IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 19, 2020, accepted June 22, 2020, date of publication June 25, 2020, date of current version July 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3004814

Defenses Against Perception-Layer Attacks on IoT Smart Furniture for Impaired People

MOUSTAFA M. NASRALLA[1], (Member, IEEE), IVÁN GARCÍA-MAGARIÑO[2,3], AND JAIME LLORET[4], (Senior Member, IEEE)

[1]Department of Communications and Networks Engineering, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]Department of Software Engineering and Artificial Intelligence, Complutense University of Madrid, 28040 Madrid, Spain
[3]Instituto de Tecnología del Conocimiento, Complutense University of Madrid (UCM), 28040 Madrid, Spain
[4]Integrated Management Coastal Research Institute, Universitat Politècnica de València, 46022 València, Spain

Corresponding author: Jaime Lloret (jlloret@dcom.upv.es)

This work was supported in part by the research project Utilisation of IoT and Sensors in Smart Cities for Improving Quality of Life of Impaired People under Grant 52-2020, in part by the Ciudades Inteligentes Totalmente Integrales, Eficientes Y Sotenibles (CITIES) funded by the Programa Iberoamericano de Ciencia y Tecnología para el Desarrollo (CYTED) under Grant 518RT0558, in part by the Diseño Colaborativo Para La Promoción Del Bienestar En Ciudades Inteligentes Inclusivas under Grant TIN2017-88327-R funded by the Spanish Council of Science, Innovation and Universities from the Spanish Government, and in part by the Ministerio de Economía y Competitividad in the Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento under Grant TIN2017-84802-C2-1-P.

ABSTRACT Internet of Things (IoT) is becoming highly supportive in innovative technological solutions for assisting impaired people. Some of these IoT solutions are still in a prototyping phase ignoring possible attacks and the corresponding security defenses. This article proposes a learning-based approach for defending against perception-layer attacks performed on specific sensor types in smart furniture for impaired people. This approach is based on the analysis of time series by means of dynamic time warping algorithm for calculating similarity and a novel detector for identifying anomalies. This approach has been illustrated by defending against simulated perception-layer magnetic attacks on a smart cupboard with door magnetic sensors. The results show the performance of the proposed approach for properly identifying these attacks. In particular, these results advocate an accuracy about 95.5% per day.

INDEX TERMS Perception-layer attack, smart furniture, smart cupboard, magnetic sensors, time series, dynamic time warping, IoT security.

I. INTRODUCTION

In the aspect of Internet of Things (IoT), there are many security attacks [1], making this technology vulnerable in some scenarios. For understanding the impact of IoT security leaks, some of the common motivation use cases are (a) the hacked baby monitors in Ohio and Texas, (b) the attacks over the devices produced by Acoustic Technology Inc, and (c) the Turning Up the Freeze attack with a Distributed-denial of Service (DDoS) over environmental control systems [2]. IoT security attacks can be classified into (1) perception layer attacks, e.g. botnets, sleep deprivation attack, node tampering & jamming and eavesdropping, (2) network layer attacks, e.g. with Man-in-the-Middle (MiM) attacks, DDoS, routing attacks, middleware attacks, authentication attacks and signature wrapping attacks, and (3) application layer attacks, e.g. with malware or code injection attack.

The associate editor coordinating the review of this manuscript and approving it for publication was Chunhua Su.

Novel smart objects are appearing in IoT, and these can easily become the target of hackers due to their lack of enough proper security mechanisms on their first launch. In this context, novel pieces of smart furniture are launching as means for (a) improving quality of life of impaired people, such as the visually impaired [3], (b) tracking symptoms of some diseases and their early detection, such as the smart cupboards (SCs) for tracking losses of memory for early detection and tracking of of Parkinson's disease [4], and (c) monitoring patients, e.g. during their sleep with smart beds [5]. In all these contexts, users rely on IoT devices for properly handling and managing highly sensitive and private information concerning their personal lives.

In general, novel pieces of smart furniture can bring security risks in smart cities. Notice that collaboration of different pieces of smart furniture [6] makes that a vulnerability in a piece of smart furniture could make an entire IoT ecosystem unreliable in a smart home, smart hospital or smart city depending on the context.

Perception-layer attacks can make IoT smart furniture useless as the information sensed by these could have been altered becoming unreliable. For example, SCs may not provide useful information about users with Parkinson disease. Smart beds may not properly report bad sleeping postures in critical patients in hospitals. Visually impaired people may have serious consequences if relying on IoT devices suffering perception-layer attacks, as these may provide misleading information.

Since perception-attacks alter input data from sensors, this approach proposes to analyze these input data to detect anomalies, considering these data as time series. The benefit of applying time-series analysis is its capacity in detecting patterns considering the values as a part of a continuous series ordered in time, being able to usually detect more anomalies in certain IoT pieces of smart furniture.

The current article proposes several defenses for smart furniture (illustrating each of these with SCs or smart beds) for certain attacks, to advance the security measures for facilitating future commercializing of pieces of smart furniture. The novelty of the proposed approach mainly focuses on perception-layer attacks and defenses, although this approach also mentions and discusses other kinds of attacks and defenses.

The remainder of this article is organized as follows. Next section introduces related works highlighting the literature gap covered by the present work, and introduces common attacks on smart furniture. Section III indicates the defenses of smart furniture against common attacks, and proposes a detailed technique for defending against perception-layer attacks based on a novel detector that analyzes time series. Section IV illustrates the proposed approach with simulated realistic perception-layer attacks on the magnetic sensors of our SC, and presents the experimentation results. Section V discusses the most relevant aspects concerning these results. Section VI mentions the conclusions and depicts our most relevant future lines of work on this topic.

II. RELATED WORK

A. TIME SERIES ANALYSIS IN IoT

Several works have analyzed time series in IoT context. For instance, [7] studied the effects of lossy compression in IoT time series when applying deep-learning classification. They focused on proposing an efficient compression technique with an error-bound compressor for reaching a trade-off between compression and quality in univariate and multivariate time series. They concluded that applying discrete wavelet transform followed by the Squeeze method helped to remove noise from input data and compress a more smooth approximation.

In addition, [8] focused on the representation of time series in IoT to later effectively and efficiently applying data mining techniques such as classification, similarity search, clustering and predict. More concretely, they proposed a novel multi-resolution hybrid representation approach for this purpose. They demonstrated the advantages of their approach with experiments on different kinds of time series datasets.

Nevertheless, none of these works focused on the application of time-series for IoT security against perception-layer attacks as the current work proposes.

B. MACHINE LEARNING IN IoT SECURITY

There are also some works that focus on learning-based IoT security. For example, [9] proposed to apply statistical learning methods to detect anomalies in the behaviors of IoT devices. They based their statistical analysis in CPU usage cycles and disk usage through IoT application program interfaces. They trained different machine learning (ML) methods to later distinguish cyber attacks and malfunctions. Their experiments showed that their proposed anomaly detection-based framework was effective to detect attacks on IoT devices.

In this line of work, [10] presented a survey about network intrusion detection systems with learning techniques showing their particularities in the IoT context. Their survey compared existing works in this context specifically considering architectures, detection methodologies, validation strategies, robustness to certain threats, and algorithms designs. In this survey, all the analyzed works used detection methodologies based either on signature, specification, anomalies or hybrid methods with some of these. The most common method was anomaly detection.

These works focused on the analysis of either IoT processing units or network traffic. However, these two works neither analyzed nor suggested security systems that focused on perception-layer attacks by analyzing the input from sensors.

C. PERCEPTION-LAYER ATTACKS

The security literature includes some works focused on perception-layer attacks. More specifically, [11] analyzed security mechanisms for protecting against perception-layer threats in IoT. They firstly described the key IoT components such as architectures, standards, protocols in relation to common security requirements at perception layer. They later focused on radio-frequency identification (RFID) and sensor networks as key enabling technologies in perception layers. They classified common attacks in these technologies and discussed some possible solutions.

In this line of research, [12] focused on security improvements on chip devices for being robust against perception-layer attacks. They proposed hardware solutions for increasing security in next generations of microcontrollers combined with other IoT perception-layer security measures. They also discussed trusted execution environments in microcontrollers and its holistic applications for addressing IoT security challenges involving perception-layer attacks among others.

Nonetheless, these works did not specifically addressed ML for analyzing time-series data from specific sensor types, as the current work does for analyzing time-series input from door magnetic sensors.

D. SMART FURNITURE

In the literature, several works propose relevant contributions about smart pieces of furniture. In particular, the self-configurable modular robots named ''Roombots'' can provide adaptive and assistive smart pieces of furniture [13]. The extended version of Roombots focused on the difficulties in real hardware, in aspects such as autonomously moving furniture, object manipulation, gripping features and easy-to-use interfaces.

Moreover, [14] reviewed smart solutions for assisting impaired and elder people. They highlighted the raising opportunities in IoT-based solutions for healthcare of these people. They specifically analyzed and discussed new smart-furniture solutions. They concluded that smart pieces of furniture should be flexible, low-cost and easy to install without expert knowledge, to be ready for commercialization. In this review, one can observe that although security is considered relevant, some security measures have not been properly addressed.

In general, these two aforementioned works reveal that most smart-furniture works are generally in prototyping or research phases, and they do not provide proper security measures against perception-layer attacks yet.

E. POTENTIAL ATTACKS ON IoT SMART FURNITURE

To identify possible attacks on smart furniture, we considered the implementation of our previous smart pieces of furniture as examples, including SCs for measuring memory and our smart beds, among others. In particular, both smart pieces of furniture were based on the analysis of input data from sensors. All the predictions and decision-making processes were based on the reliability of these input data. Hence, perception-layer attacks can be performed to alter these input data and consequently drawing all the reliability from the corresponding smart pieces of furniture.

Besides sensors, other common components on our smart pieces of furniture are (a) databases where the information is stored, (b) backend servers that manage databases and provide information to the frontend, and (c) mobile apps that allow users to interact with the system. Therefore, all the communications can be attacked for intercepting information. Authentication attacks can be performed in any of these components including the database, the backend and the apps. Attacks can pursue stealing real-time information as this is very valuable to perpetrate different kinds of illicit activities such as burglary, violent attacks and invasive advertisement.

Section II-E1 mentions possible perception-layer attacks on smart furniture, and section II-E2 indicates other common attacks on smart furniture.

1) PERCEPTION-LAYER ATTACKS ON SMART FURNITURE

In perception-layer attacks on smart furniture, attackers could provide fake perception information by the two following possibilities:

- *Hijacking physical sensors*, by for example applying magnetic fields over magnetic door sensors, or keeping pressed load sensors by any physical object. We have detected some common metrics for measuring magnetic attacks over physical sensors in works such as [15]. In that work, magnetic attacks where applied over cars in anti-lock braking systems. The first metric was the duration of attacks, as their attacks were limited by the battery lifetimes of attacker devices. The other metric type was very specific of the field showing the impact of attacks. In particular, they measured wheel speed, and compared this between normal cases and attacked cases. In a similar way, we also measure differences between normal cases and attacked cases, with our specific metric, which is the number of door events per hour in each day.
- *Directly interacting with the database*, introducing fake information about fake events, so the measures are based on this fake information. Works like [16] reveal some of the common metrics for detecting database intrusion. In particular, they used some metrics over database queries such as query length, its numeric values and length of string values. They also used other features extracted from ''order by'' clauses, ''group by'' clauses and join information. After applying their neural-based learning classifier, they used the metrics of 10-fold accuracy and p-value to evaluate their approach in a given dataset.

In the context of smart furniture, for example perception-layer attacks may arise fake alarms of memory losses or bad sleeping poses to discredit the corresponding pieces of IoT smart furniture. The novel contribution of the proposed approach focuses on defending against this kind of attacks.

2) OTHER POTENTIAL ATTACKS ON SMART FURNITURE

A group of potential attacks are aimed at stealing real-time information. In data collection of privacy-related behaviors, security is considered crucial for preserving the privacy of users in systems with mobile apps [17]. Attackers could aim at stealing real-time information from either SCs or smart beds. This could be useful to know the current status of potential victims, to determine when they are at the deepest state of sleeping or when they are cooking to perpetrate different kinds of burglary (e.g. breaking into the house) violent acts (e.g. shooting on the kitchen window), or illicit commercial activities (e.g. delivering advertisement of different food kinds based on private personal information). These attacks can depart from stealing authentication credentials, either by fishing the username and password by sending fake emails to the user, or by intercepting communications.

Another group of attacks is related to the prediction of life-style patterns from IoT devices [18]. This kind of attacks can depart from stealing credentials from the database. Based on the information retrieved of the database, the attacker could predict life-style patterns to know them in advance for taking advantage of victims. These predictions could also be useful for illicitly extracting private health-related information to be sold to health insurance companies.

MiM attacks can also attempt to compromise security of pieces of smart furniture. MiM attacks rely on intercepting messages and transmitting information, sniffing private information in the process [19]. The attacker can provide a malicious app similar to the real one, as indicated in the literature for many other domains [20]. When users have this malicious app installed on their devices, they can properly use all the app functionalities, but this app would steal the authentication information to give attackers access to all kinds of private information.

To the best of authors' knowledge, none of the existing works has proposed a time-series analysis approach against perception-layer attacks focusing on specific sensor types inputs such as the door magnetic sensors of SCs. The proposed approach covers this gap of the literature.

III. PROPOSED DEFENSES ON IoT SMART FURNITURE

The proposed approach includes the novel perception-layer defenses with analysis of time-series from smart furniture in section III-A and other security recommendations about authentication, database protection and encryption on smart furniture systems in section III-B.

A. SMART FURNITURE PERCEPTION-LAYER DEFENSES WITH A TIME-SERIES LEARNING-BASED APPROACH

This article proposes a novel approach for defending against perception-layer attacks on pieces of smart furniture. It a learning-based approach that relies on the calculation of similarity between time series.

In our smart pieces of furniture, including both the SC and the smart bed, the perception-layer information is taken from sensors. The key to make the proposed approach useful is to properly define a representative time series from the input. For example, both the SC and the smart bed use binary information from sensors. The SC detects whether each door is open and the transition events (i.e. when the door is either being opened or being closed). The smart bed has a grid of load sensors, and the relevant information is which sensors are being pressured rather than the weights, which can vary among different users. The binary information has very low precision and the signals are multivariate (i.e. several door sensors in the SC and several load sensors in the bed). Instead of using this raw information, the proposed approach recommends to gather and process these data for obtaining meaningful time series.

For instance, in the case of the SC, we decided to determine a data series with the number of door events per hour, revealing the meal-preparation activity in each hour of the day. This was defined with the following formula:

$$s(i) = (\#e : e \in E : h(e) = i) \tag{1}$$

where $s(i)$ is the value of the series in i-th position starting counting on zero in the 0 to 23 interval of hours for each day, # is the notation of the counting operator, e is the bound variable used in this operator representing each event, E is the set of all door events occurring on a specific day, and h function with type 'event→integer' returns the hour of the day (i.e. in the interval from 0 to 23) for a given door event.

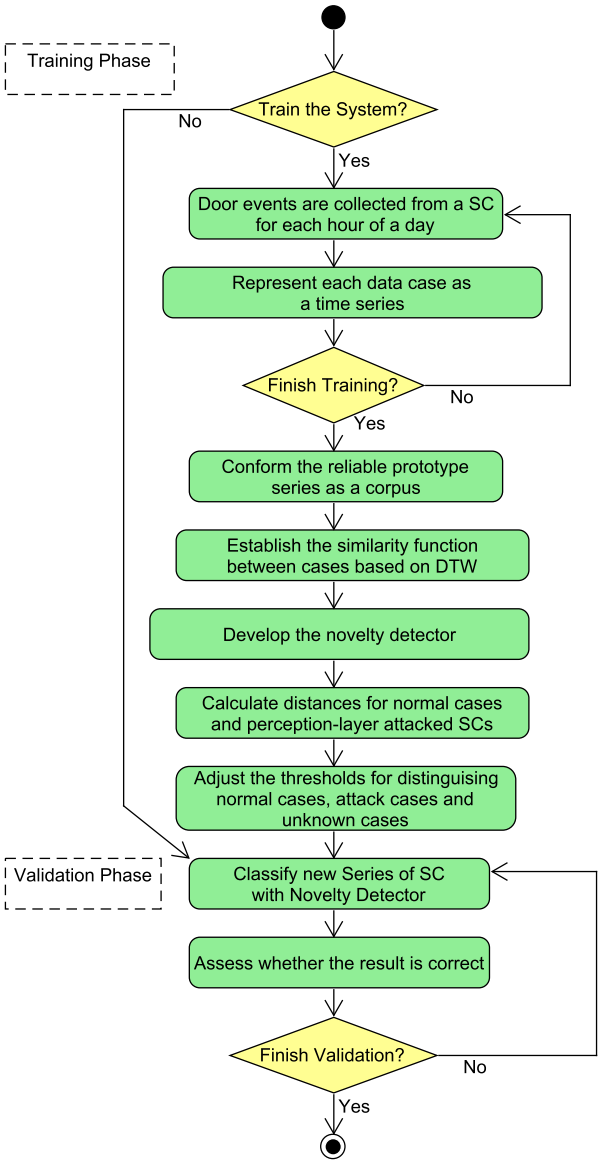


FIGURE 1. Block diagram for securing a SC against magnetic perception-layer attacks.

Figure 1 presents the block diagram for protecting a smart piece of furniture against perception-layer attacks, exemplified with the SC for facilitating its understanding. It applies a ML approach based on two phases of training and validation. It applies a novelty detector approach in which the new cases are compared with the corpus of normal cases to detect possible anomalies. The advantage of novelty detectors over other ML techniques is that they perform well without needing attack cases. Notice that our IoT SC has not commercialized yet, and consequently we have not received any real attack yet. Thus, novelty detectors fit reasonably well for emerging smart pieces of furniture.

In order to protect the SC from perception-layer attacks, we started extracting the relevant information from the raw

data of the perception-layer. In this particular case of the SC, the perception information is basically the door events concerning to whether a door has changed its state from close to open or vice versa.

The key is to extract the information so that it can classify other possible normal series as such. In the case of SCs, the activity measured as door events revealed the preparation of meals in certain times ranges of the day detecting usage patterns that could be associated with normal usages. For example, different users can prepare their meals at different times of the day, and may need different number of events. However, most users will need to prepare their big meals with sometimes in-between meals. We found it particularly useful to consider relative time order into account, extracting information in terms of time series, and gathering the events by time slots.

To fairly compare two time series, we chose a similarity comparison based on Dynamic Time Warping (DTW) [21], since this comparison is more focused on comparing the shapes of the time series rather than exact time-paired values. In this way, two time series are considered similar even if two people prepare their meals at different times.

DTW is aimed at obtaining the minimum matching of points between two time series, respecting the order of both series, but being flexible in the positions of points. DTW uses dynamic programming by calculating a matrix of costs for reaching each possible pair of points, reusing these costs for later calculations, achieving a reasonable computational cost. In each step, the cost of each matrix cell c(i, j) represents the partial matching of points for reaching this pair of points between the i-th point of first series and j-th point of the second series with the minimum cost. This algorithm goes through all the matrix performing the following operation:

$$c(i,j)=min(c(i-1,j),c(i-1,j-1),c(i,j-1))+d(i,j) \quad (2)$$

where any c(i, j) represents the cost of the matrix in position (i,j) if this is a valid position (i.e. if $i \geq 0$ and $j \geq 0$) and is evaluated as zero value if the position is not valid; and $d(i, j)$ is the distance between i-th point of the first s series and j-th point of the second t series, calculated as follows:

$$d(i,j) = |s(i) - t(j)| \quad (3)$$

In this way, DTW explores all the possible matching associations between both series respecting the order of both series. In the case of SCs, this would be all possible associations of meal preparations between each normal usage and the current usage under evaluation.

The novelty detector relies on determining the most similar meal-preparations association to check how normal the usage is. In case of high novelty, i.e. fairly different from all the normal usages, the system identifies a potential perception-layer attack.

In the training phase, this approach recommends to calibrate the distance thresholds for distinguishing between normal cases, attack cases and unknown cases, by using a set of normal cases and realistic attacks.

TABLE 1. Security measures of the proposed approach.

Perception-layer Attack	Defense
Sensor hijacking	Novelty detector for detecting strange sensor inputs
Database attack for changing perception information	(a) authentication for using any file on the server (b) parsing of any input field for avoiding SQL injection
Steal real-time information	Delay all non-critical information transmission
MiM attack	256-bit RSA encryption

In the validation phase, the proposed approach recommends to assess the performance of the defense mechanism by testing it with a different set of normal usages and realistic attacks.

B. OTHER DEFENSES AGAINST ATTACKS ON SMART FURNITURE

The proposed approach combines the novel detection of perception-layer attacks with other security measures to protect smart furniture. Table 1 summarizes the defenses against attacks on smart furniture. Previous subsection described the proposed defense to sensor hijacking based on the analysis of sensor inputs as time series with a novelty detector properly trained. Other security measures are further described in this subsection.

In order to make connections secure in smart furniture, this technique proposes all the additional following security measures, exemplified with SCs:

- Authenticate all the accesses to the PHP scripts of the server, like the following scripts concerning functionalities in our SCs:
  - Recording information from sensors, to avoid perception layer attacks based on storing fake information concerning sensors.
  - Retrieving health information, to avoid that this private information is stolen.
- Apply the common techniques for preventing SQL-injection attacks in all the parameters that end up in any SQL query, for example when registering new users.

Regarding the theft of real-time information, we propose to include a safe delay (e.g two hours), for providing any kind of information that does not need real-time actions. Thus, neither users nor potential attackers can know real-time information that can make a victim vulnerable. For example, in the case of SCs, users do not need to know their memory capacity evolution in real-time, as this is normally a slow process. Regarding smart beds, bad sleeping postures need to be informed in real time, but the information about whether a user is actually sleeping or not is not so critical to be known in real time, so the latter information can be safely delayed.

To prevent authentication information from being stolen, users can be regularly reminded that the system will never ask their credentials by email to avoid fishing attacks. All the authentication information is recommended to be encrypted for transmission, so it is difficult to be intercepted and decrypted.

TABLE 2. Parameters used in the experiments and simulations.

Parameter	Value
Time in all experiments and simulations	24 h
Most frequent big-meal times in simulations	8 h, 14 h, 21 h
Most frequent small-meal times in simulations	11 h, 17 h
Range of meal-time alterations	[-1 h, +1 h]
Minimum number of events in big meals	2
Maximum number of events in big meals	20
Minimum number of events in small meals	1
Maximum number of events in small meals	6
Probability that each small meal takes place	0.50
Number of simulations in each scenario	1000
Distance threshold for identifying normal cases	2.10 events/h
Distance threshold for identifying attacks	2.60 events/h

For avoiding direct attacks against the database, this is recommended to be configured only with access from the local host, i.e. the server in which the database is installed. Then, all the communications to the database are advised to be performed through PHP scripts with proper anti SQL-injection mechanisms.

To protect smart furniture against MiM attacks, we recommend to apply the public-key 256-bit Rivest-Shamir-Adleman (RSA) encryption for setting secure channels by interchanging a randomly-generated shared key for each channel of communication. Notice that 256-bit RSA is widely accepted as secure mechanism for establishing communications in the literature [22]. Then, the app and the backend system can efficiently and securely communicate with symmetric encryption. In addition, apps are recommended to be signed with the certificate of the smart furniture manufacturer, and users are advised to avoid using any app not signed by the manufacturer, to avoid MiM attacks by means of malicious apps.

IV. EXPERIMENTATION

The experimentation focuses on illustrating and evaluating the application of the proposed approach on SCs taking perception-layer attacks into account. We used "DTW" Python module as a tool for supporting simulations. Table 2 presents the list of all the parameters used for the experiments and simulations.

To illustrate the calculation of distances between perception-layer time series in SCs, Figure 2 shows the DTW analysis of the series of two normal usages of the SC for one day. In this figure, each point of the first series is matched with one or several points of the second series, represented with dotted lines, and vice versa. The matching of the two series is obtained by calculating the one that minimizes the sum of distances among the matching of points that preserve the order in both series, with the DTW algorithm. One can observe that the shape of the two time series are quite similar although the alignment in time slightly differs and the peak values are different.

The DTW distance between these two series was 23 door openings in a day, which were 0.96 door events per hour

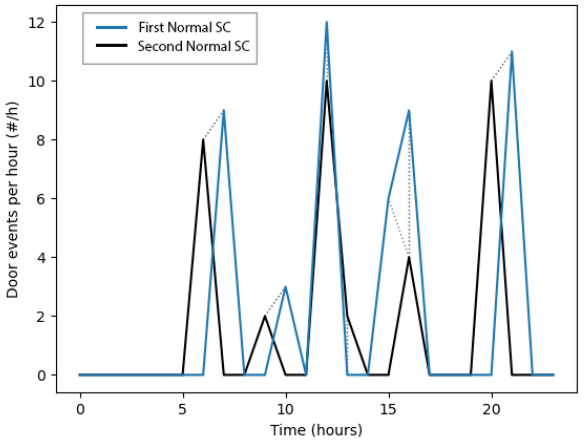


FIGURE 2. DTW comparison of time series of two normal usages of smart cupboards.

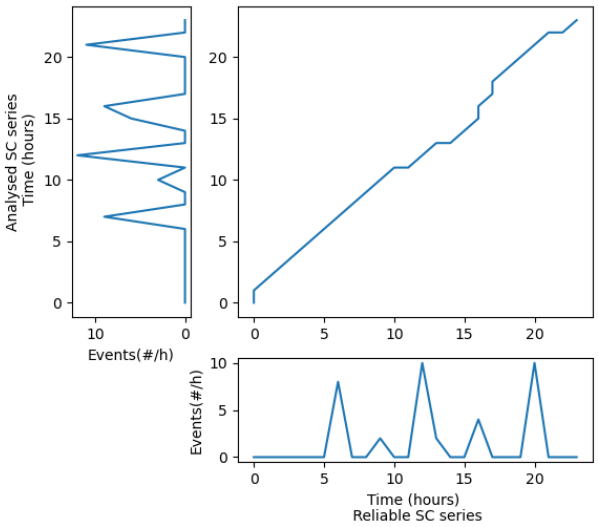


FIGURE 3. Costs extracted by DTW from two normal usages of smart cupboards.

in average. This information was also provided by the DTW algorithm.

More concretely, Figure 3 presents the matrix of costs highlighting the minimum values with a blue line, extracted with the algorithm for calculating DTW distance. The line shows the path of the minimum costs revealing the underlying matching. The i-th indexes of both series almost increase simultaneously, as one can observe that the line is almost in the diagonal. This means that both series are quite aligned although not completely.

Figure 4 shows the diagram of the Rabiner Juang Step Pattern of this DTW algorithm application for calculating the similarity between two normal usages of SCs. In particular, we used the Family VI and subtype "c" of this step pattern, which has several families and subtypes. This step patterns shows the matching model of indexes between the two time series about SCs usage over the hours. One can observe that the differences of indexes are in the range between minus

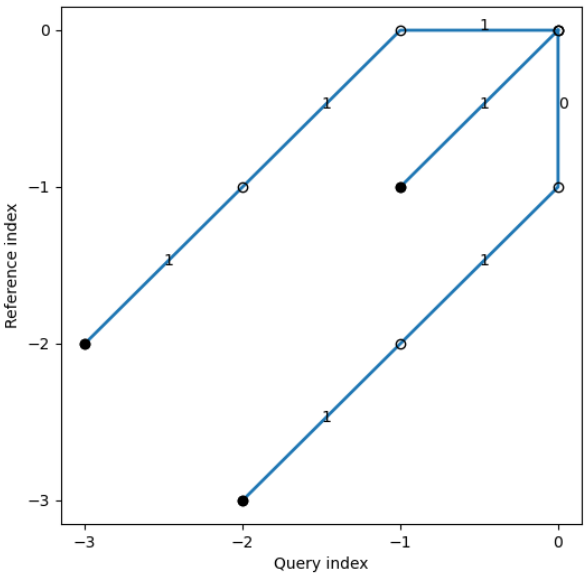


FIGURE 4. Diagram of the Rabiner Juang Step Pattern between two normal usages of smart cupboards.

```
Distance: 0.9583333333333334 door events per hour
Step pattern recursion:
 g[i,j] = min(
     g[i-3,j-2] +     d[i-2,j-1] +     d[i-1,j  ] +     d[i  ,j  ] ,
     g[i-1,j-1] +     d[i  ,j  ] ,
     g[i-2,j-3] +     d[i-1,j-2] +     d[i  ,j-1] + 0 * d[i  ,j  ] ,
 )
```

FIGURE 5. Formula of the Rabiner Juang Step Pattern between two normal usages of smart cupboards.

three to zero. This means that the best association did not have greater differences of three hours. This is reasonable as people have meals at different times depending on them.

Figure 5 presents the recursive-relation formula of this step pattern. This formula represents how both series were matched, indicating which index distances were used when finding the minimum distance between both series. They show the relative distances to the increasing indexes of the algorithm. One can observe that the matching had distances between minus three and zero, revealing that most meals between both usages were taken with a difference of three hours as maximum.

We simulated a realistic perception-layer magnetic attack on a SC, and Figure 6 presents a comparison between an example of the hacked SC events and another example from a non-attacked SC. This figure contains both series of numbers of door events per hour. It also includes points matching between both series with dotted lines provided by the DTW algorithm as the minimum distance-sum matching preserving the order. One can observe that shapes of both series are quite different from each other.

In this example, the DTW distance was 97 door events in a day, and consequently a 4.04 door events per hour in average. This high value confirms that both shapes were detected as much different than in the previous case, as we observed in the graphical comparison.

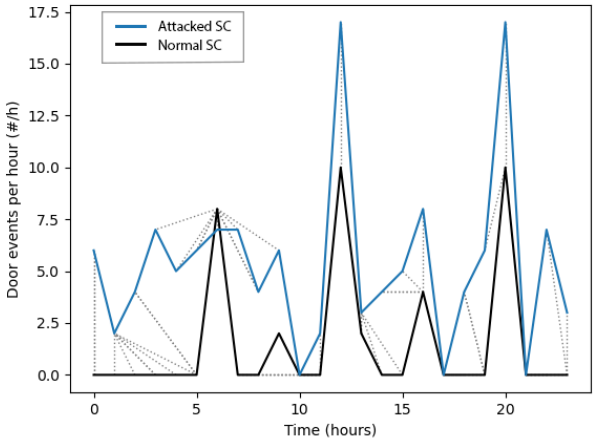


FIGURE 6. DTW comparison of time series with a smart cupboard attacked magnetically.

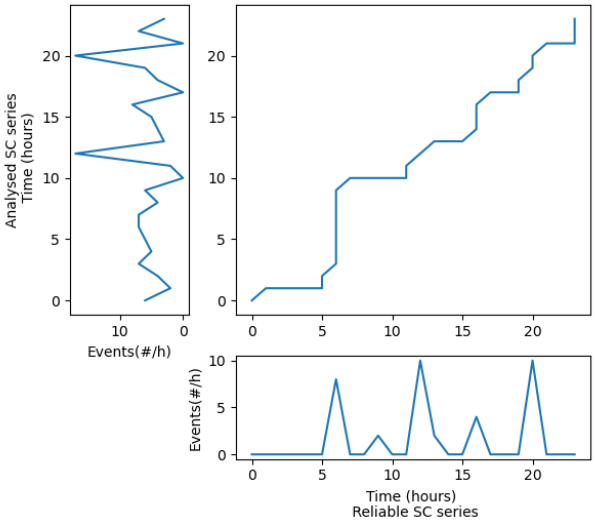


FIGURE 7. Costs extracted by DTW when for the smart cupboard with the magnetic attack.

In addition, Figure 7 shows the resulting costs matrix with the minimum value from the application of the DTW algorithm for calculating the similarity between the attacked SC and another example of reliable SC. It is worth noting that the association of minimum weights is more varied (i.e. more different from the diagonal) than in the previous case. The alignment of indexes of both series are not so far from the diagonal, but is much different than in the previous case. In fact, peaks of normal usages are associated with many values of the series from the attacked SC.

We also extracted the Rabiner Juang Pattern obtained from this comparison between the attacked SC and normal usage. The results of the matching index distances were the same as in the comparison between the two normal usages of SCs. This means that the alignment between both series were similar. However the total distance value was different, which was 4.04 instead of 0.96 as in the previous case. The similar alignment can be explained because the attacks also also

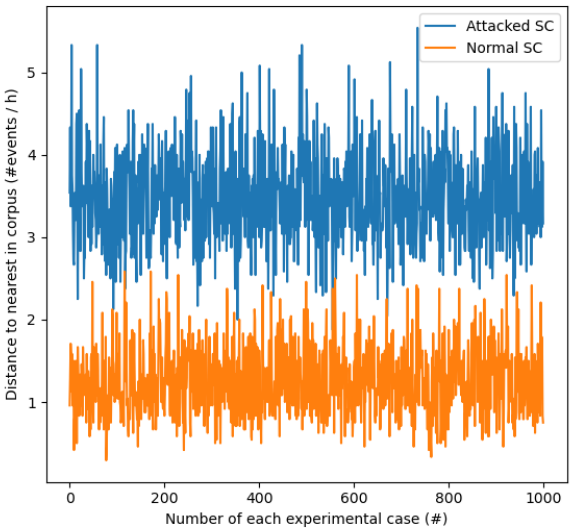


FIGURE 8. Distances to corpus of normal SCs and attacked SCs.

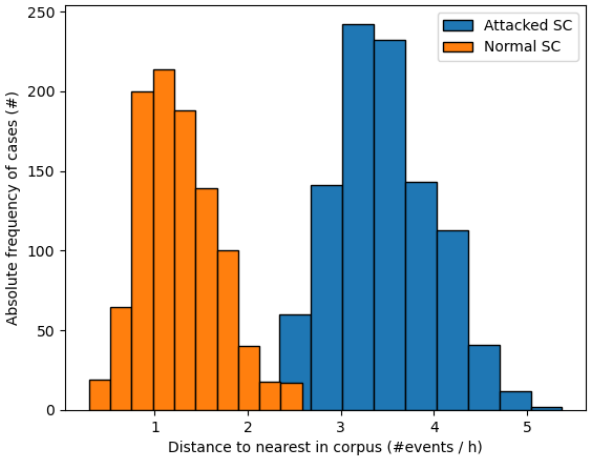


FIGURE 9. Absolute frequencies of distances of normal SCs and attacked SCs to corpus.

increased the number of events in meals, so the sum of events was higher in meal hours than in no-meal hours, and the minimum distance was obtained with a similar alignment to the one without attacks. However, the high difference in series distances reveals the perpetrated perception-layer attacks.

We simulated 1000 examples of realistic SC attacks, by applying different sequences of magnetic alterations increasing the number of door openings over a realistic normal SC signal. We also simulated 1000 realistic simulations of normal SC signals by considering three big meals (i.e. breakfast, lunch and dinner) at the common Spanish hours (i.e. 8 h, 14 h and 21 h) and two in-between optional small meals at common Spanish hours (i.e. 11 h and 17 h), all of which with random alterations of $\pm$1h. We simulated each in-between meal with a probability of 50% of taking place. We simulated the number of door events in big meals with stochastic values between 2 and 20, and the number of door events in actually occurring small meals with stochastic values between 1 and 6.

Figure 8 presents the results of the distances of the series of each simulation to a small corpus of three prototype series, considering the nearest neighbor. The distance values can be clearly distinguished between the two different categories (i.e. either with attack or not), although some few values of both categories overlapped in a small range of values. These results advocate that the novelty detector is useful for distinguishing normal usages from attacked SCs

Figure 9 shows the frequencies of the distances to the corpus in both cases. The overlapped cases are only around an average distance of 2.35 events/hour with a range of $\pm$0.25. However, most of the cases are distinguishable. This analysis of frequencies helped us to detect the right ranges to distinguish normal usages and attacked SCs to be incorporated in the novelty detector. We could also detect some small ranges of uncertainty.

TABLE 3. Classification results in attacked SCs.

	Number of Cases	Percentage (%)
Attacks properly detected	955	95.50
Attacks classified as unknown	42	4.20
Attacks wrongly classified	3	0.30

We applied the novelty detector with distance thresholds of 2.10 for classifying as normal cases and 2.60 for classifying as attacks in a new set of 1000 simulated attacks and 1000 simulated normal usages. Table 3 presents the classification results of the novelty detector when analyzing series from attacked SCs, and Figure 10 graphically shows these results with a circle chart. Most attacks were properly detected (i.e. 95.5%), and very few of these were wrongly classified as normal (0.30%). The remaining ones were classified as unknown. These few wrongly classified cases may be due to the fact that these random alterations on sensor inputs may have similar shapes to normal usages by chance.

Table 4 indicates the classification results when applying the novelty detector to the input series from normal usages. Figure 11 shows these classification results of normal SCs in a circle chart. One can observe that most cases were properly classified (96.5%), while the remaining ones where classified as unknown. The normal usages were never wrongly classified as attacks in this experimentation, but users with exceptional changes on the SC usage may look as attacks eventually in further experimentation in the future.

V. DISCUSSION

The appropriate classifications results have probably been obtained, thanks to the selection of both the analyzed time series and DTW distance for calculating similarity. Notice that although the difference in the number of door events per meal can be quite different in normal usages, the average difference is smoothed thanks to all the hours in which the SC is not used, like during the night and between meals,

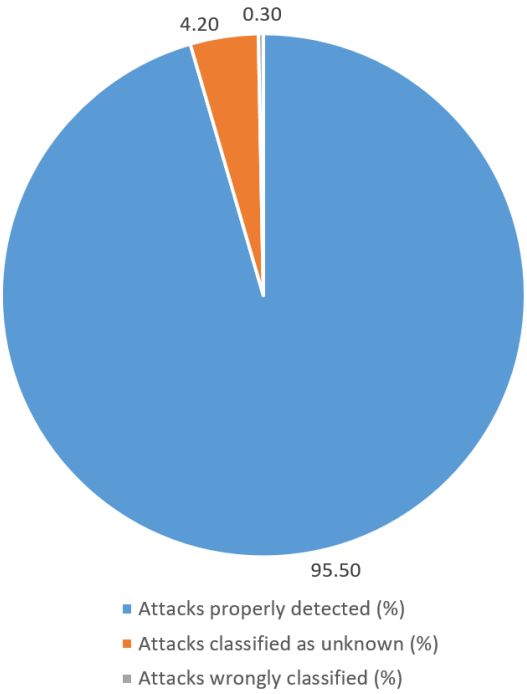


FIGURE 10. Results of the novelty detector when classifying attacked SCs.

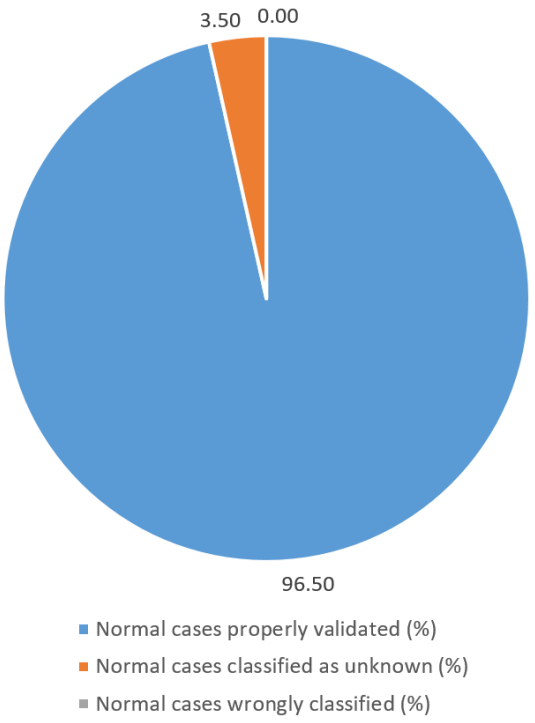


FIGURE 11. Results of the novelty detector in classifying normal SCs.

TABLE 4. Classifying results of normal SCs.

	Number of Cases	Percentage (%)
Normal cases properly validated	965	96.50
Normal cases classified as unknown	35	3.50
Normal cases wrongly classified	0	0.00

with commonly zero door openings in the case of normal usage. Notice that the specific times of the meals in different users barely influences the differences, given the nature of DTW distance, which is mainly aimed at comparing the shape rather than the paired values of each individual hour of the day.

Perception-layer attacks usually have very few slots of zero values on sensors, because they normally introduce fake perceptions so that real perceptions are disguised, and the whole information becomes worthless, for the difficulty of distinguishing real from fake perceptions. A key of the success of the proposed approach is this feature of this kind of attacks, since these fake perceptions reduce almost completely the in-between intervals with zero perceptions. Consequently, this significantly altered the shapes of time series, which were properly detected as anomalies by our proposed novelty detector. This applies to different kinds of smart furniture. For instance, door magnetic sensors of SCs can be easily attacked by new magnetic fields, but are difficult to suppress other magnetic fields. In fact, existing physical magnetic attacks on automobiles use the creation of magnetic fields rather than inhibition. For example, [15] analyzed automobile attacks that interfered on antilock braking systems and caused life-threatening situations based on perception-layer attacks on the magnetic sensors that measured wheel speed. Moreover, the same applies to load sensors of smart beds, in which perception-layer attacks would be probably introduced by pressing load sensors, as a total inhibition of these sensors would also be easily detected. This aligns with the literature on perception-layer attacks based on load sensors. For instance, load sensors are also integrated in critical systems in automobiles such as for operating on brakes [23]. In these cases, detecting fake loads is crucial for security.

It is worth highlighting that all the accuracy measures are represented for the analysis of each single day. Therefore, although 4.20% of the attacks cannot be classified on the first day and 0.30% of the attacks are wrongly classified as normal usages, these attacks may be detected on the next day. Hence, probably all attacks will be eventually detected if they are not detected on the first day. These first-day unperceived attacks are especially probable to be detected eventually if they have any stochastic component as most physical attacks, which make the input time series vary regularly. Even if the magnetic alterations of the attacks are not so variable, they can also be detected in combination with different user behaviors resulting in different time series. For example, users may change their cooking habits in different days, like over the weekend.

Given the relatively low probability of suffering magnetic perception-layer attacks, we calibrated the system to avoid unnecessary alerting the user with normal usages. We also added a new possible output (referred as unknown classification) of the system for uncertain classifications, i.e. the overlapping ranges of similarity between normal usages and attacks. This unknown classification also referred

as 'impossible to classify' output by other authors is quite common in classification and authentication literature. For example, frequently facial-authentication applications neither can verify or reject a person identity if they are not able to properly detect the faces [24]. In our experimental results, we observed that all the normal usages were classified either as normal usages (96.5% of the cases) or as unknown (i.e. 3.50% of the cases), but none of the normal usages was wrongly classified as an attack. In this manner, according to these results, users would not be unnecessarily alerted of false perception-layer attacks.

The proposed application detects attacks by analyzing long time series of 24 hours. However, in practical scenarios, attack events may happen in short time. In order to deal with such cases, the proposed approach could analyze short-time intervals depending on the domain, to detect short-duration attacks.

The problem of analyzing attacks after a long-time history is that when one realizes that has been attacked, the attack has already been perpetrated. To detect attacks in real-time, the proposed approach can be adapted to perform predictions of the next value based on the history and compare the current value with the next one predicted. In this way, attacks could be detected immediately. However, accuracy may decrease as in this case it would only be considering previous history and not following data. For applying this improvement, the similarity of the current series should be compared with time series until the same hour of the day, and then calculate a range of reasonable values. Then, the new value would be compared with the mentioned range to detect anomalies and consequently possible attacks.

VI. CONCLUSION AND FUTURE WORK

This work has presented a novel security approach for providing defenses against perception-layer attacks on IoT smart pieces of furniture. This approach has used DTW similarity for comparing input time series from specific sensor inputs for identifying anomalies with a novelty detector, previously trained from real normal data and some realistic potential perception-layer attacks. We illustrated this approach in the scenario of a SC with door magnetic sensors attacked with magnetic field variations for altering the perception of door events. The experimental results have shown the performance in identifying perception layer attacks and not unnecessarily warning the user on normal usages of the SC. More concretely in the experiments, none of the normal usages was classified as an attack, although 3.50% were not able to be validated. In addition, 95.5% of the perception layer attacks were properly identified, 4.20% of the attacks were not classified, and only 0.30% was wrongly classified as normal usages. Each of these statistics was performed per day of analysis. In several days, all the attacks will probably be identified if they are not detected in the first day.

In the future, the proposed approach is planned to be experienced with other IoT smart pieces of furniture and electrical appliances such as smart beds and smart fridges. In addition, we plan to incorporate different security defenses in SCs and test them against other kinds of realistic attacks so our SCs are ready for commercialization and assistance of impaired people in real life.

ACKNOWLEDGMENT

The authors would like to thank the management of Prince Sultan University (PSU) and the Renewable Energy Laboratory for their valuable support and provision of research facilities that were essential for the completion of this work.

REFERENCES

[1] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.

[2] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020.

[3] D. Sobnath, I. U. Rehman, and M. M. Nasralla, "Smart cities to improve mobility and quality of life of the visually impaired," in *Technological Trends in Improved Mobility of the Visually Impaired* (EAI/Springer Innovations in Communication and Computing). Cham, Switzerland: Springer, 2020, pp. 3–28.

[4] F. González-Landero, I. García-Magariño, R. Amariglio, and R. Lacuesta, "Smart cupboard for assessing memory in home environment," *Sensors*, vol. 19, no. 11, p. 2552, Jun. 2019.

[5] I. Garcia-Magarino, R. Lacuesta, and J. Lloret, "Agent-based simulation of smart beds with Internet-of-Things for exploring big data analytics," *IEEE Access*, vol. 6, pp. 366–379, 2018.

[6] I. García-Magariño, F. González-Landero, R. Amariglio, and J. Lloret, "Collaboration of smart IoT devices exemplified with smart cupboards," *IEEE Access*, vol. 7, pp. 9881–9892, 2019.

[7] J. Azar, A. Makhoul, R. Couturier, and J. Demerjian, "Robust IoT time series classification with data compression and deep learning," *Neurocomputing*, vol. 398, pp. 222–234, Jul. 2020, doi: 10.1016/j.neucom.2020.02.097.

[8] Y. Hu, P. Ren, W. Luo, P. Zhan, and X. Li, "Multi-resolution representation with recurrent neural networks application for streaming time series in IoT," *Comput. Netw.*, vol. 152, pp. 114–132, Apr. 2019.

[9] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based IoT security: Feasibility and suitability," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6396–6403, Aug. 2019.

[10] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.

[11] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019.

[12] S. K. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security enhancements to system on chip devices for IoT perception layer," in *Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS)*, Dec. 2017, pp. 151–156.

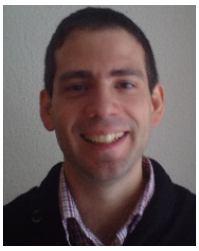
[13] S. Hauser, M. Mutlu, P.-A. Léziart, H. Khodr, A. Bernardino, and A. J. Ijspeert, "Roombots extended: Challenges in the next generation of self-reconfigurable modular robots and their application in adaptive and assistive furniture," *Robot. Auton. Syst.*, vol. 127, May 2020, Art. no. 103467.

[14] R. Frischer, O. Krejcar, P. Maresova, O. Fadeyi, A. Selamat, K. Kuca, S. Tomsone, J. P. Teixeira, J. Madureira, and F. J. Melero, "Commercial ICT smart solutions for the elderly: State of the art and future challenges in the smart furniture sector," *Electronics*, vol. 9, no. 1, p. 149, Jan. 2020.

[15] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2013, pp. 55–72.

[16] S.-J. Bu and S.-B. Cho, "A convolutional neural-based learning classifier system for detecting database intrusion via insider attack," *Inf. Sci.*, vol. 512, pp. 123–136, Feb. 2020.
[17] C. F. Libaque-Sáenz, S. F. Wong, Y. Chang, and E. R. Bravo, "The effect of fair information practices and data collection methods on privacy-related behaviors: A study of mobile apps," *Inf. Manage.*, Jan. 2020, Art. no. 103284, doi: 10.1016/j.im.2020.103284.
[18] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Gener. Comput. Syst.*, vol. 83, pp. 326–337, Jun. 2018.
[19] O. Eisen, "Catching the fraudulent man-in-the-middle," *Netw. Secur.*, vol. 2012, no. 6, pp. 18–20, Jun. 2012.
[20] H. Cai, X. Fu, and A. Hamou-Lhadj, "A study of run-time behavioral evolution of benign versus malicious apps in android," *Inf. Softw. Technol.*, vol. 122, Jun. 2020, Art. no. 106291.
[21] S.-F. Huang and H.-P. Lu, "Classification of temporal data using dynamic time warping and compressed learning," *Biomed. Signal Process. Control*, vol. 57, Mar. 2020, Art. no. 101781.
[22] A. A. Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," in *Proc. 3rd Int. Conf. Converg. Hybrid Inf. Technol.*, vol. 2, Nov. 2008, pp. 505–510.
[23] S. N. Gil and J. P. Terradas, "Mechanism with load sensor for operating a brake," U.S. Patent 7 490 699, Feb. 17, 2009.
[24] F. D. Guillén-Gámez, I. García-Magariño, J. Bravo-Agapito, R. Lacuesta, and J. Lloret, "A proposal to improve the authentication process in m-health environments," *IEEE Access*, vol. 5, pp. 22530–22544, 2017.

MOUSTAFA M. NASRALLA (Member, IEEE) received the B.Sc. degree in electrical engineering from Hashemite University, Jordan, in 2010, the M.Sc. degree (Hons.) in networking and data communications from Kingston University London, U.K, in 2011, and the Ph.D. degree from the Faculty of Science, Engineering and Computing (SEC), Kingston University. He is currently an Assistant Professor with the Department of Communications and Networks Engineering, Prince Sultan University, Riyadh, Saudi Arabia. His Ph.D. research was based on video quality and QoS-driven downlink scheduling for 2D and 3D video over LTE networks. His research interests include the latest generation of wireless communication systems, e.g., 5G, LTE-A, LTE wireless networks, M2M, the Internet of Things (IoT), machine learning, OFDMA, and multimedia communications. He is a Fellow of the Higher Education Academy (FHEA). He was a member of the Wireless Multimedia and Networking (WMN) Research Group. He received several distinguished reviewer awards from several reputable journals, such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON MULTIMEDIA, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Wireless Communications* (Elsevier), and *Computer Network* (Elsevier). He has recently received a funded project called Smart City and Adoption of 5G Technology in Saudi Arabia. He served as an Active Reviewer.



IVÁN GARCÍA-MAGARIÑO received the Ph.D. degree in computer science engineering from the Complutense University of Madrid, in 2009. From 2010 to 2014, he was a Lecturer with Madrid Open University. From 2014 to 2018, he was a Ph.D. Assistant Professor with the University of Zaragoza. He is currently a Lecturer and a Contributor with the GRASIA Research Group, Complutense University of Madrid. He actively collaborates with the EduQTech Research Group, University of Zaragoza on m-health projects, the HCI Laboratory, University of Udine, Italy, on human–computer interaction projects, the Institute of Technology Blanchardstown, Ireland, on datamining projects, and the Multicultural Alzheimer Prevention Program (MAPP), Massachusetts General Hospital and Harvard University (US) on m-health projects. His main research interests include agent-based simulators, multi-agent systems, and agent-oriented software engineering. Among journals, book chapters, conferences and workshops, he has over 135 publications (over 60 in journals with ISI Thomson JCR). He was a recipient of an FPI Scholarship, from 2006 to 2010. He is an editor in several journals and a guest editor in several special issues in journals with impact factor.

JAIME LLORET (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in physics, in 1997, the B.Sc. and M.Sc. degrees in electronic engineering, in 2003, and the Ph.D. degree (Dr.Ing.) in telecommunication engineering, in 2006. From 2012 to 2016, he was the Director of the University Master Digital Post Production. He worked as a Network Designer and an Administrator in several enterprises. He is a Cisco Certified Network Professional Instructor. He is currently an Associate Professor with the Polytechnic University of Valencia. He is also the Chair of the Integrated Management Coastal Research Institute (IGIC). He is also the Head of the Active and Collaborative Techniques and Use of Technologic Resources in the Education (EITACURTE) Innovation Group. He is also the Director of the University Diploma Redes y Comunicaciones de Ordenadores. He has led many local, regional, national, and European projects. He has authored 22 book chapters and more than 480 research papers published in national and international conferences, international journals (more than 230 with ISI Thomson JCR). Since 2016, he has been the Spanish Researcher with highest h-index in the Telecommunications journal list according to Clarivate Analytics Ranking. He is an Advisory Board Member of the *International Journal of Distributed Sensor Networks* (both with ISI Thomson Impact factor). He is an IARIA Journals Board Chair (eight journals). From 2010 to 2012, he was the Vice-Chair for the Europe/Africa Region of Cognitive Networks Technical Committee (IEEE Communications Society). From 2011 to 2013, he was the Vice-Chair of the Internet Technical Committee (IEEE Communications Society and Internet Society). From 2013 to 2015, he has been the Internet Technical Committee Chair (IEEE Communications Society and Internet Society). He has been the Co-Editor of 40 conference proceedings and a guest editor of several international books and journals. He is the Editor-in-Chief of *Ad Hoc and Sensor Wireless Networks* (with ISI Thomson Impact Factor), the international journal *Networks Protocols and Algorithms*, and the *International Journal of Multimedia Communications*. He is an Associate Editor-in-Chief of *Sensors* in the Section Sensor Networks. He is (or has been) an associate editor of 46 international journals (16 of them with ISI Thomson Impact Factor). He has been involved in more than 450 program committees of international conferences, and more than 150 organization and steering committees. He is currently the Chair of the Working Group of the Standard IEEE 1907.1. He has been the general chair (or co-chair) of 52 International workshops and conferences. He is ACM Senior and IARIA Fellow.