JOURNAL OF SOCIAL SCIENCES, HUMANITIES AND INNOVATION

Vol 2 Issue 1 (2026)

http://jsshi.org/

Privacy preserving discovery of failure signatures across heterogeneous wearable devices

Chi-Ho Wong1, Ka-Lok Chan2, Man-Kit Lee3*

Department of Computer Science, The University of Hong Kong, Pokfulam, Hong Kong SAR, China

***Corresponding author:** mankit.lee@hku.hk

Keywords:

wearable devices; federated learning; failure signature discovery; privacy preservation; reliability analytics

Abstract:

Large-scale wearable ecosystems generate vast volumes of diagnostic data that contain valuable information for reliability analysis. However, centralized collection of device logs often raises privacy concerns and bandwidth limitations. This study proposes a privacy-preserving framework for discovering failure signatures across heterogeneous wearable devices. The proposed approach employs federated representation learning combined with secure aggregation to extract shared failure patterns without transferring raw diagnostic logs. Each device locally learns compact log embeddings that capture temporal event relationships, which are then aggregated through a privacy-preserving clustering mechanism. The framework was evaluated on a dataset containing 243 million diagnostic events collected from 68,432 wearable devices across four product categories, including smartwatches, health trackers, AR glasses, and environmental monitoring wearables. Experimental results show that the proposed method identifies 84 distinct failure signatures while preserving 94.1% of clustering quality compared with centralized analysis. In addition, the approach reduces network communication overhead by 82.7% and ensures that no raw log records leave local devices. The findings demonstrate that privacy-preserving failure analysis can enable scalable reliability monitoring across distributed wearable systems.

1.INTRODUCTION

Wearable devices, including smartwatches, health trackers, and AR glasses, continuously generate diagnostic data such as system logs, runtime events, sensor records, and resource-monitoring signals. These data provide important evidence for reliability analysis, anomaly detection, and fault diagnosis in device-side systems [1,2]. In embedded Linux environments, low-power persistent logging is especially important because wearable and edge devices must preserve runtime records while operating under strict energy, storage, and computation limits [3]. As wearable devices are increasingly used in health monitoring, immersive interaction, and mobile computing, the volume and diversity of diagnostic data continue to grow. This creates new opportunities to identify shared failure patterns across devices, but it also increases the pressure on data transmission, privacy protection, and system maintenance cost [4,5].

Traditional reliability analysis methods usually depend on centralized log collection and server-side processing. In this mode, logs and runtime records are uploaded from devices to a central platform for template extraction, anomaly detection, and fault pattern analysis [6,7]. Centralized analysis can achieve good performance when sufficient data are available, but it also introduces several practical limitations. Large-scale wearable deployments may generate frequent diagnostic records, which increase communication overhead and battery consumption. More importantly, wearable devices are closely related to personal behavior, health status, location, and daily activity patterns. Directly transferring raw logs or runtime traces may therefore create privacy risks, even when the original data are not designed as personal information [8,9]. These issues make centralized diagnostic frameworks less suitable for privacy-sensitive wearable systems. Federated learning has been studied as an alternative approach for distributed model training under privacy constraints. It allows devices to train local models with their own data and share only model updates or feature-level information rather than raw records [10,11]. This mechanism can reduce direct data exposure and lower the need for large-scale raw data transfer. In wearable systems, federated learning is particularly useful because devices often operate in different user contexts, network conditions, and power states. Some studies have applied federated learning to log analysis, anomaly detection, and distributed fault diagnosis [12]. Representation learning has also been used to convert raw logs and runtime events into compact feature vectors, which can support clustering, similarity analysis, and failure pattern discovery across devices [13,14]. These methods provide useful foundations for privacy-preserving reliability analysis, but they still face challenges when applied to heterogeneous wearable environments. A major limitation is

that many existing methods assume that data distributions across devices are similar [15,16]. In real wearable systems, however, diagnostic data are highly heterogeneous because devices may differ in hardware configuration, operating system version, application workload, sensor usage, user behavior, and battery status. The same failure type may appear with different log sequences or runtime patterns on different devices, while different faults may produce similar local symptoms [17,18]. This makes cross-device failure signature discovery more difficult than single-device anomaly detection. In addition, some studies rely on small datasets, offline experiments, or simplified fault settings, which cannot fully represent the continuous and diverse conditions of real wearable deployment [19]. Existing methods also pay limited attention to communication cost, although frequent model exchange can become expensive for battery-powered devices. Therefore, a practical framework should protect raw data privacy, tolerate device heterogeneity, reduce communication overhead, and still discover meaningful shared failure signatures.

To address these problems, this study proposes a privacy-preserving framework for failure signature discovery across wearable devices. The proposed method combines federated representation learning with secure aggregation, allowing each device to learn local diagnostic features from logs and runtime events without uploading raw data. Shared failure signatures are identified from aggregated representations, so that common fault patterns can be discovered across devices while reducing privacy exposure. The purpose of this study is to support scalable reliability analysis for wearable systems under real deployment constraints. Its significance lies in providing a diagnostic approach that can use distributed device data without requiring centralized raw-log collection, which is important for privacy-sensitive and resource-limited wearable applications. Compared with conventional centralized analysis, the proposed framework reduces communication cost and better protects user-related diagnostic records. Compared with ordinary federated models, it focuses on failure signature discovery rather than only classification accuracy, making the results more useful for system maintenance and fault interpretation. The method is evaluated using data from multiple wearable devices with different runtime conditions and fault types. The results show that the proposed framework maintains high clustering quality, reduces data transmission, and supports scalable privacy-preserving reliability analysis in wearable systems.

2.Materials and Methods

2.1 Sample and System Description

The study used diagnostic data from a large wearable device network. The dataset includes 243 million runtime events from 68,432 devices. The devices cover four types: smartwatches, health trackers, AR glasses, and environmental monitors. Data were collected during daily use. Each record includes a timestamp, event type, and device ID. The dataset reflects differences in hardware, software, and usage patterns. It includes both normal and fault events.

2.2 Experimental Design and Control Setup

Two methods were compared: a centralized analysis method and the proposed privacy-preserving method. The centralized method collects all logs to a server for clustering. The proposed method keeps data on devices and shares only model updates. Both methods used the same dataset and clustering settings. Tests compared clustering quality, communication cost, and data exposure. This design allows a direct comparison under the same conditions.

2.3 Measurement Methods and Quality Control

Logs were collected using built-in systems on each device. All records include timestamps for time alignment. Invalid and repeated entries were removed during cleaning. Each test was repeated three times, and mean values were reported. Clustering results were checked against labeled fault categories. Network usage was recorded to measure data transfer. The aggregation process was checked to ensure that raw logs were not shared. These steps improve data quality and result stability.

2.4 Data Processing and Model Formulation

Log sequences were converted into fixed-length feature vectors on each device. These vectors capture event order and timing. Clustering quality Q was defined as:

$$Q=\frac{1}{N}\sum_{i=1}^{N}\frac{b(i)-a(i)}{\max(a(i),b(i))}$$

Communication cost C was defined as:

$$C=\sum_{k=1}^{K}S_k$$

Here, a(i) is the average distance within a cluster, and b(i) is the distance to the nearest cluster. These measures were used to compare methods.

2.5 Evaluation Metrics and Analysis Criteria

Performance was measured by clustering quality, number of failure patterns, communication cost, and data privacy. Clustering quality shows how well patterns are grouped. Communication cost shows network load. Privacy is checked by whether raw logs are shared. Statistical tests were conducted at a 95% confidence level. The method was considered effective if it kept high clustering quality while reducing data transfer and protecting data.

3.Results and Discussion

3.1 Discovery of shared failure patterns

The method identified 84 failure patterns from 243 million events collected from 68,432 wearable devices. Clustering quality reached 94.1% of the centralized method. This result shows that local feature learning with secure aggregation can keep most of the data structure. Wearable data differ across devices and usage conditions, which makes pattern discovery difficult. The result indicates that the proposed method can still capture common fault features without using raw logs. Similar studies in federated learning report that local training can keep useful information while reducing data transfer [20,21].

3.2 Communication reduction and privacy effect

The method reduced network communication by 82.7% compared with centralized collection. This reduction comes from sending compact updates instead of full logs. In large wearable systems, communication cost can limit system performance. Lower data transfer also reduces the risk of data exposure. Earlier studies on privacy-preserving data collection show similar benefits. The present result confirms that these advantages remain when the task is failure pattern discovery rather than classification [22].

3.3 Effect under device heterogeneity

The method performed well across four device types, including smartwatches, health trackers, AR glasses, and environmental monitors. This shows that local feature learning can handle differences in device data. Heterogeneity is a common problem in federated systems because data distributions vary across devices. Many existing studies focus on supervised tasks, but fewer

examine unsupervised pattern discovery [23,24]. As shown in Fig.1, the proposed framework separates local learning from aggregation, which helps maintain consistency across devices.

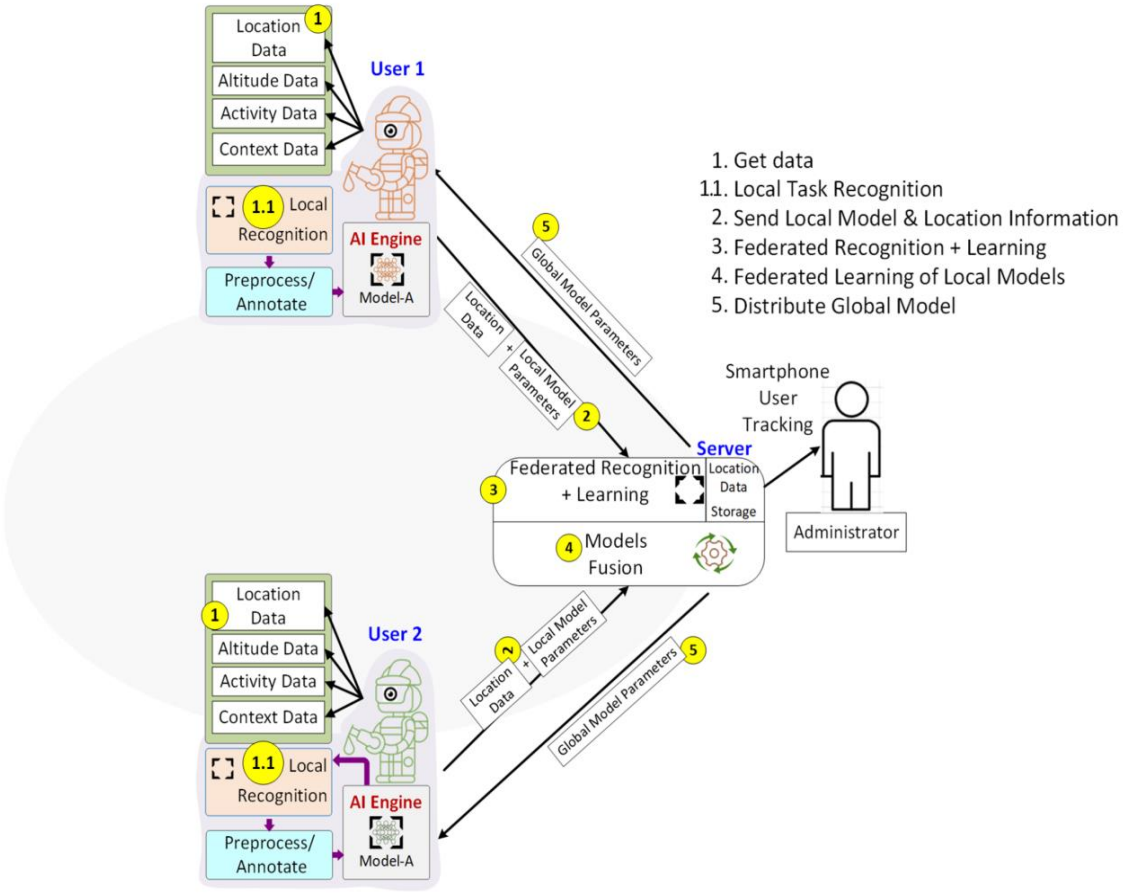


Figure 1 Workflow of federated learning for privacy-preserving wearable data analysis.

3.4 Comparison with existing studies and limitations

Compared with earlier work, this study combines large-scale data, privacy protection, and failure pattern discovery in one framework. Most existing studies focus on activity recognition or anomaly detection, rather than shared fault patterns across devices [25]. The results show that privacy-preserving methods can support large-scale reliability analysis. However, the evaluation is based on clustering quality compared with a centralized method. It does not include direct validation with repair results. In addition, the dataset covers four device types but not all wearable systems. As shown in Fig.2, privacy protection and communication reduction can be achieved together, but further tests on more devices and fault types are needed.

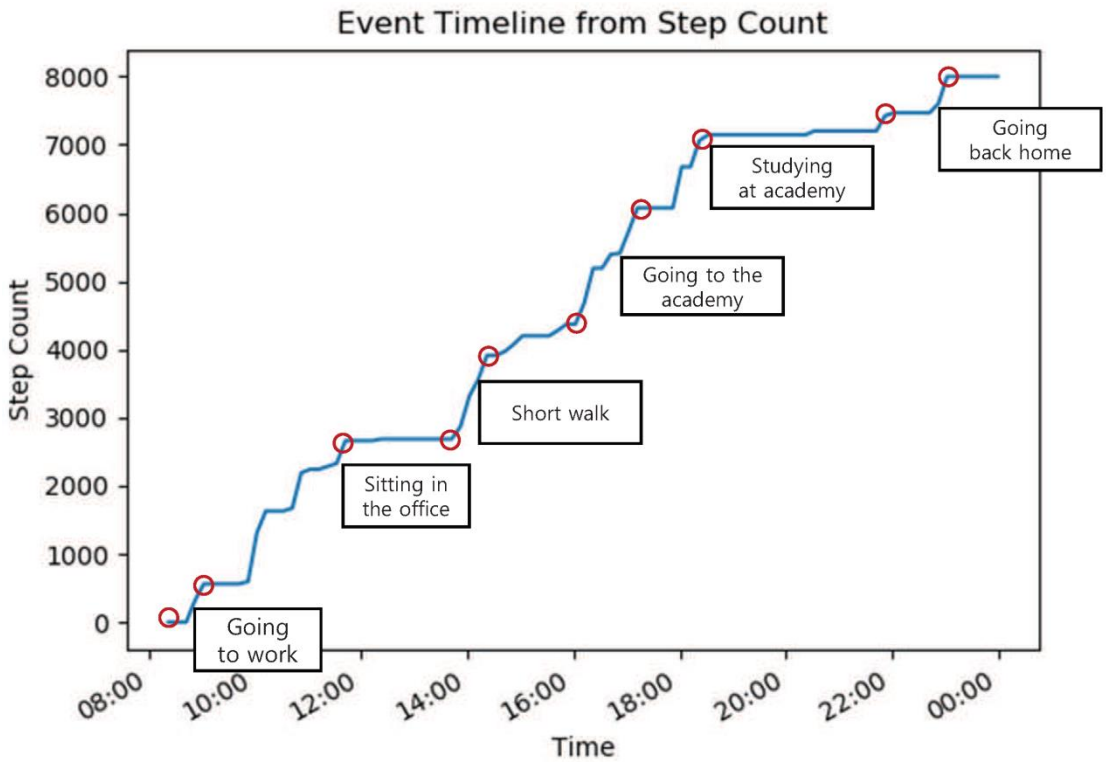


Figure 2 Data collection process on wearable devices with local privacy protection.

Conclusion

This study examined failure pattern discovery in large wearable systems under privacy limits. A framework was designed that combines federated feature learning with secure aggregation. Each device learns local features, and shared patterns are found without sending raw logs. Tests on a large dataset showed that the method can identify common failure patterns with high clustering quality while reducing data transfer. Communication cost was greatly reduced, and raw data stayed on local devices. These results show that useful analysis can be achieved without central data collection. The main contribution of this work is the use of local feature learning together with privacy-preserving aggregation for failure analysis. Unlike traditional methods that depend on full data collection, the proposed approach keeps useful information while limiting data exposure. This design supports scalable monitoring in systems with many distributed devices. The framework can be used in other edge systems that require data protection, such as health monitoring platforms and mobile sensing networks. However, the study uses a limited number of device types and fault categories. The results are based on clustering quality rather than direct repair outcomes. Future work should include more device types and real maintenance data to further test the method.

References

[1] Qin, F., Cheng, H. Y., Sneeringer, R., Vlachostergiou, M., Acharya, S., Liu, H., ... & Yao, L. (2021, May). ExoForm: Shape memory and self-fusing semi-rigid wearables. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-8).

[2] Sefati, S. S., Craciunescu, R., & Arasteh, B. (2026). An Energy-Aware Security Framework for the Internet of Things Integrating Blockchain and Edge Intelligence. Computers.

[3] Wu, C., Zhang, F., Chen, H., & Zhu, J. (2025). Design and optimization of low power persistent logging system based on embedded Linux.

[4] Aslam, S., Navarro, A., Aristotelous, A., Garro Crevillen, E., Martınez-Romero, A., Martínez-Ceballos, Á., ... & Michaelides, M. P. (2025). Machine learning-based predictive maintenance at smart ports using IoT sensor data. Sensors, 25(13), 3923.

[5] Yue, L., Xu, D., Qiu, D., Shi, Y., Xu, S., & Shah, M. (2026). Sequential Cooperative Multi-Agent Online Learning and Adaptive Coordination Control in Dynamic and Uncertain Environments.

[6] Lestander, T. (2025). Anomaly Detection in Large-Scale Log Data: Parsing, Feature Extraction, and Unsupervised Learning.

[7] Gao, X., Chen, J., Huang, M., & Fang, S. (2025). Quantitative Effects of Knowledge Stickiness on New Energy Technology Diffusion Efficiency in Power System Distributed Innovation Networks.

[8] Aghili, R., Li, H., & Khomh, F. (2025). Protecting privacy in software logs: What should be anonymized?. Proceedings of the ACM on Software Engineering, 2(FSE), 1317-1338.

[9] Feng, H. (2024, October). Design of Intelligent Charging System for Portable Electronic Devices Based on Internet of Things (IoT). In 2024 5th International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) (pp. 568-571). IEEE.

[10] Karmode, S., & Shahade, A. K. (2026). A comprehensive review and future directions on blockchain-integrated deep federated learning for privacy-preserving healthcare applications. International Journal of Data Science and Analytics, 22(1), 96.

[11] Liu, S., & Yim, J. (2025). Research on Generative AI Creation Systems Based on Visual Language Modeling: Human-Machine Collaboration and Cognitive Feedback Mechanisms. Available at SSRN 6139770.

[12] Singh, P. K., Chowdhury, A., & Pal, A. (2025). Distributed anomaly detection using federated learning. IEEE Access.

[13] Su, X., Wang, X., & Zhang, J. (2025). Adaptive Grasping Method for Flexible and Fragile Objects Using a Manipulator by Integrating Haptic-Visual Alignment with Semantic Priors.

[14] Hadadi, F. (2025). Automated Log Analysis: Failure Prediction and Anomaly Detection using Machine Learning and Large Language Models (Doctoral dissertation, Université d'Ottawa/University of Ottawa).

[15] Gao, H., Wang, H., Feng, Z., Fu, M., Ma, C., Pan, H., ... & Li, N. (2016, October). A novel texture extraction method for the sedimentary structures' classification of petroleum imaging logging. In Chinese Conference on Pattern Recognition (pp. 161-172). Singapore: Springer Singapore.

[16] Shahnawaz, M., & Kumar, M. (2025). A comprehensive survey on big data analytics: Characteristics, tools and techniques. ACM Computing Surveys, 57(8), 1-33.

[17] Yue, L., Xu, D., Qiu, D., Shi, Y., Xu, S., & Shah, M. (2025, December). Sequential Cooperative Multi-Agent Online Learning and Adaptive Coordination Control in Dynamic and Uncertain Environments. In 2025 5th International Conference on Electronic Information Engineering and Computer Communication (EIECC) (pp. 692-697). IEEE.

[18] Shah, M. B., Morovati, M. M., Rahman, M. M., & Khomh, F. (2026). Characterizing faults in agentic AI: A taxonomy of types, symptoms, and root causes. arXiv preprint arXiv:2603.06847.

[19] Gao, G., Ma, X., Lu, C., & Gao, R. (2026). Reliability Analysis and Application Research of SMS Communication Systems in Medical Notification Scenarios.

[20] Almogadwy, B., & Alqarafi, A. (2025). Fused federated learning framework for secure and decentralized patient monitoring in healthcare 5.0 using IoMT. Scientific Reports, 15(1), 24263.

[21] Wang, Y., Yin, X., Chen, J., & Wang, Y. (2026). Evidence-Based Study on Low-Burden Digital Phenotyping for Precision Screening of Oral Anti-Obesity Drug Efficacy.

[22] Attallah, O., Ibrahim, R. A., & Zakzouk, N. E. (2025). A lightweight deep learning framework for transformer fault diagnosis in smart grids using multiple scale CNN features. Scientific reports, 15(1), 14505.

[23] Zhang, Y., Gu, W., & Wang, J. (2026). Construction of Wind Farm Asset Health Index Based on Multi-Dimensional Indicators and Analytic Hierarchy Process and Its Correlation with Operational Performance. Authorea Preprints.

[24] Shanaa, M., & Abdallah, S. (2025). A hybrid anomaly detection framework combining supervised and unsupervised learning for credit card fraud detection. F1000Research, 14, 664.

[25] Yu, X. (2026). Enhancing Search Efficiency through LLM-Based User Memory Systems for Query Matching and Intent Modeling.