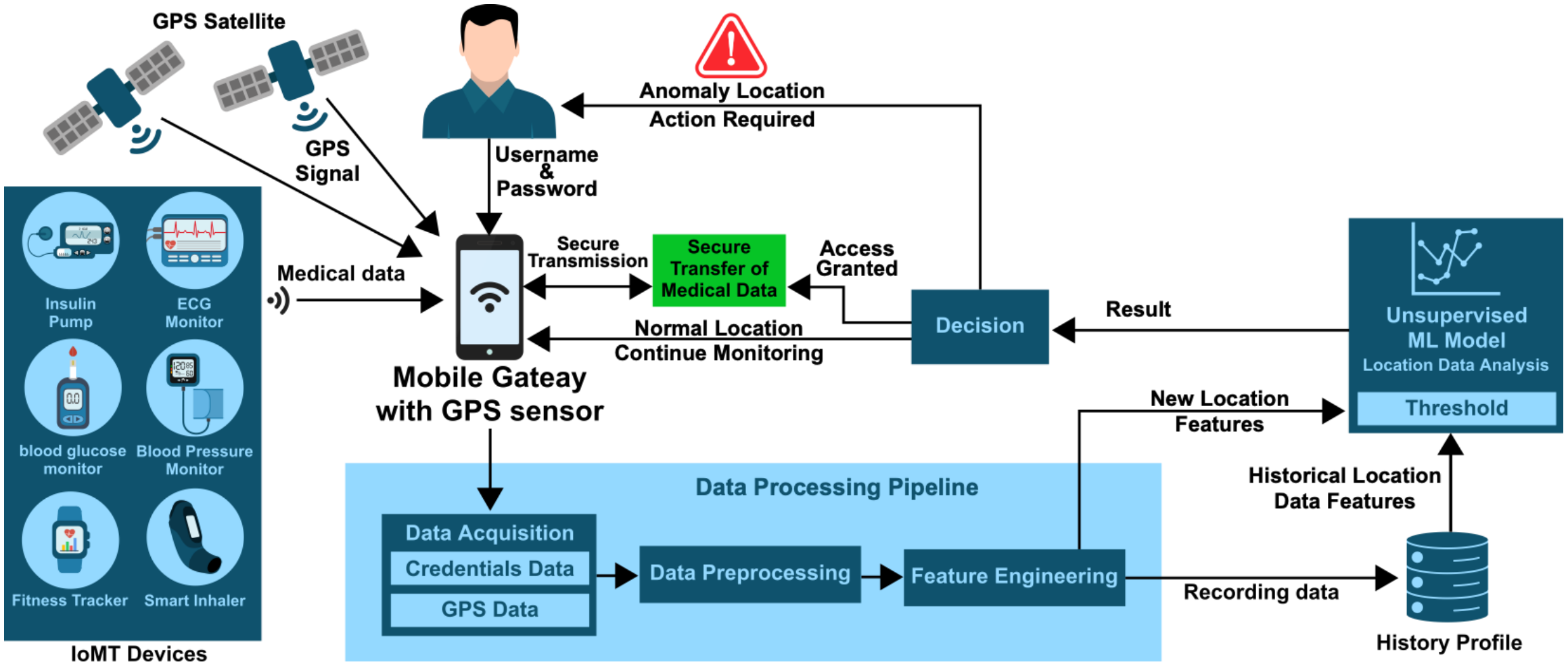


Figure 1: Security and usability tend to be inversely related

Image Source: https://www.rlvision.com/blog/authentication-with-passwords-passphrases-implications-on-usability-and-security/

ALBA Method Workflow for IoMT

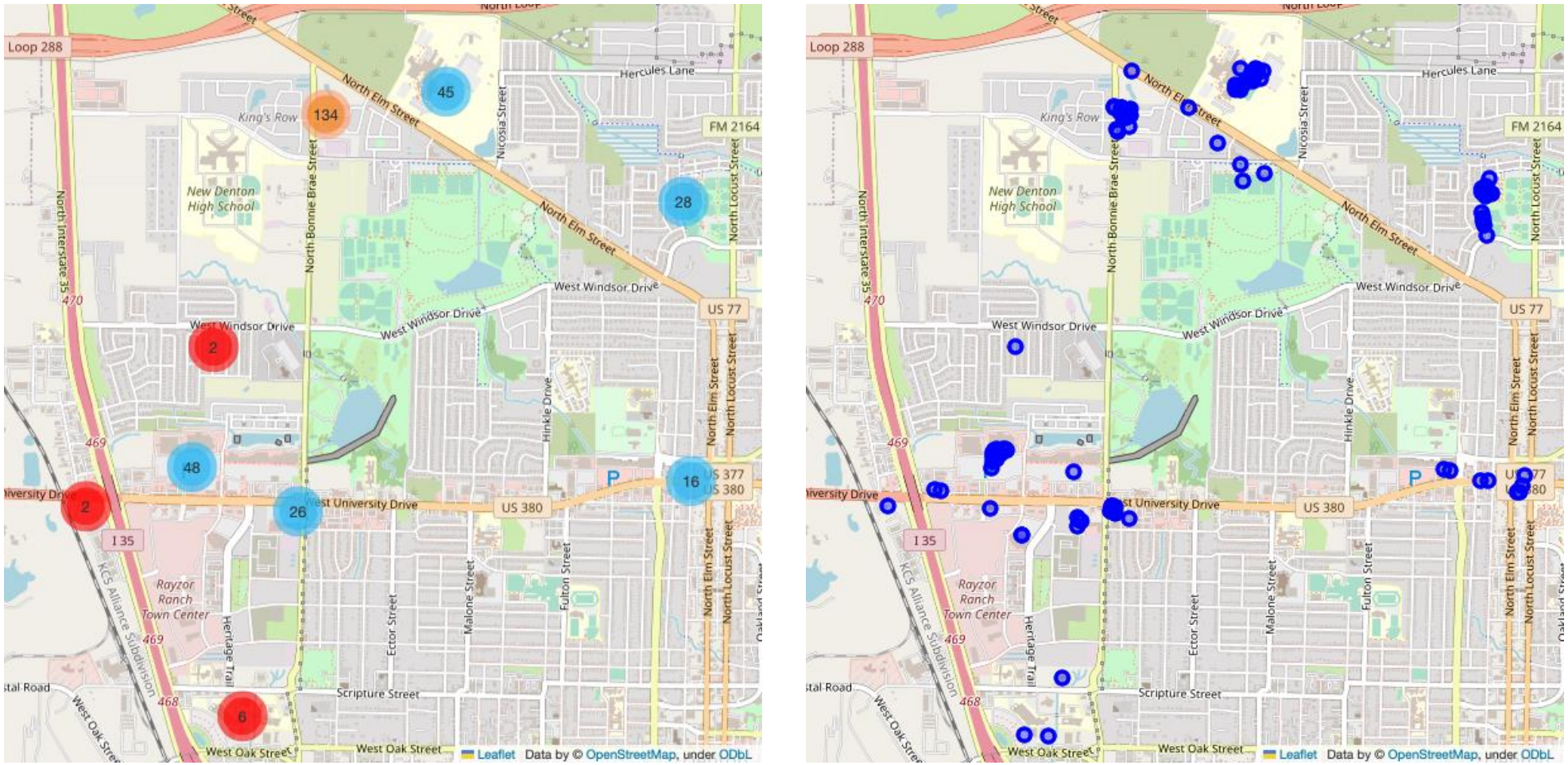


Overview of the Proposed ALBA for IoMT.

Datasets Description

Dataset	Details	Purpose
Real-world	• 359 observations • Irregular intervals over 27 days • Collected using iPhone 11 Pro	Evaluate ALBA under real-world scenarios.
Public (Kaggle)	• 40,603 observations • Collected in October 2014 • Using an Android device	Evaluate ALBA on different real-world data and scenarios.
Virtual (Python)	• 3,359 observations • 5 known anomalous locations • Different regular patterns and changes • Generated using Python	Evaluation under specific realistic scenarios not clearly present in the previous datasets.

Datasets Description

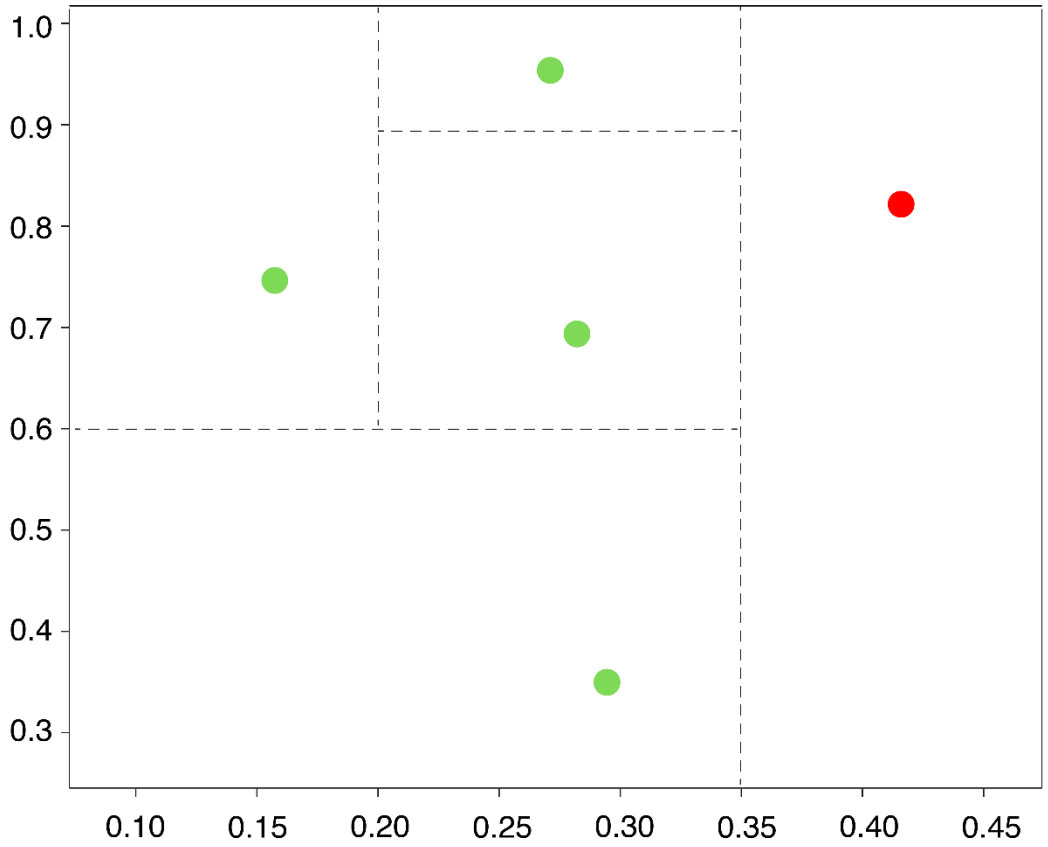


Sample of collected locations - Real-world Dataset

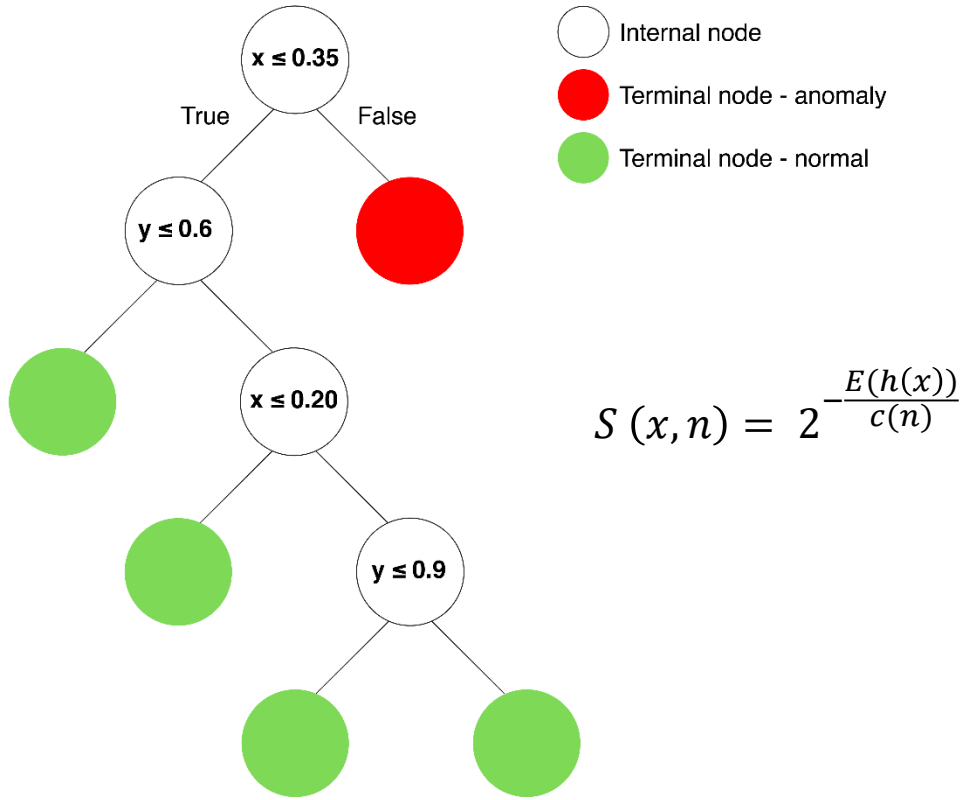
Lightweight Isolation Forest Algorithm (iForest)

- Unsupervised no pre-labeled data required.
- Low memory requirements utilizes decision trees (limited depth or fewer levels).
- Fast computation average time for each data point remains constant, leading to a linear $O(n)$ time complexity.
- Reducible model sensitivity minor data variations can be adjusted.
- Adaptable to data distribution changes.

Lightweight Isolation Forest Algorithm (iForest)



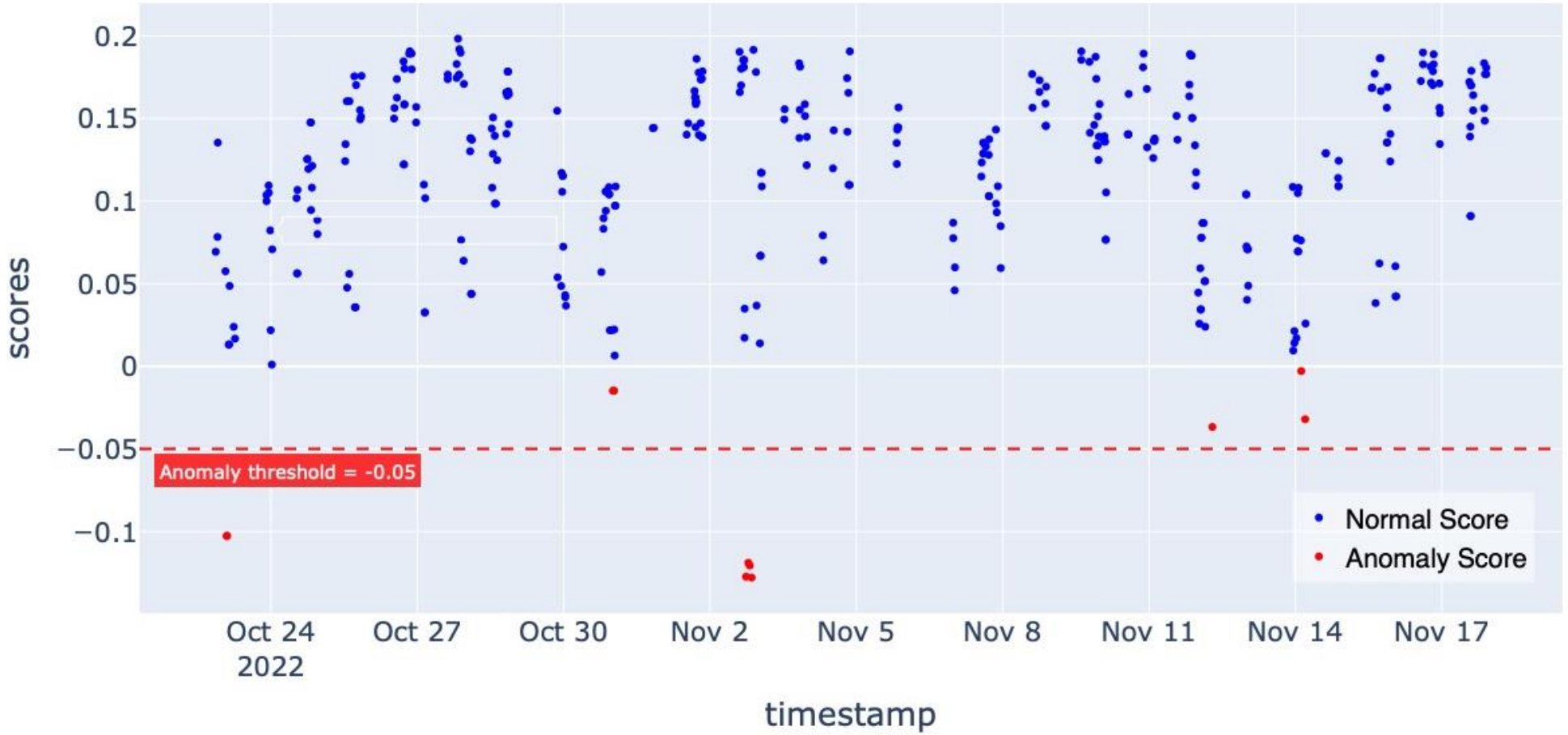
Data Distribution



$$S\,(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$$

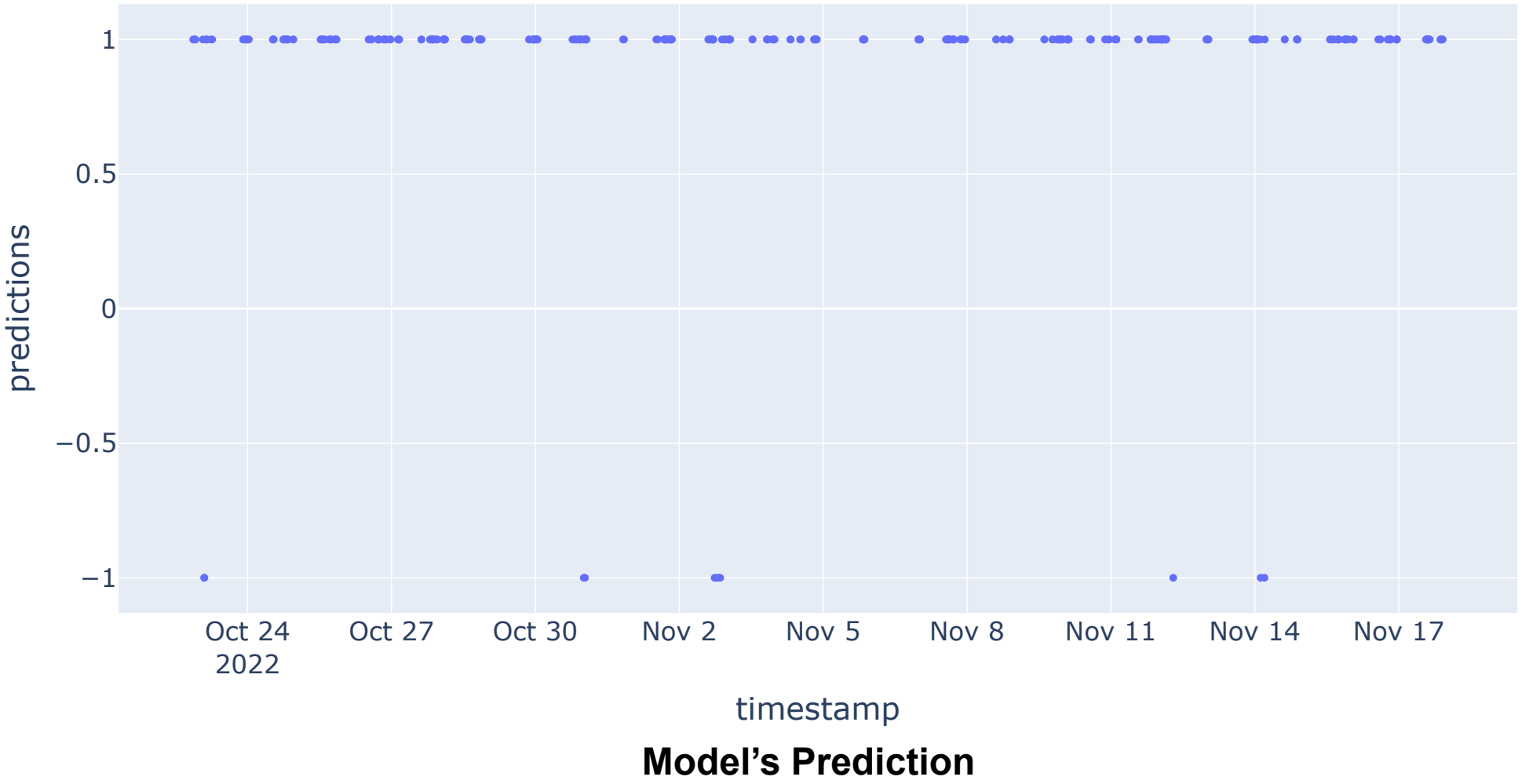
Decision Tree

Experimental Results (Real-world Dataset)

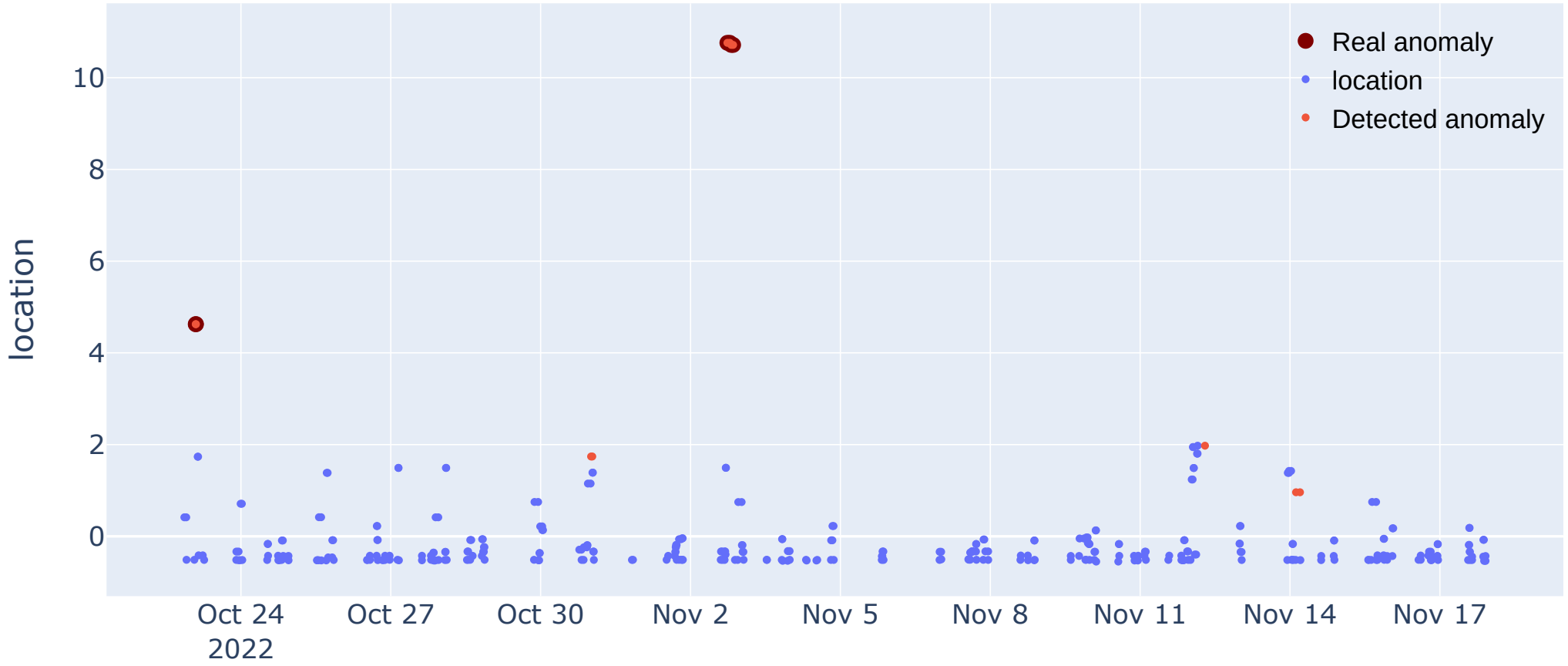


Anomaly Scores

Experimental Results (Real-world Dataset)

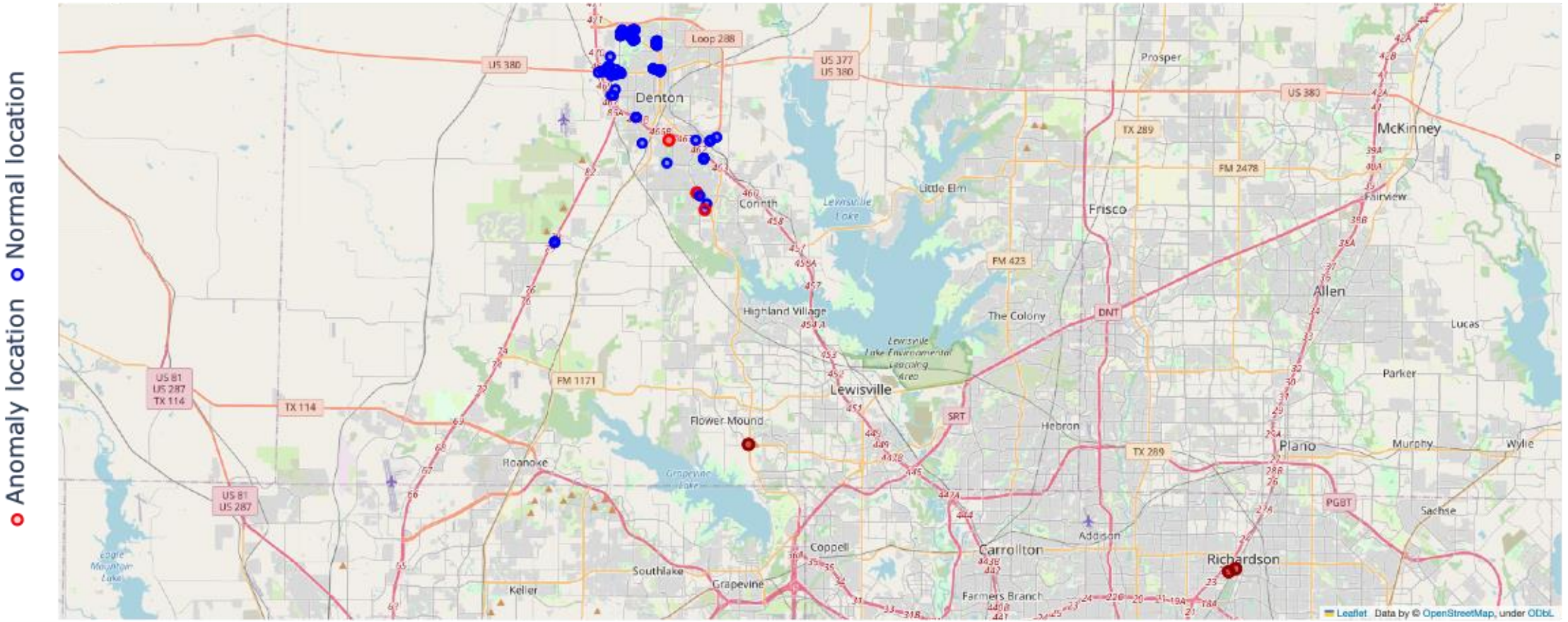


Experimental Results (Real-world Dataset)



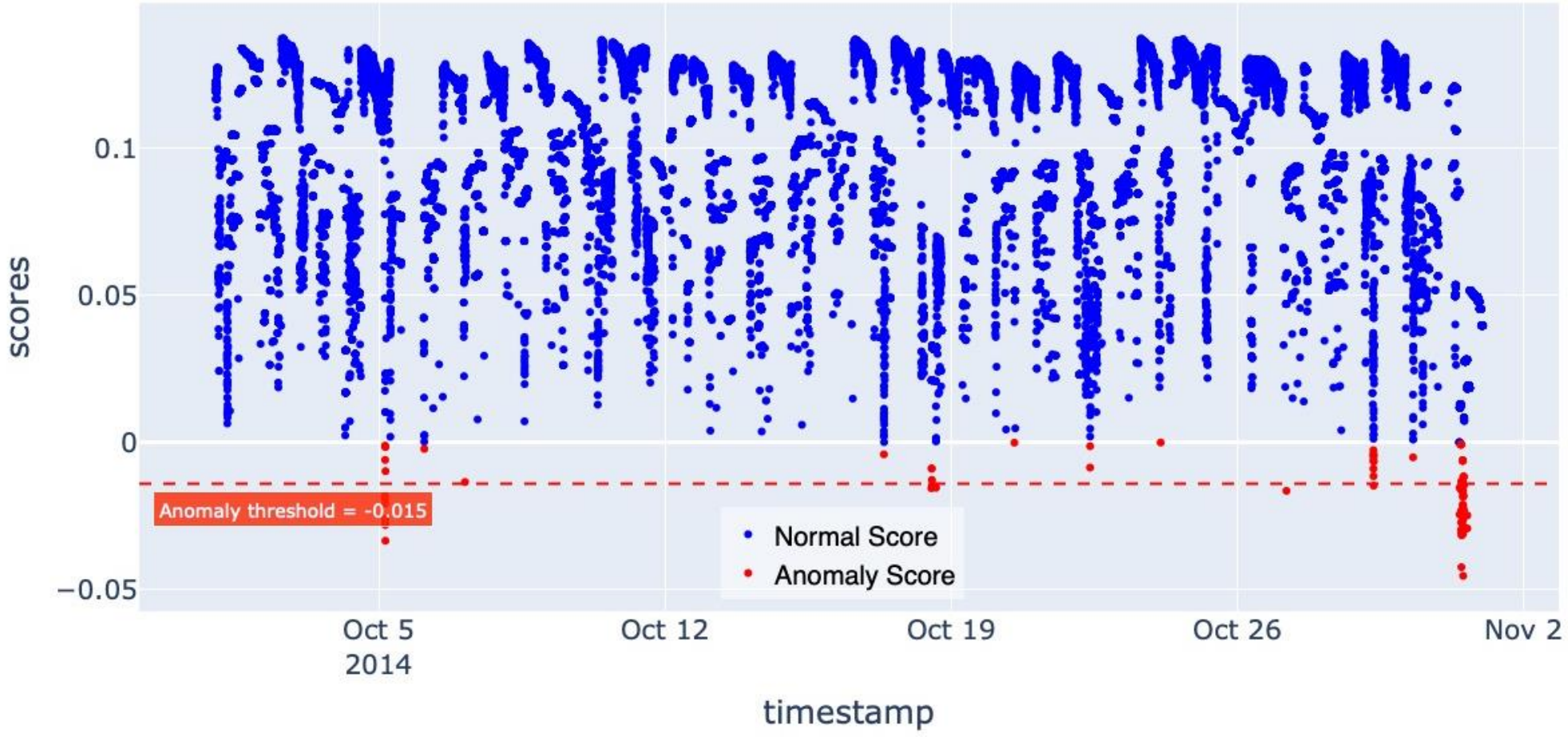
Anomalous Locations

Experimental Results (Real-world Dataset)



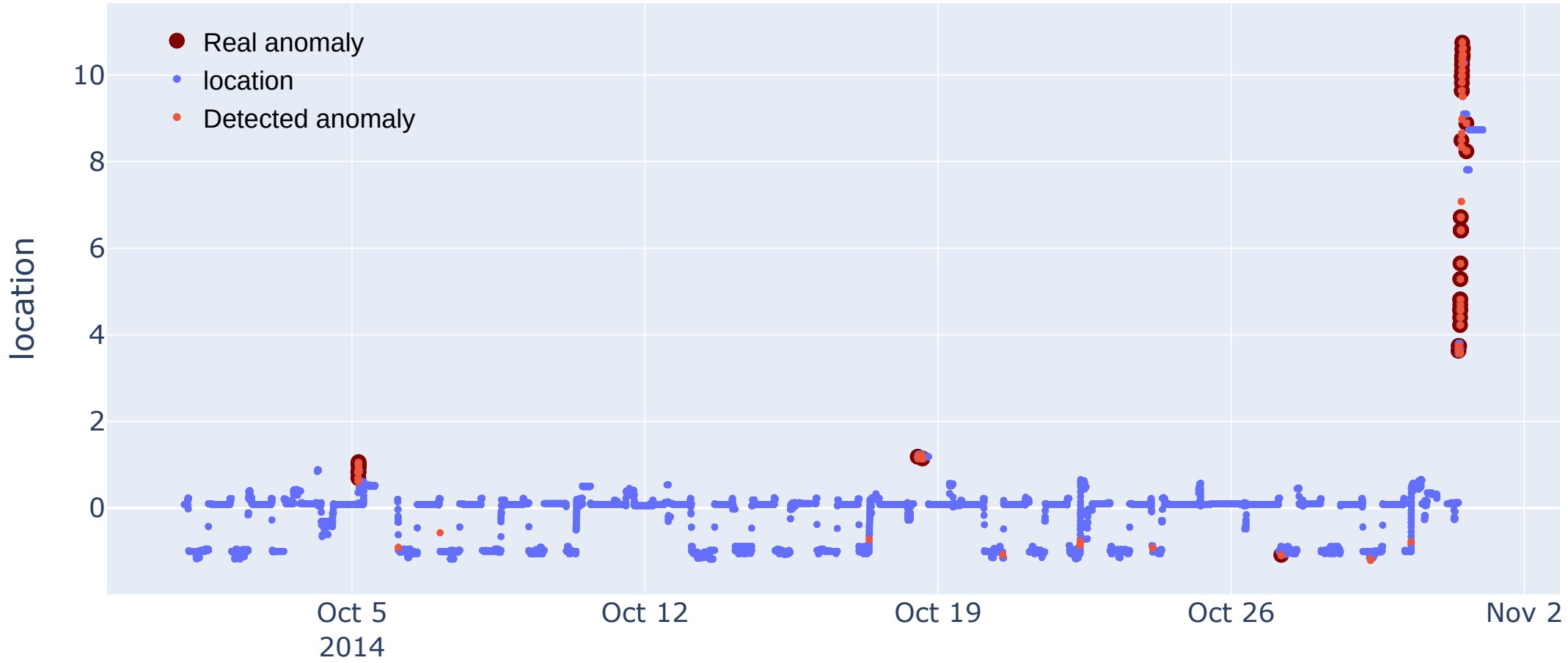
Result on map

Experimental Results (Public Dataset)



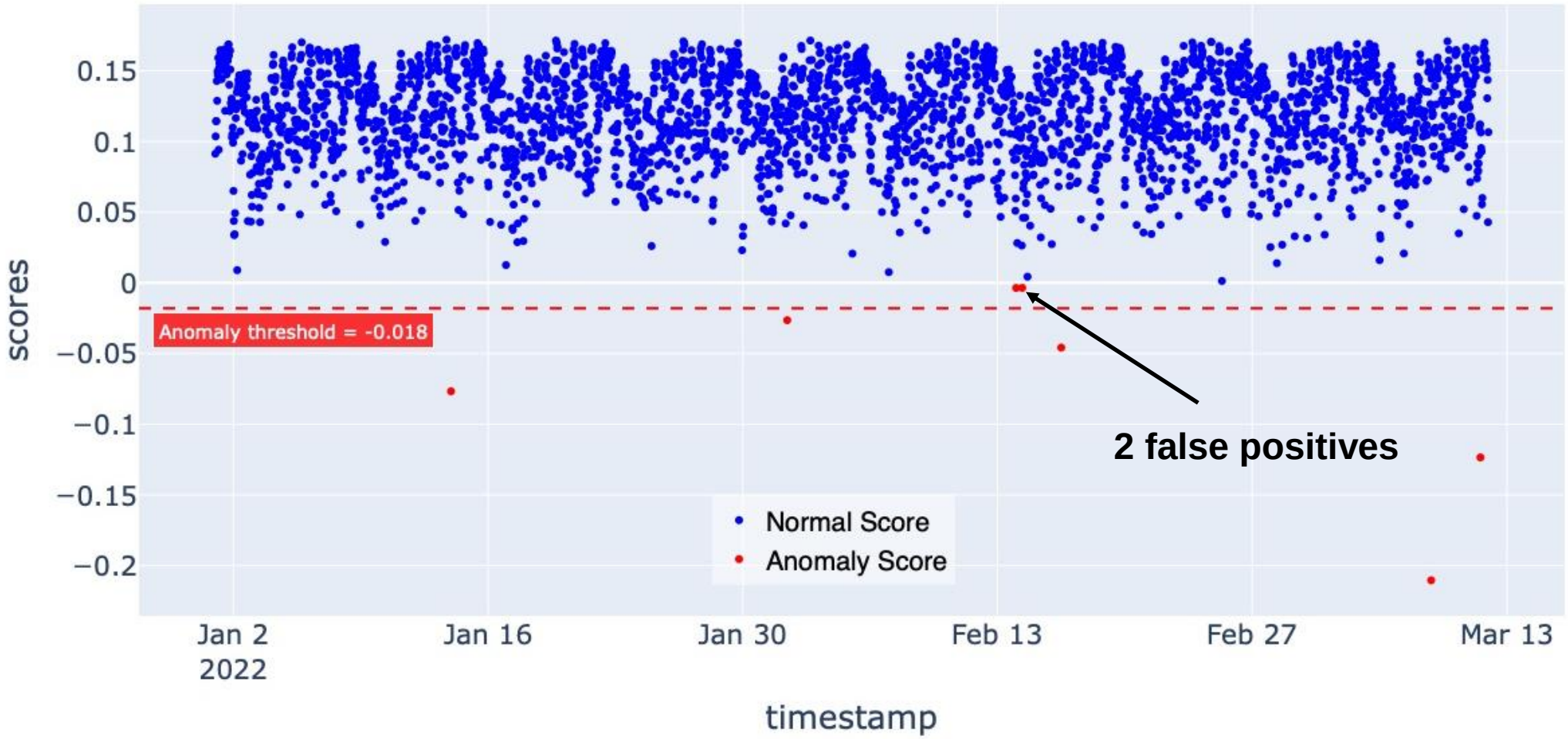
Anomaly Scores

Experimental Results (Public Dataset)



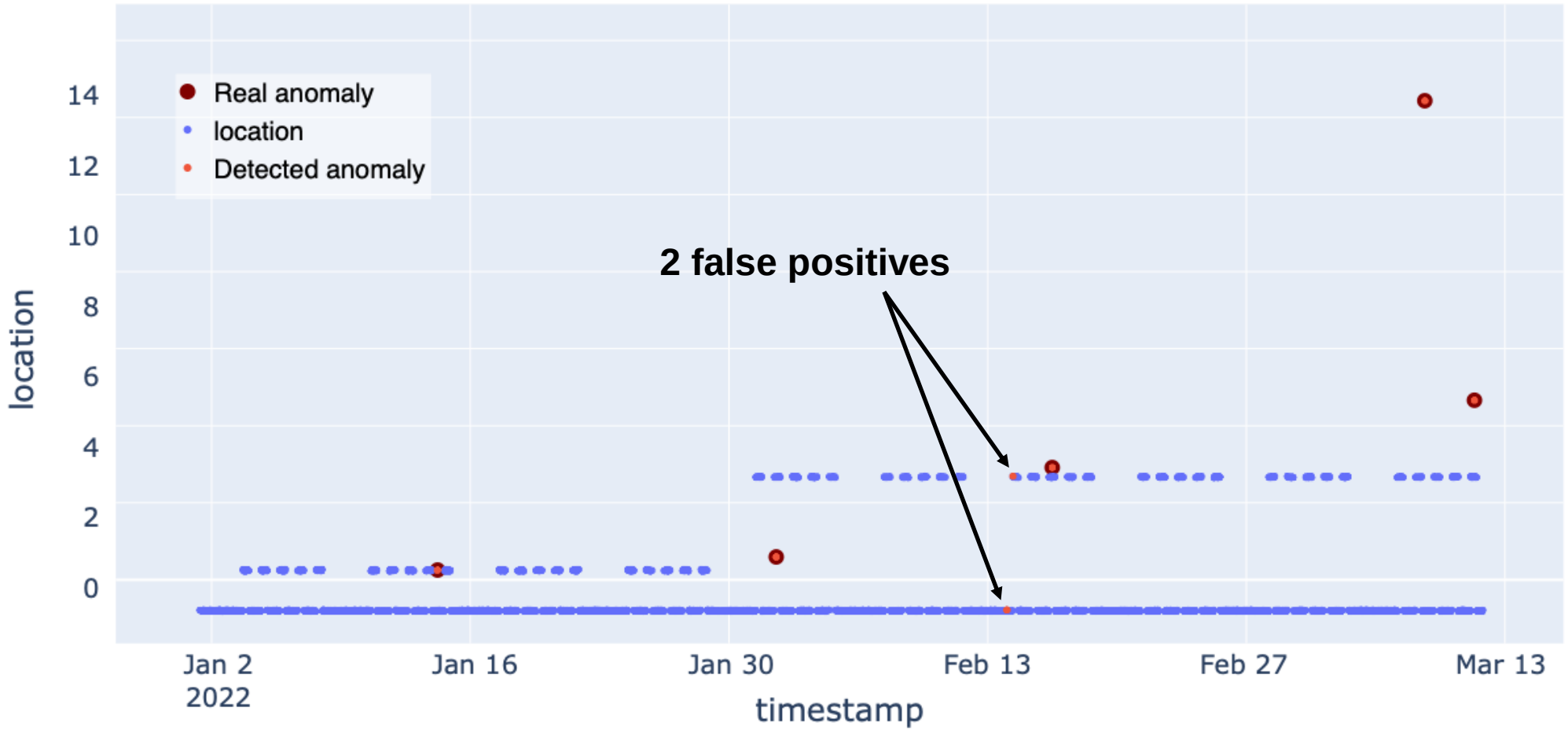
Anomalous locations

Experimental Results (Virtual Dataset)



Anomaly Scores

Experimental Results (Virtual Dataset)



Result on map

Conclusion

- Integrating GPS and ML technologies can enhance the security of traditional authentication factors.
- GPS-based behavioral patterns are more stable compared to previous studies.
- The experimental results across diverse datasets validate the model's ability to detect location deviations from normal patterns, ensuring effective authentication.

Future Research

- For future work, we suggest exploring the integration of additional behavioral patterns and data types to further improve effectiveness and robustness of authentication process.

Thank You !!