MagWatch: Exposing Privacy Risks in Smartwatches Through Electromagnetic Signals

Haowen Xu[1], Tianya Zhao[2], Xuyu Wang[2], Jun Dai[1](✉), and Xiaoyan Sun[1](✉)

[1] Worcester Polytechnic Institute, Worcester, MA 01609, USA
{hxu4,jdai,xsun7}@wpi.edu
[2] Florida International University, Miami, FL 33199, USA
{tzhao010,xuywang}@fiu.edu

Abstract. As smartwatches become increasingly integrated into daily life, their electromagnetic (EM) emissions introduce a significant yet overlooked privacy risk. This study systematically examines how EM leakage from smartwatches can be exploited to infer user interactions and behavioral patterns. We propose *MagWatch*, a novel non-intrusive attack that applies wavelet transform for signal processing and leverages a CNN-LSTM model to identify applications and in-app activities, achieving up to 90% accuracy across multiple smartwatch models. Our findings reveal a critical security vulnerability, demonstrating that attackers can passively monitor EM emissions to reconstruct user interactions, exposing sensitive information such as communication habits and app usage patterns. This research highlights the urgent need for privacy-preserving countermeasures in wearable technology and establishes a foundation for future studies on EM side-channel security risks.

Keywords: Side Channel Attack · Privacy Leakage · Electromagnetic Signal · Smartwatch

1 Introduction

The widespread adoption of smartwatches has made them an integral part of users' daily lives. According to market research, the global smartwatch market is projected to reach 253 million units by 2025 [21]. Users increasingly rely on smartwatches not only for payments, communication, navigation, and remote control but also for continuous health monitoring, including heart rate tracking, blood oxygen measurement, and sleep analysis [5,10,11,20]. As these devices become more autonomous, many users interact with them independently of their smartphones [3], making them attractive targets for security threats.

Although extensive research has been conducted on the security of mobile devices and the Internet of Things (IoT), the security of smartwatches remains relatively underexplored. Previous studies have identified various vulnerabilities

J. Han et al. (Eds.): ICICS 2025, LNCS 16217, pp. 329–346, 2026.
https://doi.org/10.1007/978-981-95-3540-8_18

in wearable devices, such as motion sensor-based attacks [25], weaknesses in authentication mechanisms, and security risks associated with third-party applications [12]. However, most existing research has focused mainly on software-based vulnerabilities, largely overlooking side-channel threats in smartwatches.

In this study, we identify and analyze for the first time a significant electromagnetic (EM) leakage issue in smartwatches, particularly when operating on cellular networks. Unlike Bluetooth-only smartwatches, cellular-enabled smartwatches generate stronger EM emissions due to their higher power consumption and continuous network communication. These emissions originate from various hardware components, including wireless communication modules (4G/5G), processors, and sensors, all of which contribute to a unique EM side-channel footprint. When users interact with their smartwatches—such as receiving notifications, making calls, or synchronizing data—the wireless transmission and computational workload induce distinguishable EM patterns. Similarly, different in-app activities trigger specific processing states, leading to identifiable EM leakage signatures that an attacker can exploit. We have designed and implemented MagWatch to demonstrate the feasibility of leveraging our reported electromagnetic side-channel leakage to launch a contactless, fine-grained, and scalable attack on smartwatches for the first time.

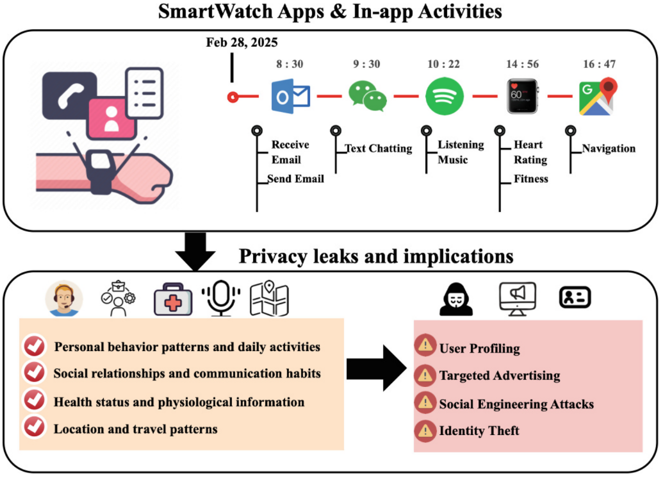

SmartWatch Apps & In-app Activities
Feb 28, 2025
8 : 30
9 : 30
10 : 22
14 : 56
16 : 47
Receive Email
Send Email
Text Chatting
Listening Music
Heart Rating
Fitness
Navigation
Privacy leaks and implications
Personal behavior patterns and daily activities
Social relationships and communication habits
Health status and physiological information
Location and travel patterns
User Profiling
Targeted Advertising
Social Engineering Attacks
Identity Theft

Fig. 1. Smartwatch Privacy Leaks and Their Consequences

EM side-channel attacks pose a particularly severe security risk as they leverage unintended physical emissions rather than software vulnerabilities [7,16,17], allowing adversaries to infer user activities without requiring malware installation or direct access to the device. Unlike cryptographic attacks that target encryption algorithms, EM-based techniques passively extract sensitive information from seemingly benign system operations, making them difficult to detect and mitigate. Moreover, these attacks can be conducted remotely, enabling an adversary to monitor smartwatch EM emissions from a distance without physical access, significantly increasing their feasibility as a scalable attack vector.

As shown in Fig. 1, beyond merely recognizing the applications in use (e.g., social media, music, or productivity apps), EM side-channel attacks can also identify fine-grained in-app activities, exposing detailed user behavior patterns. This means that even without direct access to the smartwatch, an adversary could infer whether a user is engaging in communication, media consumption, or work-related tasks, raising serious privacy concerns. More critically, the combination of app identification and in-app activity recognition enables adversaries to construct long-term behavioral profiles, revealing user preferences, app usage habits, daily routines, social interaction frequency, and even work intensity [22]. In certain cases, this could extend to exposing personal life patterns or professional confidentiality [19], demonstrating that EM side-channel attacks have far-reaching implications beyond simple app recognition.

We propose and demonstrate MagWatch, a contactless EM side-channel attack, and evaluate its effectiveness, in uncovering three key aspects of user privacy: app launching, in-app activity recognition, and behavioral inference. Our experimentation, conducted on multiple smartwatch models, demonstrates that MagWatch achieves high classification performance in different scenarios. Specifically, for *application recognition*, MagWatch successfully classifies 16 smartwatch applications, achieving an average accuracy above 90%, with only navigation and heart-rate monitoring apps showing moderate mis-classification due to similar sensor usage. Regarding *in-app activity recognition*, across multiple applications, MagWatch can differentiate specific in-app activities, with classification accuracy reaching over 85% in apps such as WeChat, Outlook, and Spotify. The attack exhibits exceptional effectiveness at close range, maintaining high accuracy. While accuracy gradually declines beyond 7.5 cm and drops below 20% at 12.5 cm, this aligns with the inherent range characteristics of EM-based attacks, which are optimized for short-distance precision, as consistently observed in the literature, such as [16,17].

This paper presents the following key contributions:

- This paper conducts systematic analysis of electromagnetic leakage in smartwatches, evaluating its impact across various applications and user activities.
- This paper introduces MagWatch, a novel contactless side-channel attack model that utilizes EM leakage to infer user interactions without requiring software exploitation.
- This paper explores countermeasures against EM-based privacy threats, proposing effective mitigation strategies while highlighting previously underestimated security risks in smartwatches.

By addressing this emerging security challenge, we aim to provide new insights into smartwatch privacy risks and contribute to the broader field of wearable device security and electromagnetic side-channel analysis.

2 Background and Related Work

2.1 Background

Electromagnetic (EM) signals arise from the movement of electric charges, as described by Maxwell's equations. When an electric current flows through a conductor, it generates both electric and magnetic fields. According to Ampère's Law with Maxwell's correction [15]:

$$\nabla \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \tag{1}$$

where $\mathbf{B}$ is the magnetic field, $\mathbf{J}$ is the current density, μ_0 is the permeability of free space, and ε_0 is the permittivity of free space. This equation indicates that both electric currents and time-varying electric fields contribute to the formation of magnetic fields. In electronic devices, rapid switching of transistors, varying clock speeds, and fluctuating power consumption introduce dynamic electromagnetic emissions. These emissions, often categorized as electromagnetic interference (EMI), are a byproduct of hardware activity and can serve as a side channel for information leakage. In smartwatches, just like in smartphones [7], various hardware components contribute to the generation of EM signals. CPU and memory operations induce fluctuating electrical currents as processes are executed, leading to distinct magnetic field variations. Power management circuits dynamically regulate voltage and current, producing low-frequency magnetic fluctuations. Display drivers and touchscreen circuits generate periodic electromagnetic variations as screens refresh or register user interactions. Since different applications invoke different hardware modules upon launching, they induce unique electromagnetic patterns, as illustrated in Fig. 2.

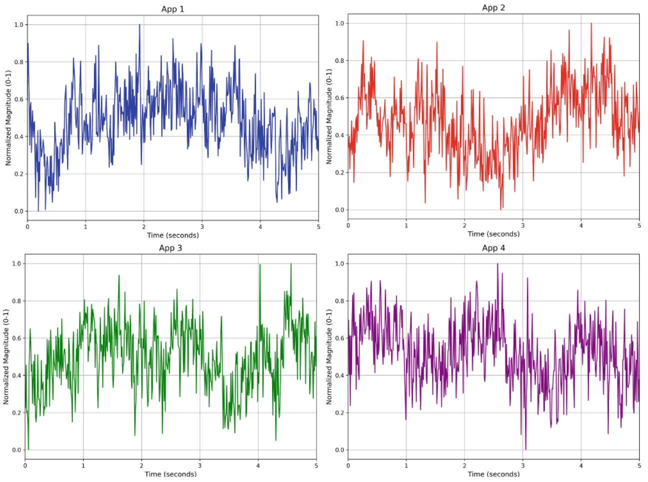


Fig. 2. Different EM Patterns of Four Apps (as Illustration)

2.2 Related Work

Most prior research on smartwatch privacy has focused on data collection and user perception rather than side-channel threats. Emmanuel Sebastian Udoh [23] and HongSuk Yoon [27] have both conducted user research on smartwatch privacy risks. Yoon's qualitative study focuses on users' perspectives regarding information tailoring and data privacy through surveys and interviews, while Udoh's exploratory study assesses American college students' privacy awareness and attitudes toward smartwatch-related privacy issues. A key concern raised in previous studies [12,24] is the "Privacy Paradox", the phenomenon where users express concerns about privacy but fail to take adequate protective measures. Many smartwatch users underestimate the extent of personal data their devices collect and share, including GPS location, health metrics, and communication logs [14]. Furthermore, the integration of third-party applications exacerbates privacy risks, as user data can be shared beyond their control, leading to potential security breaches. These researches rely on user surveys and behavioral studies rather than direct hardware-based security assessments.

Although privacy concerns regarding smartwatch applications have been studied, electromagnetic (EM) side-channel risks in smartwatches remain largely unexplored. Most existing EM side-channel attack research has been conducted on smartphones and computers, leaving wearable devices unexamined. Zhu et al. [28] first utilized mobile phone magnetometers to analyze electromagnetic radiation footprint from nearby computers, enabling app and webpage inference. Tao et al. [16,17] investigated electromagnetic side-channel leakage in smartphones during wireless charging, revealing how sensitive information can be inferred from EM emissions. Similarly, Yushicheng et al. [4] studied EM-based privacy leakage from computers, exposing vulnerabilities in cryptographic implementations and system operations. Furthermore, Yongjian Fu et al. [7] demonstrated how EM emissions from smartphones can be exploited to infer user activities and extract sensitive data. Additionally, prior work has demonstrated EM-based fingerprinting of USB devices [8] and profiling of IoT device activities through side-channel emissions [1]. These studies highlight the risks associated with EM-based side channels in traditional computing devices, yet the potential privacy threats posed by EM emissions from smartwatches remain largely unexamined. Given the compact design, reliance on multiple sensors, and frequent connectivity with smartphones and other IoT devices, smartwatches may exhibit distinct EM leakage characteristics, warranting further investigation.

3 Threat Model

We consider a realistic threat scenario where a victim wears a smartwatch and engages in daily activities such as making payments, answering calls, and monitoring heart rate (Fig. 3). These interactions generate distinct electromagnetic (EM) emissions, which an attacker can exploit to infer sensitive behaviors. This attack can occur in public or semi-public environments such as *cafes, offices,* *and public transportation hubs (e.g., airport, train station, or subway compartments)*, where users frequently interact with their smartwatches near tables and desks.

We assume that the attacker can be in close proximity to the victim, either by being physically present in the same space or by strategically placing hidden EM sensing devices in frequently visited locations. The adversary may be an unauthorized third party, such as a cybercriminal, a corporate espionage agent, or a surveillance entity seeking to extract private information. The attacker can discreetly deploy malicious EM sensing devices, such as software-defined radios (SDRs) or concealed antennas, under tables or desks to passively capture smartwatch-generated EM signals. Due to their small size, these sensing devices can be disguised as common objects such as earphones, chargers, power banks, or wireless mice, making them difficult to detect. Once deployed, these devices enable continuous and covert data collection. Beyond hardware attacks, the attacker may also exploit a compromised smartphone app running on the victim's paired device, using side channels to extract EM data in the background and upload it to a remote server for further analysis. More sophisticated attackers may deploy multiple hidden sensors across an environment, such as different tables in a shared workspace or a cafe, allowing them to aggregate signals from various perspectives to enhance tracking accuracy and improve the reconstruction of user activities. By analyzing these captured EM emissions, the attacker can infer financial transactions, call and messaging patterns, health monitoring behaviors, and authentication gestures, posing significant privacy risks. This threat model demonstrates that EM side channels can be practically leveraged to infer smartwatch activities without requiring direct access to the device, highlighting the feasibility and stealthiness of such attacks.

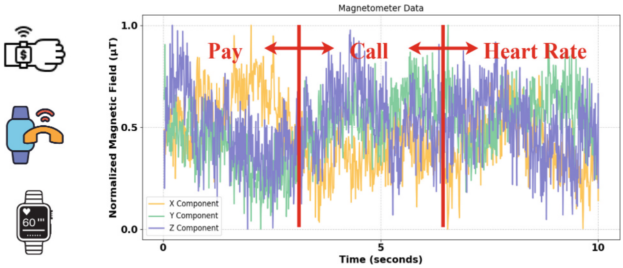


Fig. 3. Motivating Example Scenario: A user wearing a smartwatch sequentially makes a payment, receives a call, and checks their heart rate. Each action activates the smartwatch's corresponding functions, generating distinct electromagnetic signals throughout the process.

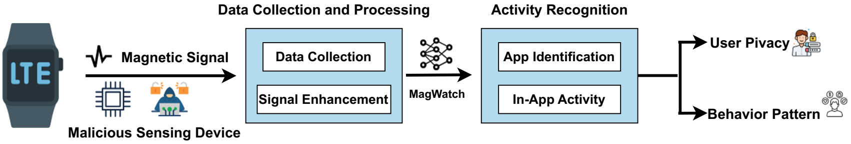


Fig. 4. Overview of MagWatch

4 Approach Overview

In this section, we provide a detailed overview of MagWatch, followed by an in-depth discussion of each stage in the pipeline. As illustrated in Fig. 4, the proposed system begins with data collection, where magnetic signals emitted by the smartwatch are captured using a malicious sensing device. These signals undergo enhancement and processing to improve their quality before being analyzed by the MagWatch model. The recognition phase leverages machine learning techniques to infer in-app activities and app launching events. Ultimately, this extracted information can be used to deduce user privacy risks and uncover behavioral patterns.

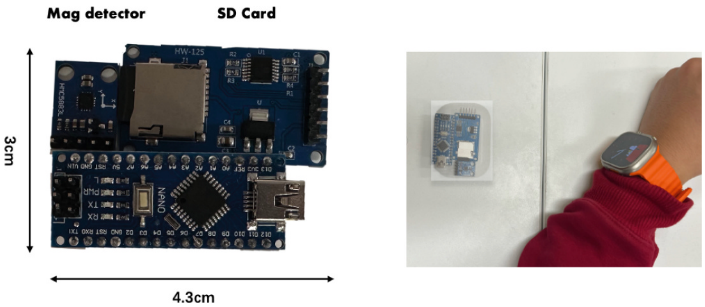


Fig. 5. Attack Device and Attack Scenarios

4.1 Data Collection

Data collection involves discreetly capturing EM signals in public or semi-public environments. Specifically, to record electromagnetic emissions from an iWatch 11.2 and iWatch 10 under various operating conditions, we developed a covert attack device designed for unobtrusive data collection, as shown in Fig. 5. This device is equipped with a QMC5883L sensor and an Arduino Nano, which processes the captured electromagnetic signals. Its compact and concealed design enhances effectiveness for covert data collection.

Algorithm 1. Electromagnetic Signal Enhancement via Wavelet Analysis

```
Require: EM signal sequence $X = \{x_1, x_2, \ldots, x_n\}$ with axes $\{x, y, z\}$, window size $w$
Ensure: Enhanced signal sequence $X_{enhanced}$
Initialize empty list $X_{enhanced}$
while number of samples in $X \geq w$ do
    Fetch subsequence $X'$ of length $w$ from $X$
    for each axis $a \in \{x, y, z, magnitude\}$ do
        $S_a \leftarrow$ signal values of axis $a$ from $X'$
        $S_a \leftarrow S_a - \text{mean}(S_a)$                ▷ Remove DC component
        $S_a \leftarrow S_a / \text{std}(S_a)$                 ▷ Normalize signal
        $C_a \leftarrow \text{WaveletDecompose}(S_a, \text{'db4'}, \text{level} = 4)$
        for each detail coefficient level $i \in \{1, 2, 3, 4\}$ do
            $T_i \leftarrow 0.5 \times \text{std}(C_a[i])$            ▷ Adaptive threshold
            $C_a[i] \leftarrow \text{SoftThreshold}(C_a[i], T_i)$
            $C_a[i] \leftarrow \text{sign}(C_a[i]) \times |C_a[i]|^{0.75}$    ▷ Non-linear enhancement
        end for
        $S'_a \leftarrow \text{WaveletReconstruct}(C_a, \text{'db4'})$
        $S'_a \leftarrow S'_a[0 : w]$                     ▷ Trim to original length
    end for
    Create enhanced frame $F_{enhanced}$ by combining all axes $S'_a$
    Append $F_{enhanced}$ to $X_{enhanced}$
end while
return $X_{enhanced}$
```

4.2 Signal Enhancement

This paper proposes an electromagnetic signal enhancement algorithm based on wavelet transform [6], specifically designed for processing multi-axis electromagnetic signals with subtle variations. The proposed method integrates wavelet decomposition with adaptive thresholding to enhance significant signal features while preserving overall signal integrity.

For wavelet selection, the Daubechies-4 (db4) wavelet is employed as the basis function due to its optimal balance between smoothness and localization, making it particularly suitable for electromagnetic signal analysis. The algorithm utilizes a multi-level wavelet decomposition strategy, where the signal is decomposed into approximation and detail coefficients across multiple frequency bands, enabling localized feature extraction.

To effectively suppress noise while retaining essential signal structures, adaptive thresholding is applied based on the statistical properties of wavelet coefficients, as shown in Algorithm 1. Specifically, the threshold value at each decomposition level is computed dynamically as:

$$T_j = 0.5 \times \sigma(C_a[i]) \tag{2}$$

where $\sigma(C_a[i])$ represents the standard deviation of the wavelet coefficients at level j. After thresholding, the detail coefficients undergo a non-linear enhancement transformation formulated as:

$$\hat{d}_{j,k} = \mathrm{sign}(d_{j,k}) \left((|d_{j,k}| - T_j)_+ \cdot |d_{j,k}|^{0.75} \right) \tag{3}$$

where $(x)_+$ denotes the positive part of x, ensuring that only coefficients exceeding the threshold contribute to the enhanced signal. The power-law transformation with an exponent of 0.75 amplifies relevant features while suppressing noise interference.

The proposed approach effectively enhances both global and localized signal variations, ensuring robust performance across diverse signal conditions. By processing each spatial axis independently and subsequently integrating them into a coherent enhanced signal, the method preserves both temporal and spatial relationships within the data.

This methodology is particularly advantageous for electromagnetic signal processing, where traditional enhancement techniques may struggle to capture subtle but meaningful variations. The combination of wavelet-based decomposition, adaptive thresholding, and non-linear enhancement makes this approach especially suitable for applications requiring high-precision signal analysis, such as pattern recognition in electromagnetic data.

4.3 Activity Recognition

Convolutional Neural Networks (CNNs) [26] are extensively used across different domains and demonstrate strong performance in feature extraction and classification tasks. Once we obtain the enhanced EM signal sequence, we first use a CNN to extract key features for subsequent activity recognition. To balance efficiency and performance, we opt for a simple two-layer CNN in this study, ensuring feature extraction without imposing a heavy computational load.

The first convolutional block consists of a convolution layer with 64 filters of size 7 and a stride of 1, followed by a max-pooling layer with stride 2, a ReLU activation [9], and a batch normalization layer. The second convolutional block has a similar structure as the previous one, except that the convolution layer is different. The second convolutional layer has a kernel size of 5, a stride of 1, and 128 output channels. After extracting the EM features, we then introduce two Long Short-Term Memory (LSTM) [13] layers to model the temporal dependencies. The first LSTM layer, with 128 units, processes the output features from the convolutional layers and transfers the information to the subsequent layer. To prevent overfitting and enhance generalization, a dropout layer with a rate of 0.3 is applied after the first LSTM layer. The second LSTM layer, consisting of 64 units, further refines the learned sequential features and outputs a fixed-length representation of the data, capturing the underlying temporal patterns. Last, a fully connected layer with 64 units and a ReLU activation function is added to process the output from the LSTM layers for the final activity prediction. A dropout layer follows to help prevent overfitting.

To validate the effectiveness of these hyperparameter settings, we evaluate the impact of different LSTM unit sizes and dropout rates on model accuracy in Sect. 5.3. The results indicate that a configuration of 128 LSTM units with a dropout rate of 0.3 achieves the highest validation accuracy of 93%.

5 Evaluation

5.1 Experiment Setup

Our evaluation involves two sets of equipment: an attack device for data collection and a computing device for processing, training, and testing the collected data. We can use the attack device we designed to discreetly collect the electromagnetic signals, as introduced in Sect. 4.1. We can also opt to use a smartphone's built-in electromagnetic sensor, as demonstrated in this experimental setup, for data collection instead. The experiment was carried out by collecting electromagnetic (EM) signals from the victim's device at a sampling rate of 10 milliseconds per data point.

The environment was intentionally non-isolated, with electromagnetic interference from other electronic devices to simulate a realistic setting. To capture the side-channel signals covertly, the receiver was placed underneath the victim's desk, directly below the target device. This setup replicates a realistic attack scenario where the attacker collects EM emissions without direct physical access to the victim's device, a method commonly used in practice, as documented in the literature.

The Sensor Logger app [2] was used to record electromagnetic signals, ensuring a controlled and systematic data acquisition process. To maintain consistency, the battery level of the smartwatch was kept between 60% and 80%, preventing extreme power states from affecting the collected signals. Additionally, all background applications on the smartwatch were forcefully closed, ensuring that only the target application was running during the experiments, allowing for consistent and comparable data.

5.2 Datasets

We construct four datasets using commodity smartwatches under different conditions to evaluate their effectiveness in Sect. 5.4. These datasets are collected from four smartwatch models (Apple Watch Ultra 2, Apple Watch 10, Xiaomi Watch S3, and Huawei Watch 4) to train various models and assess their performance in app recognition, in-app activity classification, signal analysis across different distances, and cross-device application.

Table 1. App Categories and Corresponding App List

Category	App List (on Both Android and iOS)
Video & Music	Youtube, Spotify, Apple Music
Social	Wechat, Message, Outlook, QQ Email, WhatsApp
Navigation	Apple Map, Google Map, Baidu Map, Weather
Health	Heart Rate, Fitness
Pay	BofA, Alipay

- $\mathcal{D}_{\mathbf{app}}$: We selected 16 commonly used smartwatch apps listed in Table 1 from categories such as health, music, communication, and navigation. For each app in the categories, we recorded 3 s of EM signals and repeated the collection 100 times.
- $\mathcal{D}_{\mathbf{act}}$: We selected 5 representative apps from the collected set and recorded EM signals for 5 different in-app activities. Each activity was recorded for 3 s and repeated 100 times.
- $\mathcal{D}_{\mathbf{dis}}$: We collected EM signals at different distances from the smartwatch, spanning from 0 cm to 20 cm, with increments of 2.5 cm, to analyze the signal variations across a range of proximities. Each recording lasted 10 s and was repeated 100 times per distance.
- $\mathcal{D}_{\mathbf{dev}}$: We collected usage data from four smartwatch devices while connected to a cellular network. Each device's dataset includes three key components: app recognition, in-app activity classification, and signal analysis at different distances.

These datasets, gathered from Apple Watch Ultra 2, Apple Watch 10, Xiaomi Watch S3, and Huawei Watch 4, are used to train models and evaluate their performance in distinguishing apps, identifying specific activities within apps, and assessing the impact of distance on signal variations. This comprehensive dataset enables cross-device comparisons and enhances the robustness of our analysis.

5.3 Hyperparameter Evaluation

In our hyperparameter optimization experiments for the CNN-LSTM architecture, we conducted a grid search across LSTM units (50–250) and dropout rates (0.1–0.5). Figure 6 illustrates two cross-sectional analyses of the hyperparameter tuning results: the left graph examines the effect of varying LSTM units with the dropout rate fixed at 0.3, while the right graph explores different dropout rates with the LSTM unit count fixed at 128, evaluating validation accuracy across different settings.

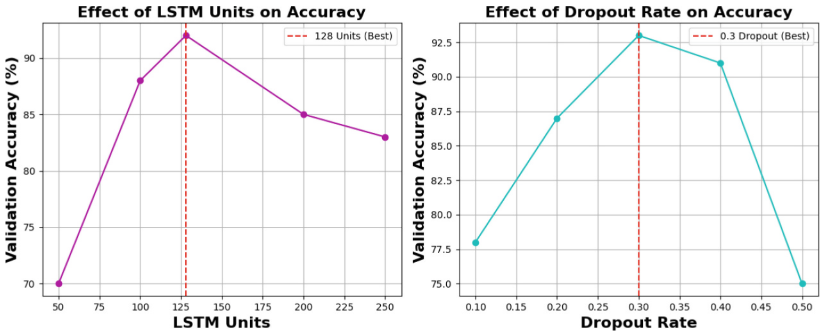
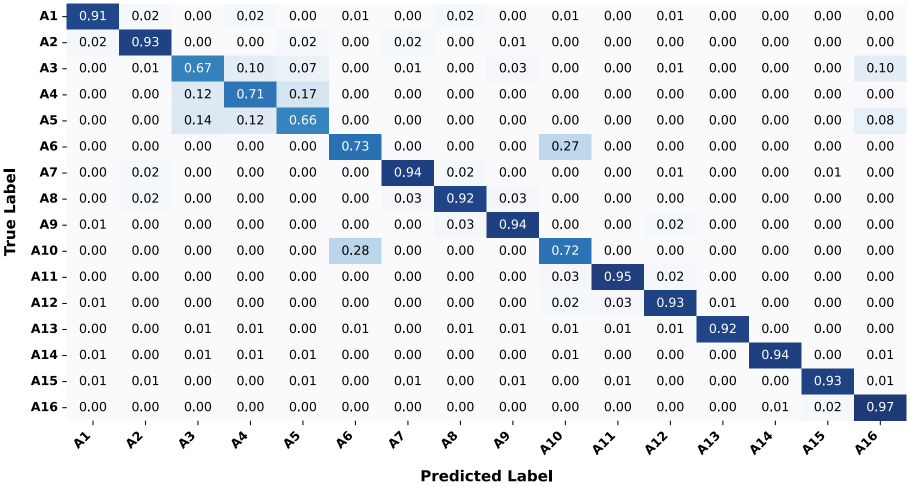


Fig. 6. Effect of Different Units and Dropout Rates

Our results indicated that 128 LSTM units yielded the highest validation accuracy, as additional units increased complexity without further improving performance, leading to a decline in validation accuracy. Similarly, a dropout rate of 0.3 achieved the best trade-off between regularization and performance, resulting in 93% validation accuracy. Higher dropout rates (0.4–0.5) led to excessive information loss, whereas lower dropout rates (0.1–0.2) provided insufficient regularization, reducing the model's generalization ability.

5.4 Effectiveness

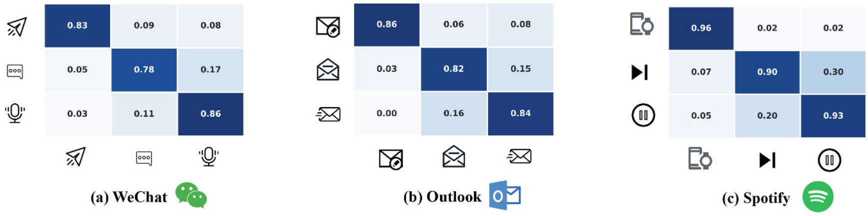


True Label \ Predicted Label	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
A1	0.91	0.02	0.00	0.02	0.00	0.01	0.00	0.02	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.00
A2	0.02	0.93	0.00	0.00	0.02	0.00	0.02	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A3	0.00	0.01	0.67	0.10	0.07	0.00	0.01	0.00	0.03	0.00	0.00	0.01	0.00	0.00	0.00	0.10
A4	0.00	0.00	0.12	0.71	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A5	0.00	0.00	0.14	0.12	0.66	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.08
A6	0.00	0.00	0.00	0.00	0.00	0.73	0.00	0.00	0.00	0.27	0.00	0.00	0.00	0.00	0.00	0.00
A7	0.00	0.02	0.00	0.00	0.00	0.00	0.94	0.02	0.00	0.00	0.00	0.01	0.00	0.00	0.01	0.00
A8	0.00	0.02	0.00	0.00	0.00	0.00	0.03	0.92	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A9	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.94	0.00	0.00	0.02	0.00	0.00	0.00	0.00
A10	0.00	0.00	0.00	0.00	0.00	0.28	0.00	0.00	0.00	0.72	0.00	0.00	0.00	0.00	0.00	0.00
A11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.95	0.02	0.00	0.00	0.00	0.00
A12	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.03	0.93	0.01	0.00	0.00	0.00
A13	0.00	0.00	0.01	0.01	0.00	0.01	0.00	0.01	0.01	0.01	0.01	0.01	0.92	0.00	0.00	0.00
A14	0.01	0.00	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.94	0.00	0.01
A15	0.01	0.01	0.00	0.00	0.01	0.00	0.01	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.93	0.01
A16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.02	0.97

Fig. 7. The Classification Performance of MagWatch on iWatch

Effectiveness of App Launching Recognition. The confusion matrix in Fig. 7 presents the effectiveness of our method in recognizing 16 different applications on iWatch Ultra 2 (used here for illustration) based on EM signals. To evaluate the classification performance, we utilize 80% of each application from the $\mathcal{D}_{\mathbf{app}}$ for training and assess the model using the remaining 20% data.

Overall, the recognition model achieves an average accuracy exceeding 90% across most applications, demonstrating its robustness in distinguishing different app usage scenarios. However, specific application groups, such as A3, A4, and A5 (navigation and mapping apps) and A6 and A10 (heart rate and fitness apps), exhibit lower classification accuracy. This is likely due to their reliance on the same underlying sensors (GPS for navigation apps and heart rate sensors for fitness-related apps), resulting in similar EM signal patterns that increase misclassification rates. Despite this challenge, our model is still capable of effectively distinguishing applications based on the type of sensors they utilize. This indicates that even when fine-grained app differentiation is difficult, EM signal analysis remains effective in *identifying the broader sensor usage patterns*, such as whether an app primarily interacts with GPS, heart rate sensors, or other components.



(a) WeChat (b) Outlook (c) Spotify

Fig. 8. Accuracy of In-App Activity Recognition Across Different Applications

Effectiveness of In-App Activity Recognition. To further validate the effectiveness of MagWatch, we conduct additional experiments by using $\mathcal{D}_{\textbf{act}}$ of three widely used applications—Spotify, WeChat, and Outlook—each involving three distinct activities. We then implement a CNN-based classification model to assess the feasibility of distinguishing fine-grained in-app activities based on their EM signatures.

Specifically, as shown in Fig. 8(a)-Fig. 8(c), in Spotify, we evaluate the recognition of skipping a song, pausing playback, and switching devices. In WeChat, we analyze the ability to classify receiving a message, sending a message, and listening to a voice message. Similarly, for Outlook, we investigate the recognition of receiving an email, sending an email, and editing an email.

The results show MagWatch's classification accuracy of 83.0%, 78.0%, and 86.0% for WeChat, 82.0%, 84.0%, and 86.0% for Outlook, and 90.0%, 93.0%, and 96.0% for Spotify, in recognizing the in-app activities elaborated above. These results validate the effectiveness of MagWatch, which not only identifies the launched application but also accurately recognizes fine-grained in-app activities.

Impact of Position and Distance. Figure 9 illustrates the impact of distance on the classification accuracy of app launching recognition. In practice, an attacker could place a disguised device near the target smartwatch at various distances to capture EM emissions. To evaluate this, we conducted experiments by positioning the attacking device at distances ranging from 0 cm to 20 cm at increment of 2.5 cm.

The results indicate that while the model maintains high accuracy at close range, the performance gradually declines as the distance increases. Beyond 7.5 cm, the accuracy drops significantly, and at 12.5 cm, it falls below 20%, making app recognition nearly ineffective. This decline, as consistently observed in the literature such as [16,17], suggests that as the distance increases, the EM

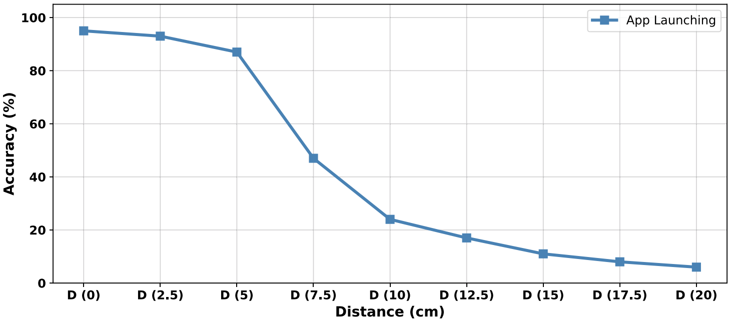


Fig. 9. Impact of Distance

signal disturbances become too weak to be reliably captured, limiting the effectiveness of remote attacks. This outcome highlights the practical constraints of EM-based side-channel attacks, where attackers must be in close proximity to achieve high classification accuracy. The results suggest that physical distance and shielding could serve as natural countermeasures to mitigate such privacy risks.

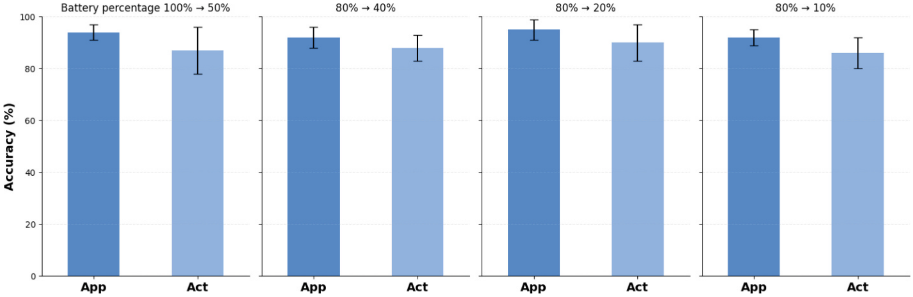


Fig. 10. Impact of Battery Level

Impact of Battery Level. To evaluate the impact of smartwatch battery levels on the performance of MagWatch, we conducted experiments under four different battery conditions: 60%, 40%, 20%, and 10%. The dataset for these experiments was collected from the Apple Watch Ultra 2 (used here for example), including both app usage data (denoted as "App" data in Fig. 10) and in-app activity data (denoted as "Act" data). The classification accuracy, as shown in Fig. 10, represents the mean accuracy across multiple trials and remains largely unaffected by battery fluctuations. One key factor contributing to this stability is the power-efficient architecture of modern smartwatches, which ensures consistent computational performance regardless of battery level. These findings underscore MagWatch's strong generalization capability across different battery conditions, reinforcing its robustness and reliability for electromagnetic-based inference. This ensures that MagWatch can be robustly operated under varying real-world scenarios without concerns about performance degradation due to battery fluctuations.

5.5 Analysis of Cold/Hot Start

Table 2. Classification Results of EM Signals Generated During COLD/HOT-Start

	kNN	SVM	CNN	CNN-LSTM
Cold	67%	75%	83%	93%
Hot	6%	9%	13%	16%

As stated in [18], cold start and hot start exhibit distinct characteristics during the application launch process. Cold start refers to launching an application from scratch, requiring CPU initialization, memory allocation, and data loading. This process generates more prominent EM signal characteristics, making it easier to identify. In contrast, a hot start occurs when an application is partially loaded in the background, allowing the system to restore data from cache with reduced CPU activity. This results in weaker EM signal characteristics, which makes identification more challenging.

This phenomenon is not limited to smartphones; it also applies to smartwatches and other wearable devices, as demonstrated in Table 2. The table presents the results of applying various classification models (kNN, SVM, CNN, CNN-LSTM) to smartwatch EM emission data collected from cold start versus hot start scenarios. It clearly shows that classification accuracy is high in cold start scenarios, particularly with CNN-LSTM, while accuracy is significantly lower in hot start scenarios across all models. Given that smartwatches typically use more aggressive power management strategies, the result in Table 2 is expected, as the differences in resource scheduling between cold and hot starts are even more pronounced in smartwatch devices.

6 Discussion

In this section, we discuss the limitations of MagWatch, the potential defense countermeasure, and the future work.

Limitations. We have implemented MagWatch to demonstrate the feasibility of electromagnetic (EM) side-channel inference for smartwatch applications. While the results are promising, several limitations remain in the current work.

First, MagWatch is evaluated in controlled experimental settings where the smartwatch remains stationary during app interactions. However, we have not fully explored its performance in dynamic scenarios, such as users wearing the smartwatch while walking or performing other activities. Theoretically, MagWatch could still capture meaningful EM traces in these cases by refining signal preprocessing techniques and adapting feature extraction methods. However, movement introduces additional noise and variability, making real-time inference more challenging.

Second, our experiments are conducted under relatively close-range and controlled environmental conditions to validate the feasibility of EM-based inference. The accuracy of MagWatch may degrade as the distance between the sensor and the smartwatch increases due to EM signal attenuation. To extend its applicability, further studies are required to refine the model to accommodate varying distances and external interference.

Countermeasures. Several countermeasures can help mitigate EM information leakage from smartwatches. One approach is physical shielding with ferromagnetic materials to reduce magnetometer interference, though this is often overlooked due to design constraints prioritizing size and weight. Increasing physical distance(in Sect. 5.4) can naturally reduce privacy risks. Detecting and excluding nearby devices that may capture EM signals could further enhance protection. Lastly, current EM emission regulations may be too lax; enforcing stricter standards could prevent adversaries from inferring user behavior through app usage patterns.

Future Work. For future work, we plan to explore real-world deployment scenarios, considering factors such as user motion, device orientation, and environmental EM noise. Additionally, we aim to improve the generalization of MagWatch by integrating adaptive learning techniques to enhance robustness across different smartwatch models and operating conditions.

7 Conclusion

This paper explores and demonstrates the feasibility of EM-based side-channel attacks towards smartwatches, where EM emissions generated during smartwatch operations can be captured to reveal both app usage and in-app activities without requiring direct device access. We have designed and implemented MagWatch, a novel non-intrusive attack that utilizes wavelet transform for signal processing and a CNN-LSTM model to identify applications and in-app activities, achieving up to 90% accuracy across multiple smartwatch models. To the best of our knowledge, this is the first attack targeting smartwatch EM emissions to infer user privacy and behavior patterns related to app interaction/navigation.

Acknowledgment. Drs. Xiaoyan Sun and Jun Dai are supported by NSF DGE-2409851. Dr. Jun Dai is also supported by NSF DGE-1934285/2403603.

References

1. Amodei, A., et al.: Experimental analysis of side-channel emissions for IOT devices activities' profiling. In: 2023 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT), pp. 42–47 (2023). https://doi.org/10.1109/MetroInd4.0IoT57462.2023.10180188
2. App Store: Sensor Logger. https://apps.apple.com/us/app/sensorlogger-csv-export/id15052035. Accessed 22 Feb 2025
3. Chen, X., Chen, W., Liu, K., Chen, C., Li, L.: A comparative study of smartphone and smartwatch apps. In: Proceedings of the 36th Annual ACM Symposium on Applied Computing, pp. 1484–1493 (2021)
4. Cheng, Y., et al.: Magattack: guessing application launching and operation via smartphone. In: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp. 283–294 (2019)
5. Chuah, S.H.W., Rauschnabel, P.A., Krey, N., Nguyen, B., Ramayah, T., Lade, S.: Wearable technologies: the role of usefulness and visibility in smartwatch adoption. Comput. Hum. Behav. **65**, 276–284 (2016)
6. Farge, M., et al.: Wavelet transforms and their applications to turbulence. Annu. Rev. Fluid Mech. **24**(1), 395–458 (1992)
7. Fu, Y., Yang, L., Pan, H., Chen, Y.C., Xue, G., Ren, J.: Magspy: Revealing user privacy leakage via magnetometer on mobile devices. IEEE Trans. Mob. Comput. (2024)
8. Ibrahim, O.A., Sciancalepore, S., Oligeri, G., Pietro, R.D.: Magneto: fingerprinting USB flash drives via unintentional magnetic emissions. ACM Trans. Embed. Comput. Syst. **20**(1) (2020).https://doi.org/10.1145/3422308
9. Ioffe, S., Szegedy, C.: Batch normalization: accelerating deep network training by reducing internal covariate shift. In: International Conference on Machine Learning, pp. 448–456. PMLR (2015)
10. Isakadze, N., Martin, S.S.: How useful is the smartwatch ECG? Trends Cardiovasc. Med. **30**(7), 442–448 (2020)
11. Jat, A.S., Grønli, T.M.: Smart watch for smart health monitoring: a literature review. In: International Work-Conference on Bioinformatics and Biomedical Engineering, pp. 256–268. Springer (2022)
12. Kang, H., Jung, E.H.: The smart wearables-privacy paradox: a cluster analysis of smartwatch users. Behav. Inf. Technol. **40**(16), 1755–1768 (2021)
13. Karim, F., Majumdar, S., Darabi, H., Chen, S.: LSTM fully convolutional networks for time series classification. IEEE Access **6**, 1662–1669 (2017)
14. Kim, J.W., Lim, J.H., Moon, S.M., Jang, B.: Collecting health lifelog data from smartwatch users in a privacy-preserving manner. IEEE Trans. Consum. Electron. **65**(3), 369–378 (2019)
15. Maxwell, J.C.: The Scientific Papers of James Clerk Maxwell..., vol. 2. University Press, Cambridge (1890)
16. Ni, T., et al.: Exploiting contactless side channels in wireless charging power banks for user privacy inference via few-shot learning. In: Proceedings of the 29th Annual International Conference on Mobile Computing and Networking, pp. 1–15 (2023)
17. Ni, T., et al.: Uncovering user interactions on smartphones via contactless wireless charging side channels. In: 2023 IEEE Symposium on Security and Privacy (SP), pp. 3399–3415. IEEE (2023)
18. Pan, H., et al.: Magthief: stealing private app usage data on mobile devices via built-in magnetometer. In: 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1–9. IEEE (2021)

19. Qiao, Y., Zhao, X., Yang, J., Liu, J.: Mobile big-data-driven rating framework: measuring the relationship between human mobility and app usage behavior. IEEE Network **30**(3), 14–21 (2016)
20. Reeder, B., David, A.: Health at hand: a systematic review of smart watch uses for health and wellness. J. Biomed. Inform. **63**, 269–276 (2016)
21. StraitsResearch: Report: Smartwatch market trends, growth, and forecast 2033. https://straitsresearch.com/report/smartwatch-market. Accessed 06 Jan 2025
22. Tu, Z., et al.: Your apps give you away: distinguishing mobile users by their app usage fingerprints. Proc. ACM Interact. Mob. Wearable Ubiquit. Technol. **2**(3), 1–23 (2018)
23. Udoh, E.S., Alkharashi, A.: Privacy risk awareness and the behavior of smartwatch users: A case study of indiana university students. In: 2016 Future Technologies Conference (FTC), pp. 926–931 (2016). https://doi.org/10.1109/FTC.2016.7821714
24. Udoh, E.S., Alkharashi, A.: Privacy risk awareness and the behavior of smartwatch users: a case study of Indiana university students. In: 2016 Future Technologies Conference (FTC), pp. 926–931. IEEE (2016)
25. Williams, M., Nurse, J.R., Creese, S.: (smart) watch out! encouraging privacy-protective behavior through interactive games. Int. J. Hum Comput Stud. **132**, 121–137 (2019)
26. Wu, J.: Introduction to convolutional neural networks. national Key Lab for Novel Software Technology. Nanjing University. China **5**(23), 495 (2017)
27. Yoon, H.S., Shin, D.-H., Kim, H.: Health information tailoring and data privacy in a smart watch as a preventive health tool. In: Kurosu, M. (ed.) HCI 2015. LNCS, vol. 9171, pp. 537–548. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21006-3_51
28. Zhu, Z., Pan, H., Chen, Y.C., Ji, X., Zhang, F., You, C.W.: Magattack: remote app sensing with your phone. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, pp. 241–244 (2016)