Internet of Things device authentication via electromagnetic fingerprints

Artur Souza | Ivo Carlson | Heitor S. Ramos | Antônio A.F. Loureiro | Leonardo B. Oliveira

Abstract
We quickly approach a future where Internet of Things (IoT) devices are the norm. In this scenario, humans are surrounded by a multitude of heterogeneous devices that assist them in almost every aspect of their daily routines. The realization of this future demands strong authentication guarantees to ensure that these devices are not abused and that their users are not endangered. However, providing authentication for these systems is challenging due to the high heterogeneity of IoT applications. In this paper, we first review several IoT application scenarios and promising authentication methods for each. We identify the key characteristics of each IoT application scenario, present the strengths and weaknesses of prominent authentication methods from the literature, and review which authentication methods have been proposed in the literature for each application. Then, we present a novel authentication method for IoT based on electromagnetic noise. The key advantage of electromagnetic noise is that any electronic device intrinsically generates electromagnetic noise during normal operation. We extract features from these electromagnetic emanations and use machine learning algorithms to identify devices based on these features. Our method achieves 77% accuracy when identifying devices among a set of seven devices.

Keywords
Internet of Things, authentication, device fingerprint

1 | INTRODUCTION
The Internet of Things (IoT) denotes a paradigm where users are surrounded by computing elements and sensors attached to all sorts of everyday objects. This enables a series of new and ubiquitous applications that impact every aspect of users’ day-to-day routine. Example applications range from temperature, humidity, and growth sensors coupled to crops, to everyday wearables that connect to a smartphone to retrieve and display emails, text messages, and biometric information. Figure 1 shows an example of IoT in the context of vehicular networks. In this case, the computing elements (vehicles, road infrastructure, and even the user’s personal devices) interoperate to improve traffic efficiency and safety (cf, Section 2.2), accuracy when identifying devices among a set of seven devices.
The ubiquitous nature of the IoT, however, brings forth a series of security concerns. In this scenario, computing elements are ubiquitous and track every aspect of users’ daily routines. It means that devices have access to vast amounts of sensitive information about its users, which, in turn, raises privacy concerns. Besides, the rapidly growing number of devices in these systems mean these networks will be massively larger than other networks, meaning adversaries have several more targets to exploit. A good example of the risk of leaving these systems unprotected is the recent Mirai botnet attack.

Notably, authentication is a critical security property for IoT systems. Authentication ensures that devices can verify the source (source authentication) and content (data authentication) of messages received. It forms the basis for secure communication channels since it allows devices to trust messages exchanged. In IoT systems, authentication allows devices to communicate and cooperate in providing their intended applications safely.

The main contribution of this paper is twofold. Firstly, we review existing IoT application scenarios and authentication solutions. We discuss several IoT computing applications, highlight their defining characteristics, and how these characteristics impact security solutions. We then review several authentication solutions that are promising for the devices and applications often found in IoT. We conclude our review by presenting some of the authentication solutions currently proposed for each IoT application scenario and which authentication methods they rely on. Finally, we present a proof of the concept of the possibility to find intrinsic signatures for IoT devices based on electromagnetic emanations. Previous work has shown that electronic devices naturally emanate electromagnetic noise due to the electric current passing through the devices’ circuits. We analyze the electromagnetic noise generated by multiple devices and show that it is possible to identify a specific device based on the intricacies of the noise generated. Further, we show that it is possible to distinguish even between devices of the same make and model. Our results show that we can identify a specific device with up to 77% accuracy and believe there is still room to improve (cf, Section 7).

This paper is organized as follows. Section 2 presents a review of existing IoT applications. Section 3 presents existing authentication strategies. Section 4 identifies promising authentication directions for each application scenario. Sections 5 and 6 describe the EM emanations, how it can be used as an authentication method and the results we obtained. Finally, in Section 7 we present our next steps and conclude this work.

2 | IOT SCENARIOS

The defining characteristic of the IoT is that computing elements are coupled to everyday objects to allow them to communicate and interoperate to provide applications. IoT enables applications for almost every aspect of users’ daily routines.
TABLE 1 Summary of pervasive computing application scenarios

| Application | Advantages | Disadvantages |
|-------------|------------|---------------|
| WSN         | • Easy to bootstrap | • Resource constrained |
|             | • Homogeneous devices | • Limited power supply |
|             | • Resourceful base stations | • Easy adversary access |
| V2X         | • Sustainable power source | • Very high mobility |
|             | • Little resource constraint | • Time-sensitive applications |
|             | • Predictable mobility | • Massive network size |
|             | • Privacy concerns | • Intermittent connectivity |
| Wearables   | • Possible biometric authentication | • Privacy concerns |
|             | • Resourceful devices as managers | • Resource constrained |
|             | • Controlled environment | • Limited power supply |
| CPHS        | • Users as possible resource | • Heterogeneous applications |
|             | • Physical authentication factors | • May require user interaction |
|             | | • Physical world complications |

In this section, we present the most prominent pervasive application scenarios and review their challenges for security solutions. Table 1 shows a summary of the challenges for IoT authentication solutions presented in this section.

2.1 Wireless sensor networks

Wireless sensor networks (WSNs) comprises a broad spectrum of IoT where the computing elements are sensors distributed in a wide area to monitor physical and environmental conditions. These sensors are often linked to a base station to which they report the sensed data. Applications of WSNs vary greatly based on what is being sensed and where, for instance, sensors may be deployed in crops to monitor humidity and soil conditions or throughout a city to monitor its levels of air pollution.

There are several limitations to the development of authentication solutions for WSNs. First, sensors are often severely resource-constrained and have no sustainable power source. It means that authentication solutions for WSNs must be lightweight so that computations can be done on time with minimal impact on the sensor’s lifespan. Besides, sensors are often deployed in unsupervised environments, which makes it easier for adversaries to physically access the device and attempt to physically extract information (including cryptographic material) from the device. On the other hand, one advantage of WSNs is that sensors are all bootstrapped in the base station before being deployed. It facilitates the deployment of cryptographic material inside the sensor.

2.2 Vehicle-to-everything

Vehicle-to-everything (V2X) comprises the communication between vehicles and any other interlocutor. V2X encompasses communication patterns like vehicle-to-vehicle (V2V or VANETs), vehicle-to-infrastructure, or vehicle-to-roadside (V2I or V2R), vehicle-to-pedestrian (V2P), and vehicle-to-device (V2D). V2X applications can be classified into (i) safety applications, (ii) entertainment applications, (iii) efficiency applications. Examples of the former include forward collision warning, electronic emergency brake lights, and wrong-way driving warning. Entertainment applications include media streaming, car-to-car messaging, and local touristic information. The latter refers to applications like congestion control, improved location systems, and improved route planning. Finally, V2X is also the cornerstone for intelligent transportation systems (ITS), which are expected to improve public transportation services greatly.

There are several complications to the design of authentication solutions for V2X. The first is the vehicles’ high-speed mobility, which means applications are very time-sensitive and, therefore, authentication must incur in minimal
time overhead.\textsuperscript{22} The second is the network’s massive size, VANETs are likely to be one of the largest mobile ad hoc networks,\textsuperscript{22} this imposes burdens in the deployment and management of cryptosystems and incurs in computational overheads as it means vehicles will have to authenticate several other nodes in the network.\textsuperscript{23} Third, V2X suffers from intermittent connectivity as vehicles’ will sometimes move to areas without connectivity like highways or rural areas,\textsuperscript{22} which means solutions cannot rely on a central entity available at all times to manage the cryptosystem. Finally, privacy is a major concern in V2X as information about the driver’s identity, or location may facilitate the action of adversaries and put the driver at risk.\textsuperscript{24} Despite the above complications, V2X networks present some advantages over other scenarios. The first being that vehicles carry a rechargeable battery, meaning energy overheads are not a serious concern. Another advantage is that vehicles are not severely resource-constrained, meaning they can afford to run more expensive cryptographic algorithms, especially for applications that are not time sensitive.\textsuperscript{22}

\section*{2.3 Wearables and IMDs}

Wearable and Implanted Medical Devices (IMDs) are devices attached to the user’s body.\textsuperscript{25,26} Although there is a fundamental difference in purpose between Wearables and IMDs, we grouped these two scenarios due to their similarities for authentication. The core idea in this scenario is that devices are attached to users’ bodies, and they attempt to insert the user himself as a component in the pervasive paradigm.\textsuperscript{26} These devices also act as body sensors, monitoring physical conditions like body temperature, movement, and health conditions (eg, heartbeats).\textsuperscript{25}

Because of the amount of sensitive information stored in these devices, privacy is a paramount concern.\textsuperscript{27} Illegitimate access to these devices allow adversaries to access the user’s private information (eg, emails, messages), body conditions (eg, temperature, movement), and even monitor medical conditions (eg, presence of pacemakers).\textsuperscript{25,27} At the same time, these devices often have low computational power and rely on other, more powerful devices to perform computations.\textsuperscript{28}

There are also a few similarities between Wearables/IMDs and previous application scenarios. For instance, similar to sensors in WSNs, these devices have low computational power and have no sustainable energy source, although wearable devices can be more easily recharged. Besides, these devices sometimes require direct user involvement, which concurrently brings new challenges and possibilities for these applications. These devices can also rely on the presence of other powerful devices (to which they report data) to perform heavier operations and are often in very controlled environments (worn by the users or attached to their bodies), which complicates the action of adversaries.

Unlike previous applications, however, wearables and IMDs are always in contact with the user’s body. It creates possible new venues for authentication based on the user’s physical information. For instance, a pacemaker can use information about the heartbeat to authenticate,\textsuperscript{25} while fitness trackers can use gait recognition\textsuperscript{29} for authentication.

\section*{2.4 Cyber-physical-human systems}

Cyber-Physical-Human Systems (CPHSs) is a rendezvous between cyber systems, the physical world, and human beings. Cyber-Physical-Systems (CPSs) refers to the integration of the cyber and physical worlds.\textsuperscript{30} CPHSs, in turn, put people in the loop by making them not only a user of CPSs but also part of them.\textsuperscript{31} CPHS applications are highly diverse, including cyber-physical medical systems, critical infrastructure control, workspace automation, among many others.\textsuperscript{32}

The high diversity of CPS, and consequently CPHS, make the conception of authentication solutions a challenge since resources in one context may not be available in others. However, two characteristics are staple for CPHS. First of all, humans are directly involved in CPHS applications; for instance, the workers in a workspace or the doctors in cyber-physical systems.\textsuperscript{33} Further, CPHS aim at integrating the cyber and physical worlds, meaning environmental conditions will always be a central piece of these systems. The integration of characteristics of the physical world in the authentication is a promising venue for CPHS.

\section*{3 Authentication Methods}

There are several different methods for achieving the authentication of users and data. Each of these methods has its advantages and disadvantages, making it more or less suitable for each application scenario. In this section, we review some of the most prominent authentication methods in the literature.
3.1 Elliptic curve digital signature algorithm

The elliptic curve digital signature algorithm (ECDSA) is a more viable alternative to the traditional DSA.\textsuperscript{34} The ECDSA is much more efficient in both storage and computation than the traditional DSA as it requires smaller parameters to sign, and the signature generation is significantly faster.\textsuperscript{35} The ECDSA still requires a certification method, like traditional digital certificates.

To avoid the high costs of digital certificates, Brown et al. have proposed a novel certification scheme for ECDSA called Implicit certificates.\textsuperscript{36} The main idea behind implicit certificates is that the user's public key and certificate are combined in a single element, called the public key reconstruction data. Implicit certificates are considerably smaller and faster to verify than traditional certificates.\textsuperscript{36}

3.2 Short signatures

The Boneh-Lynn-Shacham short signature scheme (BLS)\textsuperscript{37} is a certificate-based signature scheme that generates signatures that are much shorter than DSA and ECDSA signatures.\textsuperscript{35} The small size of the signatures generated is the main strength of BLS. Another interesting aspect of BLS is that its computational overhead is asymmetric: verifying signatures is much more expensive than generating them. BLS is well-suited for applications where resource-constrained devices generate signatures but verified by powerful devices (eg, Section 4.1). However, these signatures are still certificate-based, meaning they suffer from the complexity and high overhead of digital certificates.

3.3 Identity-based cryptography

The idea behind identity-based cryptography (IBC) was first proposed by Shamir,\textsuperscript{38} but was only made possible with the advent of pairing-based cryptography.\textsuperscript{39} The key idea of IBC is that the user's keys can be derived directly from the user's identity in the system (eg, his e-mail address). It means that the user's key is intrinsically bound to the user, which, in turn, dismisses the need for other certification methods like digital or implicit certificates. Since IBC dismisses certification, the cryptosystem incurs lower storage and communication overheads and simplifies key management.

IBC, however, is not a panacea. In IBC, private keys are not generated by their respective owners but rather by a Private Key Generator (PKGs), a central entity in the cryptosystem. It means that the PKG must be trustworthy since it can impersonate any user in the system.\textsuperscript{40} It is the well-known key escrow problem of identity-based systems. Besides, the centralized key generation creates a significant vulnerability in the system if the PKG is compromised. Finally, bilinear pairings, the mathematical foundation of IBC, are computationally expensive to compute, consequently, so are cryptographic operations in IBC.

3.4 Certificateless schemes

The certificateless scheme\textsuperscript{41} was proposed as a middle ground between IBC and traditional Public-Key Infrastructure (PKI). The cryptosystem is similar to IBC in that it dismisses certification schemes. However, it avoids the key escrow problem by splitting the key generation between the user and central authority in the cryptosystem. The main advantage of certificateless is that keys can be easily shared and verified, without the key escrow problem. One drawback of the Certificateless approach is that public keys can no longer be easily derived from the user's identity like in IBC. Instead, public keys must be explicitly made public by their owners. Besides, certificateless is also based on expensive bilinear pairings.\textsuperscript{42}

3.5 Attribute-based cryptography

Attribute-based cryptography (ABC)\textsuperscript{43} is an extension of IBC that focuses on attributes instead of identities. In ABC, users' keys are derived from a set of attributes they possess, rather than their identifier. In this setup, users no longer sign messages to prove their identities. Instead, users prove they possess a set of attributes from the system. ABC is particularly
well-suited for access-control policies, especially attribute-based access control. As an extension of IBC, however, ABC also suffers from the key escrow problem and bilinear pairings.

### 3.6 Hash-based signatures

Hash-based signatures (HBSs) are signature schemes based solely on cryptographic hash functions. HBSs has gained much attention in the last decade because of their high efficiency and resistance to quantum cryptanalysis. HBSs are often classified into two categories: one-time signature schemes (OTS) and multitime signature schemes (MTS). As their name suggests, in OTS, private keys can only be used to sign messages once and must then be renewed, while in MTS, private keys can be used to sign a large, but still limited, number of messages before being renewed. The need for constantly renewing private keys can become a burden in HBS solutions. Another disadvantage of HBSs is that they also require some form of certification, much like DSA and ECDSA. Unlike ECDSA, however, there are no cheaper certification alternatives for HBS, so they rely on expensive digital certificates.

### 3.7 Group signatures

In group signature schemes, users sign messages to prove they are a valid member of a group, instead of proving their identity in the system. Group signatures are always anonymous in the sense that other users cannot know who generated a signature. In these schemes, a group manager is responsible for generating and distributing keys to other users. The group manager is also responsible for adding or removing users from the group. Unlike the other members of the group, the group manager can "open" a signature to reveal its signer. It is used to identify and remove malicious users in the group.

Group signatures have the clear advantage of being anonymous and simple, as each user need only know the group generation and verification keys. However, the group manager has a significant overhead to manage the devices, especially if the group is highly dynamic. Also, since all devices use the same group key, a single device that is compromised means the entire group must be redone.

### 3.8 Ring signatures

Ring signatures are an extension of group signature schemes. Much like in group signature schemes, users sign messages as one of the members of a group of users. However, in-ring signature schemes, the group need not be truly formed, and the other users need not be aware of the group. The user may choose a set of users and sign a message as one of the set’s users.

There are two main differences between group signatures and ring signatures. The first is that ring signature schemes do not need group managers since the groups are formed by the user himself when generating the signature. The second is that, since no group manager is available, no one can trace back the generator of a signature. Therefore the signatures are completely anonymous.

Ring signatures are interesting replacements for group signatures for scenarios where there is no suitable candidate for the group manager or when groups are challenging to form. One drawback of ring signatures is that they require a previous set up of public/private key pairs, and the efficiency of the ring signature depends on the underlying cryptosystem.

### 3.9 Mesh signatures

Mesh signatures are an extension of ring signatures. Like its precursor, mesh signatures allow users to sign a message anonymously, providing only a list of possible signers. Mesh signatures, however, possess two differences when compared to ring signatures. First, mesh signatures allow any individual to be included in the list of possible signers, even if the user's real public key is unknown. Second, mesh signatures provide threshold signing. That is, messages may be signed as a subset of members of the group of possible signers.

One drawback of mesh signatures, however, is that it enables users to collude to generate signatures that each of the users alone would not be able to generate. It could allow users to collude to bypass certain system conditions or to satisfy
signer requirements. For example, a computer science student could collude with an engineering professor to sign a message as a computer science professor.

### 3.10 Physical signatures

Physical signatures are signatures based on features of the physical world. These signatures are strong complements to cryptographic schemes in applications where there is constant interaction with the physical world. These signatures can be either intrinsic or extrinsic, depending on how they are generated. Intrinsic signatures are generated from inherent characteristics from devices, channels, or the physical environment. For instance, Wu et al have proposed authenticating media through the Electric Network Frequency (ENF) of the place where the media was recorded.

On the other hand, extrinsic signatures are signals and data that are intentionally injected and monitored in a system. For instance, physical-layer watermarks. Previous works have investigated the random injection of extrinsic signatures guided by cross-layer system modeling and cryptographically random number generation.

### 4 AUTHENTICATION FOR IOT APPLICATIONS

In this section, we review authentication proposals for each of the application scenarios presented in Section 2.

#### 4.1 Wireless sensor networks

The biggest impediment to authentication for WSNs is the inherent resource constraint of the sensors. It means that authentication solutions must rely on methods that require low computing resources, low bandwidth, and low energy consumption. To achieve this, proposed solutions rely on cheaper authentication tools such as short signature schemes, group signatures, IBC, or even traditional symmetric cryptography. These approaches leverage the presence of the resourceful base station to bootstrap and manage the necessary cryptosystems. Solutions for WSNs must also account for the vulnerability of sensors to physical attacks. It is usually addressed through clever key management solutions or secure hardware modules.

#### 4.2 Vehicle-to-everything

Several authors have proposed security solutions based on PKI in the early days of vehicular communication. Most prominently, Raya and Hubaux devise and evaluate two PKI architectures for PKI, based on digital signatures and a set of anonymous keys that the vehicle must renew with a central authority periodically. However, the massive number of nodes (vehicles, roadside units, and pedestrians) and fast communication required from V2X renders these PKI solutions inadequate due to their high overheads.

Solutions based on group signatures are another common strategy in V2X. In these solutions, roadside units often play the role of group authority, managing the group keys. Hao et al, for instance, propose a distributed group signature scheme, where only a subset of the vehicles verifies message signatures based on proximity to message source. Since only a few vehicles verify each message, the overall cost of authentication is reduced. Islam et al propose a password-based group signature scheme, where a password is used to control group key generation and new vehicles joining the group signature scheme.

Solutions based on other cryptosystems have also been proposed to simplify management and lessen authentication costs. Zhang et al, for instance, propose an IBC solution with distributed central authorities, to prevent the key escrow problem. In their solution, a central authority and roadside units generate the IBC keys of vehicles together but independent of one another. Thus, no one but the vehicle knows the full private key. In a similar vein, Horng et al have proposed a certificateless-based solution, to leverage the benefits of IBC while avoiding the key escrow problem. At last, Shen et al have proposed a solution based on chameleon hash signatures, ensures authentication with nonrepudiation while maintaining the vehicles’ privacy.
4.3 Wearables and IMD

The predominant strategy in wearables and IMDs is to use physical signatures. The constant contact of these devices with the user’s body enables several different physical authentication venues. Rostami et al., for instance, propose using electrocardiogram data to authenticate IMDs to external medical devices. Similarly, Venkatasubramanian et al. propose using physiological signals to generate cryptographic keys, that are then used together with traditional symmetric cryptographic algorithms. As a different type of physical signature, Kalamande et al. use distance to authenticate wearable devices. Their solution uses the received signal strength (RSS) of devices to determine whether two devices are close during authentication.

There are still authors that propose purely cryptographic authentication solutions. He and Zeadally propose an authentication solution for IMDs based on a modified IBC cryptosystem that dismisses bilinear pairings. Liu et al. propose an authentication solution for wearables and IMDs based on certificateless cryptography. At last, Almulhim and Zaman propose a solution based on group signatures and ECC. Although normally more expensive, cryptographic solutions do not need specific sensors for authentication, a common drawback of some physical signature-based schemes.

4.4 CPHS

Authentication for CPHS often seeks to leverage the intrinsic connection to the physical world. Vuppala et al., for instance, propose an authentication scheme based on “device fingerprints”, intrinsic device characteristics extracted from device features like CPU loads, memory usage, and signal strength. Mo et al. propose adding noisy watermarks to a CPHS system and later checking this watermark to strengthen authentication. The work of Vuppala et al is an example of an intrinsic physical signature being used for authentication, while Mo et al is an example of an extrinsic physical signature.

A few proposals also exist for authentication in specific CPHS scenarios. As an example, Chakravarty et al. has proposed two authentication protocols for smart grids based on symmetric cryptography. Their solution seeks to provide long-term security by adding protocols to replace or update cryptographic material securely. More recently, Neto et al. have proposed an authentication solution for smart homes based on IBC and ABC. ABC is used to enforce an attribute-based access control system, where users, via their smartphones, can access home appliances based on their attributes.

5 ELECTROMAGNETIC AUTHENTICATION

Researchers found that each network produced a different pattern of interference when analyzing the jamming caused in recorded multimedia by a power distribution network. Using those patterns they were able to link each multimedia to its geographic location of recording, showing that multimedia signals often can carry useful underline information that comes from interferences during the recording.

Knowing that signals can carry information about the state of the physical world during the moment of recording, Oliveira et al. proposed to use the physical world as a source of signatures. That approach would be more robust once it carries information about time and location.

Covert/side-channels is a side effect of the current that flows in a processor. When a processor executes a command, it has an electric current flowing in its components. That current varies depending on the data previously stored in it, and, therefore, carries information about the processor contents. As this current creates an electromagnetic wave that can be noticed by nearby sensors, it can be treated as a potential leak source.

It is known that all electronic devices emanate electromagnetic noise when an electric current goes through their circuits. In that same paper, the researchers mention that the processor leaks a different signal when executing each function. Hence, an attacker can know what is being processed without any connection with the device, just by analyzing those electromagnetic emanations.

In another line, an important note about electronic devices is their hardware-level divergence. Even devices that share the same model manufacturer and even production batches are not identical in all aspects. Small variations in the resistance, shape, and paths of the transistors used in the process may lead to a difference of the current flowing in the device, making that current differ for the current in another device. As the electromagnetic wave is due to the current in a circuit, that wave will be different for two devices.
When processing a program that consists of a loop that repeatedly calculates upon random numbers using functions that leak more information we were able to see a peak of operation, knowing that the time of execution of the program’s loop matches the period of the generated EM wave.

When exploiting both the group of functions and the differences that come from the manufacturing process, Devadas et al. were able to map and categorize which one of those functions are more discernible and able to create signals that contain features that are specific of the hardware. They called that group physical unclonable function (PUF). A PUF will generate a pair of challenge and response (c-r) that, due to the hardware level differences, are unique for the device that runs the function.

Since PUF generates a distinguishable result, researchers that were concerned about the counterfeiting problem on integrated circuits (IC) and on FPGA boards attempt to link a signal to a device based on what was expected. They used a probe to observe the FPGA and analyzed if it was close to what was expected. They performed a probabilistic analysis that observed some technical features such as pikes and amplitudes.

Using a similar approach, Zhu et al. proposed a method of authentication for edge computing. They placed a coil close to the SMPS that was linked to the edge host. This signal that represents the power along the time was collected on a database. After that, a set of features vastly used for machine learning using an Support Vector Machine (SVM) classifier was extracted from the previously recorded signal. The main idea is to compare the signal passing by cloud with the signal that has previously passed and has already proved legitimacy.

Our novel authentication method presumes that each device’s signal will be different due to hardware-level distinction. It extracts a device fingerprint from these electromagnetic emanations and uses this fingerprint to authenticate devices. We propose to use these fingerprints as an intrinsic physical signature scheme. The advantage of this method is that it does not interfere with the device’s everyday operation, incurring no overheads. It also pairs nicely with existing cryptographic based authentication solutions, for example, the fingerprint can be extracted when a device generates a digital signature or authentication code.

Our authentication solution has two asymmetrical roles; one device acts as the authenticator and another as the verifier. The authenticator can be any computing device; in our case, we use an Arduino to represent a generic (slightly constrained) IoT device. The verifier, on the other hand, must be capable of capturing and processing electromagnetic

![FIGURE 2](image-url) Our proposed electromagnetic authentication method. Here, the recording device is authenticating the target device via the electromagnetic noise generated by the target device
devices. We use a software-defined radio module\(^1\) attached to a computer to capture and process the signal. An SDR is a radio that has software to act as components such as amplifiers and filters. This kind of module was chosen due to it is relatively low cost and simple operation. The fact that an SDR operates based on the frequency of the signal also was considered alongside with the possibility to implement components such as filters to improve the signal collection, whenever it is necessary. Figure 2 illustrates our setup.

We can extract features and define a fingerprint for the device from the intrinsic differences in each device’s electromagnetic emanation. We define a device’s fingerprint via a combination of 12 features from the device’s electromagnetic emanation, following the work of Das et al.\(^7,8\) These features are divided into nine time-domain features (eg, the signal’s mean amplitude) and three frequency-domain features (eg, the signal’s spectral centroid). The complete list of features used is shown in Table 2.

We then use a machine-learning algorithm to identify a device based on its fingerprint. We experiment with SVMs,\(^8,4\) and Random Forests (RF)\(^8,5\) for the classifier, but note that our approach is not limited to these classifiers. The details of our experimental setup, dataset construction, and model implementation are presented in Section 6.

### 6 | EVALUATION

We evaluate our solution following the setup illustrated in Figure 2. We use seven Arduino Mega 2560 as our IoT devices, an RTL2832U SDR module to capture the electromagnetic signals and a Dell Vostro notebook as the verifier. We record the signal from five different distances, ranging from 10 to 50 centimeters. The radio center frequency was set to 32MHz, the peak of its operation. All of the signals were recorded in a laboratory room, where noise from multiple other devices was also present. All signals were recorded under the same conditions.

The data for each device was generated by recording the signal continuously for a period, then splitting the signal into smaller fragments. We record the signal of each device for 10 seconds, then split this signal into smaller fragments. Each of these fragments corresponds to an entry in our dataset. We experiment with 0.1 and 0.05 second fragments in our scenarios.

We also experimented with pre-processing filters to assess the impact of noise. We evaluate the performance of the classifiers with the raw signals and with pre-processed signals. The pre-processed signals were filtered with a low pass filter with a cut-off of 34.5 MHz, the highest operative frequency found on the devices. We then extracted the features using a Python script to generate the fingerprint.

Tables 3 and 4 show the accuracy of our classifiers with 5-fold cross-validation. We note that the RF classifier achieved higher accuracy in all cases. At its peak, the RF classifier achieved 87% accuracy, compared to 49% for the SVM classifier. Both classifiers achieve better accuracy when 0.1s splits are used, compared to 0.05s splits.

---

\(^1\)https://www.rtl-sdr.com/tag/rtl2382u/
| TABLE 3 | Accuracy for the RF classifier. |
|---------------------------|---------------------------|
| **Table** | **Unfiltered** | **Filtered** |
| **0.1s** | **0.05s** | **0.1s** | **0.05s** | **Mean** |
| 10 cm | 0.711 | 0.708 | 0.870 | 0.820 | 0.777 |
| 20 cm | 0.466 | 0.472 | 0.639 | 0.593 | 0.543 |
| 30 cm | 0.655 | 0.615 | 0.696 | 0.638 | 0.651 |
| 40 cm | 0.698 | 0.637 | 0.638 | 0.629 | 0.650 |
| 50 cm | 0.830 | 0.742 | 0.804 | 0.763 | 0.785 |
| **Mean** | 0.672 | 0.635 | 0.729 | 0.689 |

| TABLE 4 | Accuracy for the SVM classifier. |
|---------------------------|---------------------------|
| **Table** | **Unfiltered** | **Filtered** |
| **0.1s** | **0.05s** | **0.1s** | **0.05s** | **Mean** |
| 10 cm | 0.491 | 0.433 | 0.484 | 0.407 | 0.454 |
| 20 cm | 0.325 | 0.312 | 0.295 | 0.248 | 0.295 |
| 30 cm | 0.259 | 0.256 | 0.239 | 0.223 | 0.244 |
| 40 cm | 0.295 | 0.275 | 0.227 | 0.211 | 0.252 |
| 50 cm | 0.332 | 0.293 | 0.263 | 0.244 | 0.283 |
| **Mean** | 0.340 | 0.314 | 0.301 | 0.267 |

| TABLE 5 | Confusion matrix of our best classifier on an unseen test set. |
|---------------------------|---------------------------|
| **Predicted class** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **TrueClass** | | | | | | | |
| 1 | 100 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 89 | 0 | 11 | 0 | 0 | 0 |
| 3 | 0 | 0 | 100 | 0 | 0 | 0 | 0 |
| 4 | 7 | 0 | 0 | 92 | 1 | 0 | 0 |
| 5 | 0 | 0 | 0 | 3 | 97 | 0 | 0 |
| 6 | 0 | 0 | 35 | 0 | 0 | 65 | 0 |
| 7 | 0 | 83 | 0 | 17 | 0 | 0 | 0 |

The distance between the devices had a different impact on each classifier. The distance between the devices negatively impacts the SVM classifier; accuracy goes down as the distance between devices increases. On the other hand, the distance has no significant impact on the RF classifier; the mean accuracy at 10 cm is similar to the mean accuracy at 50 cm. There is no clear trend between the accuracy of the RF and the distance between devices.

The low pass filter also affected each classifier differently. The low pass filter had opposite effects between the classifiers. The SVM classifier had performed better on the raw signal, indicating that the filter removed valuable information from the SVM signal. On the other hand, the RF classifier performed better on the filtered signal, indicating that no valuable information was lost.

At last, we evaluate the best configuration found during cross-validation on a test set. Table 5 shows the confusion matrix of the best classifier we achieved on a test set of 700 signal fragments. The final accuracy of this test set was 77.57%. We note that the classifier correctly classified the signals of most of the devices. The classifier, however, performed poorly on two of the seven devices (devices 6 and 7).

7 | CONCLUSION

Computing is quickly becoming ubiquitous through the IoT, creating a demand for more robust security solutions. In particular, authentication solutions tailored for IoT applications are paramount. In this paper, we reviewed noteworthy
scenarios where IoT is quickly establishing itself, existing authentication methods, and the intersection between these two fields, i.e., existing authentication proposals for the IoT. We also propose our authentication method for IoT based on electromagnetic fingerprints. Our method is a promising pair for traditional cryptographic authentication solutions, as it requires no additional hardware from IoT devices. We have evaluated our approach under different settings and achieved 77% accuracy when distinguishing from a set of seven devices.

We have several plans for our next steps in this work, we believe the results presented in this paper already show the promise of such an approach, but in order to bring a practical method, the accuracy must be improved. In future iterations, we plan to expand the number of IoT devices in the experiments running generic programs that are used in day-to-day operations. We will test our solution with different devices, with varied computing capabilities. We will also evaluate our solution under different environments and at longer distances to further assess our approach’s flexibility. Another idea is to record the same signal in different places so that we can isolate the signal from jamming more effectively. Finally, we pretend to evaluate the significance of each feature to get to a group of the most obvious ones. Alongside these group of refined features, we intend to use different classification algorithms, more suited to these kind of signal analysis.

ACKNOWLEDGEMENTS
We fully acknowledge financial support for this work from Conselho Nacional de Desenvolvimento Científico e Tecnológico, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, and Fundação de Amparo à Pesquisa do Estado de Minas Gerais.

PEER REVIEW INFORMATION
Engineering Reports thanks Yun Lin, Satyanarayana Vuppalaand, and Jun Wang for their contribution to the peer review of this work.

CONFLICT OF INTEREST
The authors declare no potential conflict of interest relevant to this article.

ORCID
Artur Souza https://orcid.org/0000-0002-6927-4275
Heitor S. Ramos https://orcid.org/0000-0003-4523-6466

REFERENCES
1. Satyanarayanan M. Pervasive computing: vision and challenges. *IEEE Personal Commun.* 2001;8(4):10-17.
2. Atzori L, Iera A, Morabito G. The Internet of Things: a survey. *Comput Netw.* 2010;54(15):2787-2805.
3. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Generat Comput Syst.* 2013;29(7):1645-1660.
4. Oliveira LB, Pereira FMQ, Misoczki R, et al. The computer for the 21st century: present security & privacy challenges. *J Internet Serv Appl.* 2018;9(1):24.
5. Souza A, Cunha IB Oliveira L. NomadiKey: user authentication for smart devices based on nomadic keys. *Int J Netw Manag* 2017;28:e1998.
6. Antonakakis M, April T, Bailey M, et al. Understanding the mirai botnet. Paper presented at: Proceedings of the USENIX Security Symposium; 2017:1092-1110.
7. Stinson D. *Cryptography: Theory and Practice.* Boca Raton, FL: CRC Press; 2002.
8. Akyildiz IF, Vuran MC. *Wireless Sensor Networks.* Vol 4. Chichester, UK: John Wiley & Sons; 2010.
9. Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. *Ad Hoc Netw.* 2005;3(3):325-349.
10. Arampatzis T, Lygeros J, Manesis S. A survey of applications of wireless sensors and wireless sensor networks. Paper presented at: Proceedings of the 2005 IEEE International Symposium on, Mediterranean Conference on Control and Automation Intelligent Control; vol 2005, 2005.
11. Luk M, Perrig A, Whillock B. Seven cardinal properties of sensor network broadcast authentication. Paper presented at: Proceedings of the Workshop on Security of Ad Hoc and Sensor Networks (SASN); 2006.
12. Oliveira LB, Dahab R. Pairing-based cryptography for sensor networks. Paper presented at: Proceedings of the 5th IEEE International Symposium on Network Computing and Applications; 2006; Cambridge, MA.
13. Liu A, Kim M, Oliveira LB, Tan H. Wireless sensor network security. *Int J Distrib Sens Netw.* 2013;9:362385.
14. Ye W, Heidemann J, Estrin D. An energy-efficient MAC protocol for wireless sensor networks. Paper presented at: Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies; 2002.
15. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: security protocols for sensor networks. *Wirel Netw*. 2002;8(5):521-534.
16. Amadeo M, Campolo C, Molinaro A. Information-centric networking for connected vehicles: a survey and future perspectives. *IEEE Commun Mag*. 2016;54(2):98-104.
17. Jakubiak J, Koucheryavy Y. State of the Art and Research Challenges for VANETs. In: *IEEE Consumer Communications and Networking Conference*. 2008.
18. Qian Y, Moayeri N. Design of secure and application-oriented VANETs. Paper presented at: Proceedings of the Vehicular Technology Conference; 2008:2794-2799; VTC Spring, IEEE.
19. Bauza R, Gozalvez J, Sanchez-Soriano J. Road traffic congestion detection through cooperative vehicle-to-vehicle communications. Paper presented at: Proceedings of the 2010 IEEE 35th Conference on IEEE Local Computer Networks (LCN); 2010:606-612.
20. Karagiannis G, Altintas O, Ekici E, et al. Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun Surv Tutor*. 2011;13(4):584-616.
21. Weiß C. V2X communication in Europe—{}from research projects towards standardization and field testing of vehicle communication technology. *Comput Netw*. 2011;55(14):3103-3119.
22. Raya M, Hubaux JP. Securing vehicular ad hoc networks. *J Comput Sec*. 2007;15(1):39-68.
23. Kargl F, Waldschmidt C, Moser S, Slomka F. Wireless channel-based message authentication. Paper presented at: Proceedings of the Vehicular Networking Conference (VNC); 2015.
24. Förster D, Kargl F, Löhr H. PUCA: a pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. *Ad Hoc Netw*. 2016;37:122-132.
25. Rostami M, Juels A, Koushanfar F. *Heart-to-Heart (H2H): authentication for implanted medical devices*. Paper presented at: ACM Conference on Computer and Communications Security, CCS; 2013.
26. Wei J. How wearables intersect with the cloud and the Internet of Things: considerations for the developers of wearables. *Consum Electr Mag*. 2014;3(3):53-56.
27. Raij A, Ghosh A, Kumar S, Srivastava M. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. Paper presented at: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2011.
28. Di Pietro R, Mancini IV. Security and privacy issues of handheld and wearable wireless devices. *Commun ACM*. 2003;46(9):74-79.
29. Derawi MO, Nickel C, Bours P, Busch C. Unobtrusive user-authentication on mobile phones using biometric gait recognition. Paper presented at: Proceedings of the 2010 6th International Conference on IEEE Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP); 2010:306-311.
30. Lee EA. Cyber physical systems: design challenges. Paper presented at: Proceedings of the 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC 2008); 2008:363-369.
31. Lee EA. Cyber physical systems: design challenges. Paper presented at: Proceedings of the 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC 2008); 2008:363-369.
32. Wu M, Quintão Pereira F, Liu J, Ramos H, Alvim M, Oliveira L. New directions: proof-carrying sensing — towards real-world authentication in cyber-physical systems. Paper presented at: Proceedings of the Conference on Embedded Networked Sensor Systems (SenSys); 2017.
33. Cardenas AA, Amin S, Sastry S. Secure control: towards survivable cyber-physical systems. Paper presented at: Proceedings of the 28th International Conference on IEEE Distributed Computing Systems Workshops, 2008. ICDCS’08; 2008:495-500.
34. Schirner G, Erdogmus D, Chowdhury K, Fadir T. The future of human-in-the-loop cyber-physical systems. *Computer*. 2013;46(1):36-45.
35. Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *Int J Inf Sec*. 2001;1(1):36-63.
36. Oliveira LB, Kansal A, Gouvêa CP, et al. Secure-TWS: authenticating node to multi-user communication in shared sensor networks. *Comput J*. 2011;55(4):384-396.
37. Brown DR, Gallant R, Vanstone SA. Provably secure implicit certificate schemes. Paper presented at: Proceedings of the International Conference on Financial Cryptography; 2001:156-165; Springer.
38. Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. *Adv Cryptol—ASIACRYPT*. 2001;2001:514-532.
39. Shamir A. Identity-based cryptosystems and signature schemes. Paper presented at: Proceedings of the International Cryptology Conference on Advances in Cryptology (CRYPTO); 1984.
40. Boneh D, Franklin MK. Identity-based encryption from the weil pairing. Paper presented at: Proceedings of the International Cryptology Conference on Advances in Cryptology (CRYPTO); 2001.
41. Chatterjee S, Sarkar P. *Identity-Based Encryption*. New York, NY: Springer Science & Business Media; 2011.
42. Al-Riyami SS, Paterson KG. Certificatless public key cryptography. Proceedings of the Asiacrypt; 2003.
43. Neto ALM, Souza AL, Cunha I, et al. AoT: authentication and access control for the entire IoT device life-cycle. Paper presented at: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems; 2016.
44. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Paper presented at: Proceedings of the Conference on Computer and Communications Security (CCS); 2006.
45. Yuan E, Tong J. Attributed based access control (ABAC) for web services. Paper presented at: Proceedings of the International Conference on Web Services (ICWS); 2005.
46. Ouechtati H, Azzouna NB. Trust-ABAC towards an access control system for the Internet of Things. Paper presented at: Proceedings of the International Conference on Green, Pervasive, and Cloud Computing (GPC); 2017.
48. Bernstein DJ. Introduction to Post-quantum Cryptography. New York, NY: Springer; 2009.
49. Hülsing A. W-OTS—shorter signatures for hash-based signature schemes. Paper presented at: Proceedings of the International Conference on Cryptology in Africa; 2013.
50. Buchmann J, Dahmen E, Seydlo M. Hash-based digital signature schemes. *Post-Quantum Cryptography*. 2009;1:35-93.
51. Chaum D, Van Heyst E. Group signatures. Paper presented at: Proceedings of the Advances in Cryptology—EUROCRYPT’91; 1991.
52. Rivest R, Shamir A, Tauman Y. How to leak a secret. Paper presented at: Proceedings of the Advances in Cryptology—ASIACRYPT 2001; 2001.
53. Boyen X. Mesh signatures. Paper presented at: Proceedings of the Conference on the Theory and Applications of Cryptographic Techniques; 2007.
54. Maji HK, Prabhakaran M, Rosulek M. Attribute-based signatures. Paper presented at: Proceedingsof the Conference on the Theory and Applications of Cryptographic Techniques; 2007.
55. Garg R, Hajj-Ahmad A, Wu M. Geo-location estimation from electrical network frequency signals. Paper presented at: Proceedingsof the Conference on the Theory and Applications of Cryptographic Techniques; 2007.
56. Satchidanandan B, Kumar P. Dynamic watermarking: active defense of networked cyber–physical systems. *Proc IEEE*. 2017;105(2):219-240.
57. Souza E, Wong HC, Cunha I, Cunha I, Vieira LFM, Oliveira LB. End-to-end authentication in under-water sensor networks. Paper presented at: Proceedingsof the Conference on the Theory and Applications of Cryptographic Techniques; 2007.
58. Zhu S, Setia S, Jajodia S. LEAP+: efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans Sens Netw*. 2006;2(4):500-528.
59. Oliveira LB, Aranha DF, Gouvêa CP, et al. TinyPBC: pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Comput Commun*. 2011;34(3):485-493.
60. Aranha D, Oliveira LB, López J, Dahab R. NanoPBC: implementing cryptographic pairings on an 8-bit platform. Paper presented at: Proceedings of the Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc (CHiLE 2009); 2009.
61. Plößl K, Federrath H. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Comput Stand Interf*. 2008;30(6):390-397.
62. Papadimitratos P, Buttyan L, Holczer T, et al. Secure vehicular communication systems: design and architecture. *IEEE Commun Mag*. 2008;46(11):100-109.
63. Hao Y, Cheng Y, Zhou C, Song W. A distributed key management framework with cooperative message authentication in VANETs. *J Select Areas Commun*. 2011;29(3):616-629.
64. Islam SH, Ohbaidat MS, Vijayakumar P, Abdulhay E, Li F, Reddy MKC. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Generat Comput Syst*. 2018;84:216-227.
65. Zhang L, Wu Q, Domingo-Ferrer J, Qin B, Hu C. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Trans Intell Transp Syst*. 2016;18(3):516-526.
66. Horng SJ, Tseng SF, Huang PH, Wang X, Li T, Khan MK. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Inf Sci*. 2015;317:48-66.
67. Venkatasubramanian KK, Banerjee A, Gupta SKS. PSKA: usable and secure key agreement scheme for body area networks. *IEEE Trans Inf Technol Biomed*. 2009;14(1):60-68.
68. Kalamandeen A, Scannell A, Lara de E, Sheth A, LaMarca A. Ensemble: cooperative proximity-based authentication. Paper presented at: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services; 2010.
69. He D, Zeadally S. Authentication protocol for an ambient assisted living system. *IEEE Commun Mag*. 2015;53(1):71-77.
70. Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Trans Parall Distrib Syst*. 2013;25(2):332-342.
71. Almulhim M, Zaman N. Proposing secure and lightweight authentication scheme for IoT based E-health applications. Paper presented at: Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT); 2018:481-487.
72. Vuppala S, Mady AED, Mehta D. A novel asset authentication scheme for cyber physical systems. *Global IoT Summit (GIoTS)*. New York, NY: IEEE; 2019.
73. Mo Y, Weerakkody S, Sinopoli B. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Syst Mag*. 2015;35(1):93-109.
74. Long-lived authentication protocols for process control systems. *Int J Critical Infrastr Protect*. 2010;3(3):174-181.
75. Hajj-Ahmad A, Garg R, Wu M. ENF-based region-of-recording identification for media signals. *IEEE Trans Inf Forens Sec*. 2015;10(6):1125-1136. https://doi.org/10.1109/TIFS.2015.2398367.
76. Wu M, Pereira FMQa, Liu J, Ramos HS, Alvim MS, Oliveira LB. Proof-carrying sensing: towards real-world authentication in cyber-physical systems. Paper presented at: Proceedings of the 15th ACM Conference on Embedded Network Sensor SystemsSenSys ’17 Association for Computing Machinery; 2017; New York, NY.
77. Yilmaz BB, Callan RL, Prvulovic M, Zaji A. Capacity of the EM covert/side-channel created by the execution of instructions in a processor. *IEEE Trans Inf Forens Sec*. 2018;13(3):605-620. https://doi.org/10.1109/TIFS.2017.2762826.
78. Das A, Borisov N, Caesar M. Do you hear what i hear? fingerprinting smart devices through embedded acoustic components. Paper presented at: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications SecurityCCS ’14; 2014:441-452; New York, NY, ACM.
79. Sehatbakhsh N, Hong H, Lazar B, et al. Syndrome: spectral analysis for anomaly detection on medical IoT and embedded devices-experimental demonstration. Paper presented at: Proceedings of the Hardware Demo at IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2018); 2018.

80. Herder C, Yu M, Koushanfar F, Devadas S. Physical unclonable functions and applications: a tutorial. Proc IEEE. 2014;102(8):1126-1141.

81. Ahmed MM, Hely D, Barbot N, et al. Radiated electromagnetic emission for integrated circuit authentication. IEEE Microw Wirel Compon Lett. 2017;27(11):1028-1030.

82. Ahmed MM, Hely D, Perret E, et al. Authentication of microcontroller board using non-invasive EM emission technique. Paper presented at: Proceedings of the 2018 IEEE 3rd International Verification and Security Workshop (IVSW); 2018:25-30.

83. Wang J, Ni M, Wu F, Liu S, Qin J, Zhu R. Electromagnetic radiation based continuous authentication in edge computing enabled Internet of Things. J Syst Arch. 2019;96:53-61. https://doi.org/10.1016/j.sysarc.2018.12.003.

84. Vapnik VN. The Nature of Statistical Learning Theory. New York, NY: Springer-Verlag; 1995.

85. Criminisi A, Shotton J, Konukoglu E. Decision forests: a unified framework for classification, regression, density estimation, manifold learning and semi-supervised learning. Found Trends® Comput Graph Vis. 2012;7(2–3):81-227.

How to cite this article: Souza A, Carlson I, Ramos HS, Loureiro AA, Oliveira LB. Internet of Things device authentication via electromagnetic fingerprints. Engineering Reports. 2020;2:e12226. https://doi.org/10.1002/eng2.12226