IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 8, 2020, accepted November 22, 2020, date of publication November 26, 2020,
date of current version December 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3040914

Secure IoT Analytics for Fast Deterioration Detection in Emergency Rooms

LOREDANA CARUCCIO[1], ORNELLA PIAZZA[2], GIUSEPPE POLESE[1], (Member, IEEE), AND GENOVEFFA TORTORA[1], (Senior Member, IEEE)

[1]Department of Computer Science, University of Salerno, 84084 Fisciano, Italy
[2]Department of Medicine and Surgery, University of Salerno, 84084 Baronissi, Italy

Corresponding author: Loredana Caruccio (lcaruccio@unisa.it)

ABSTRACT IoT data analytics can potentially bring benefits to several critical application domains, especially in healthcare. In fact, especially in emergency rooms the detection of critical patients can be a critical task when the number of patients to be monitored is high with respect to the available medical personnel. However, it is also necessary to pay attention to ethics, privacy, and security issues, aiming to prevent attacks and unauthorized access to sensitive data of patients, guaranteeing the correct functioning of the system in a secure environment. To this end, this article presents a knowledge representation framework enabling the intelligent video surveillance of patients, which can be used in combination with IoT-based systems to enhance the detection of critical patients in emergency rooms, while dealing with ethics, privacy, and security issues. These are guaranteed by means of an event-based visual access control specification method, constraining the access to both devices and users. We also describe a clinical scenario related to the early treatment of sepsis in an emergency room, showing how the proposed framework can enhance the detection of such critical disease while guaranteeing ethics, privacy, and security.

INDEX TERMS IoT data analytics, video surveillance, role-based and event-based access control, event modeling, ICU, knowledge representation.

I. INTRODUCTION

IoT and IoT Data Analytics methods are spreading in many different application domains, such as healthcare, video-surveillance, smart cities, and so on. However, if on one hand, they promise to bring increased efficiency in such domains, on the other hand, the management of so many connected IoT devices poses several problems, among which access control and privacy preservation. These become particularly critical in the context of healthcare, where also several ethical issues arise not only in preventing the disclosure of video recording of patients or results of machine learning algorithms on IoT collected clinical data, but also in the efficacy of treatments, which might be altered as a result of unauthorized access to patients data and related treatments.

Having the possibility to secure IoT-based systems would increase the possibilities of exploiting Evidence Based Medicine (EBM), supporting the clinician in deciding the most useful investigations and therapies based on the outcomes of relevant clinical trials. Thus, the introduction of advanced IoT devices for monitoring the status of patients, together with advanced IoT data analytics techniques can furtherly boost the employment of EBM within emergency rooms of hospitals, potentially enhancing the timeliness of critical diagnosis.

This article presents the system SPASM (Secure PAtient Surveillance and Monitoring) relying on visually specified event-based access control policies [1], and an event-based knowledge representation framework [2], enabling the secure and privacy-preserving usage of systems combining IoT data analytics and video surveillance, which can be effectively exploited in several application domains, and in particular in the medical domain. We have tuned the system and its underlying methods for usage in emergency departments of hospitals, where the usage of many connected IoT devices, together with IoT data analytics methods, can enhance the detection of critical patients also with medical personnel shortage. Nevertheless, this is such a context in which urgency could yield leakage of IoT collected data, or unauthorized access to them, potentially infringing severe privacy regulations.

Cybersecurity attacks represent a concern in many critical environments, being a threat for many organizations. For

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

instance, mitigating the risk of attacks towards the security and privacy of patients is a fundamental requirement for software systems used in healthcare. However, designing secure software systems can be nowadays a particularly complex task, since high-volume data are continuously generated and travel throughout networks, also connecting different kinds of devices. As a consequence, proper actions need to be undertaken not only to secure all resources, but also to mitigate the ability of attackers to navigate across resources of different infrastructure layers [3].

The knowledge representation framework underlying SPASM enables the modeling of scenarios based on video records, IoT data, and short textual descriptions, by means of Element of Context and Events Forms (ECE Forms). The latter provide a unified structure for capturing all the information necessary to perform inferences from textual, graphic, and hybrid textual/graphic information, which abounds in the medical and several other domains. SPASM also relies on visual language technologies to provide a visual policy editor enabling the user-friendly specification of event-based access control policies, which are automatically translated in XACML or other access control languages by means of visual language compilers. This is particularly useful in IoT settings, where the dynamic customization of access control policies becomes a particularly complex task, due to the possibly high number of heterogeneous IoT devices to monitor and the necessity to specify and/or verify who/what can be involved in the analysis process and for which tasks, also depending on the role owned in the given scenario.

SPASM and its underlying framework have been used to describe a clinical scenario related to the early treatment of sepsis in an emergency department, showing how they can effectively combine IoT data coming from cameras and other IoT devices to enhance the identification of critical diseases while simplifying the specification of complex policies to abide by severe regulations in healthcare.

The article is organized as follows: Section II introduces the related work illustrating the main approaches of the literature. The knowledge representation framework is presented in Section III. Section IV describes the SPASM prototype. The application of SPASM and its underlying framework to the clinical scenario of the sepsis is presented in Section V, whereas its evaluation is provided in Section VI by using a Pneumonia and Septic Shock scenario. Finally, conclusions and future developments are reported in Section VII.

II. RELATED WORK

In this section, we survey existing approaches and healthcare information systems, with particular emphasis on decision support systems supporting EBM, on privacy-preserving models applied in the healthcare domain, and on issues and solutions related to privacy preservation in IoT environments.

Several Decision Support Systems (DSSs) have been described in the literature [4]–[7]. In particular, in [4] Wu *et al.* assert that providing support to clinical decisions into the electronic patient record can enhance patient safety, decrease medical errors, minimize undesirable practice variations, and improve patient outcomes.

Zhuang *et al.* in [8] describe the specific case of the design of a framework for an intelligent DSS as part of medical examinations by General Practitioners. This approach highlights the processes of recognition of a specific pathology, stores this information, investigates and determines the elements determinants for decision through a poll on the examinations, and it meets the need for support in making decisions. Finally, it proposes a framework of intelligent decision support as a strategy for helping physicians to choose the appropriate test or analysis for diagnosis. The process and the framework developed orient the physician on the basis of past information (diagnosis) contained in the medical record of the patient.

In [9], Delir Haghighi *et al.* consider the problem of the emergency decisions provided on the basis of the experience and the knowledge of staff individual members who are directly involved. They show how it is important to collect and share into a knowledge base or domain ontology these types of experiences.

Finally, in [5] Fogli and Guida focus on the design of DSSs for helping emergency personnel in planning, coordination, and control of decisions taken in critical situations. A methodology is derived from a real case of emergency management during the pandemic flu emergency. A rational and structured approach supports the design ''knowledge-centered'' for modeling the knowledge about the environment, the domain of application, interested users and their tasks, and activities that the specific DSS expects to supply.

The necessity to develop secure intelligent systems to support clinicians in decisions concerning human lives, requires also the management of security and privacy issues, aiming to prevent any possible cybersecurity attack. To this end, many models have been proposed in the literature for guaranteeing security and privacy in the healthcare domain. Among these, in [10] a healthcare security model for transmitting medical data in IoT environments has been proposed. It integrates a stenography technique and hybrid encryption models to secure both diagnostic textual data and medical images.

Instead, in [11] biometry has been used to guarantee identification and authentication into the Naked environment. It aims to provide health services in a smart hospital environment without using specific gadgets for accessing the services. Moreover, medical sensors embedded in the environment provide users with the required digital services by employing a biometric-based authentication schema.

Finally, aiming to restrict any central authority for storing local access control policies in the healthcare domain, in [12] a distributed cross-domain access control model has been described. It provides flexible access control with resistance against reply attacks, attribute collusions, and privacy of attributes.

Privacy issues become particularly complex to manage in IoT environments. In fact, not only IoT devices can

collect and distribute "private" user information, but it is also necessary to manage access control mechanisms aiming to properly authorize resources and/or devices, also named entity authentication [13]. Authentication and access control mechanisms for IoT devices can also permit to protect sensitive information so that attackers cannot access user information if they compromise some devices [14]. For instance, in [15] two authentication processes are proposed to satisfy major security requirements for IoT-oriented Body Sensor Network (BSN) infrastructures, where the entity authentication is guaranteed through security credentials, and a secure communication channel permits to assure data integrity and confidentiality. Guaranteeing security on communication channels of IoT networks has been an extremely popular topic in the last few years. Many studies analyzed how existing protocols, platforms, and networking stacks can be applied to secure IoT systems, by also highlighting possible limitations concerning security issues [16]–[18]. Nevertheless, also some novel models and solutions have been proposed. For instance, in [10] authors propose a hybrid security model for securing the diagnostic text data in medical images, which uses a wavelet transform steganography technique with a hybrid encryption scheme employing AES and RSA algorithms. Finally, concerning privacy issues, a recent study tackles the possibility for an observer to derive sensitive data by relating contents according to features provided by smart objects involved in a Multi-network IoT system [19]. In particular, authors defined a new model for guaranteeing user privacy by applying k-anonymity and t-closeness privacy-preserving techniques, aiming to organize smart objects into groups, so as to mix-up features of objects inside a group, and to create a single external view.

III. ECE FORMS

Understanding clinical scenarios is a complex task. The use of IoT devices can potentially enhance the quality of diagnosis, but it entails the fact that several low-level data have to be composed in order to correctly interpret them. Moreover, it is important to be able to represent specific contexts, and to restrict the focus on the specific elements of them, in order to specialize the understanding effort to the relevant elements of the modeled scenario. In this way, it is possible to define events at several levels of complexity, which manage the information related to such elements of context. Another important task towards the representation/interpretation of a clinical scenario is to outline the way in which events might occur; in fact, in some cases, different sequencing of the same information may represent semantically different concepts of the same scenario.

According to these considerations we defined a knowledge representation framework to characterize specific elements of context and events that are involved in the management of clinical scenarios, with particular emphasis on those related to clinical anomalies. In particular, we introduce ECE Forms to convey the concept of events, which can be linked in a sequence of events, and composed by more elementary ones.[1] Moreover, by modeling anomalous scenarios through the proposed framework it possible to (1) exploit the stored knowledge to interpret the current events, by reducing events to the more elementary ones, and by using actual data to instantiate both elements of context and events; and (2) perform reasoning to supply lacking information in current events through inferential process on the events already occurred.

In the following subsections we describe how to use ECE Forms to model the elements of context (Section III-A) and the events (Section III-B), and how to define critical clinical scenarios in terms of event sequences (Section III-C).

A. MODELING ELEMENTS OF CONTEXT

The context of a clinical scenario can be considered as a set of relevant elements that describe a situation. The representation of these aspects through ECE Forms enables the characterization of specific elements that must be captured and monitored in order to correctly interpret a clinical situation. In particular, an element of context can be characterized through the following features, which enable a formal definition of it:

- *Type*. A scenario may contain different types of elements. The basic types through which it is possible to define the elements of context are *Actor* and *Object*. Starting from them, an element of context can be represented by new specialized types of other ones, so enabling the management of inheritance hierarchies.
- *Observer*. The same element of context can be observed by different devices, which can be considered as providers of information related to the element. As an example, if a patient is monitored through a *pulse oximeter*, it is possible to obtain information related to the *chardiac rhythm*.
- *Properties*. Several specific properties may belong to an element. The definition of properties in ECE Forms refers to properties that can be captured through observers and/or ad-hoc or well-known algorithms, such as feature extraction algorithms [21].
- *Entry condition*. In order to distinguish an element from others, some of them have to satisfy an *Entry Condition*. The latter also permits to consider an element as relevant in the scene. As an example, a *PATIENT* individual can be discriminated from a generic *PERSON* if it presents an entry condition specifying the *being on the bed* property.

Table 1 shows an example of element of context specification in which the features of a *PATIENT* are described.

B. MODELING EVENTS

The recognition and interpretation of a clinical situation require the recognition of single events into a specific scenario. When an event occurs it could lead to a side effect, yielding to possible changes in the context.

[1] ECE Forms represent a particular implementation of frames, so enabling the possibility to design Frame-based representation systems [20].

TABLE 1. An example of element of context.

PATIENT	
Features	**Description**
Type	Actor
Observer	Camera, Microphone, Thermometer, Pulse_oximeter, Sphygmomanometer, Rainbow Acoustic Monitoring
Properties	Location: XValue, YValue Area: dim Volume: VValue Frequency: FValue Cardiac_Rhytm: CRValue Oxigen_Sat: OSValue Arterial_Press: APvalue1, APvalue2 Temperature : Tvalue Resp_Frequency: RFvalue
Entry Condition	(IS ON, bed) (HAS, legs)

In terms of event representation, ECE Forms permits to characterize the features that must be used to interpret a specific event. In particular, an event can be characterized by the following features:

- *Type*. The type specifies the fact that an event might be *simple*, or be *composite* of several other events. In order to detect the former, it is necessary to simply analyze the instantiation of its properties. Instead, a composite event represents an event that depends on other ones. As an example, the *increase temperature* event related to a patient depends on simpler events, such as the *CHANGE_TEMP* event.
- *Elements*. We refer to the elements of context involved in an event. In general, an event could involve an *Actor*, an *Object*, a specific specific type depending on them, or an *ActorObject*. The latter is used when there are no constraints with respect to the types of elements that an event involves.
- *Rule*. The interpretation of an event is characterized by the definition of some rules. A rule can be a simple logic rule or a complex procedure, always returning a truth value. Moreover, it can use some properties of Elements of context that involves. As an example, the rule for the *CHANGE_TEMP* event has to simply catch the change of temperature on the monitored patient.
- *Effect*. The recognition of an event could yield to context update. This is characterized in terms of effects. The latter are very important due to the possibility for a system to manage changes in the context on basis of events that are occurring.

Table 2 shows an example of event specification in which the features of the *CHANGE_TEMP* event are described.

The main difference between Elements of context and Event forms is the fact that the first type of forms represents static knowledge that can be instantiated by users or as an effect in the context, after the recognition of an event. Instead, an event can be instantiated after the interpretation of the rule characterizing it. The interpretation of events can be also accomplished according to a dynamic recognition of scenarios, so enabling the dynamic selection of events involved in them.

TABLE 2. An example of event representation.

CHANGE_TEMP	
Features	**Description**
Type	Simple
Elements	Actor
Rule	Actor.Temperature ! = (GET_TEMP, Actor)
Effect	(SET_TEMP, Actor)

C. MODELING SCENARIOS

In order to let users define anomalous scenarios, it is possible to use a specification of the scenario composed by the definition of (1) the context, and (2) the sequence and composition of events that should occur. Such a recognition should yield to raising an alarm.

In other words, ECE Forms allow us to characterize the structure of the knowledge representing the elements of context and the events involved in a specific scenario. However, in order to define an anomalous scenario, it is necessary to only specify a sequence and/or composition of events, and the relevant elements involved in it. In particular, for sequencing events, it is possible to use different types of occurrences, which are described in the following.

- *Mandatory*. The recognition of a scenario is constrained to the occurrence of all mandatory events. In other words, a mandatory event is strictly required.
- *Optional*. Optional events are not strictly required. Thus, a scenario could be recognized even though one or more optional events do not occur. However, this type of events strengthens the scenario recognition.
- *One of*. An event can participate in a set of events in which a single event becomes optional if one or more other events occur.
- *Minimum number*. An event can participate in a set of events in which a minimum number of them must occur.
- *Jointly*. Some events can be considered relevant if and only if they occur together with some other ones.
- *Repeatable*. An event may also occur more than one time. It can be associated with a timer, whose aim is to define the period by which to apply the recognition of the event, and select a novel interpretation of it.

It is worth to notice that a single event can be specified with more than one occurrence types.

Visual Representation. To simplify the definition of events composition/sequence we also introduce a visual language, which represents events as circles that can be related to other ones by directed links. However, there exist several ways to connect event circles, and this defines how an event is instantiated in a scenario. The icons for the visual representation of instantiation modalities are shown in Figure 1.

In particular, a circle linked through a solid directed arrow defines how a *Mandatory* event can be specified, whereas

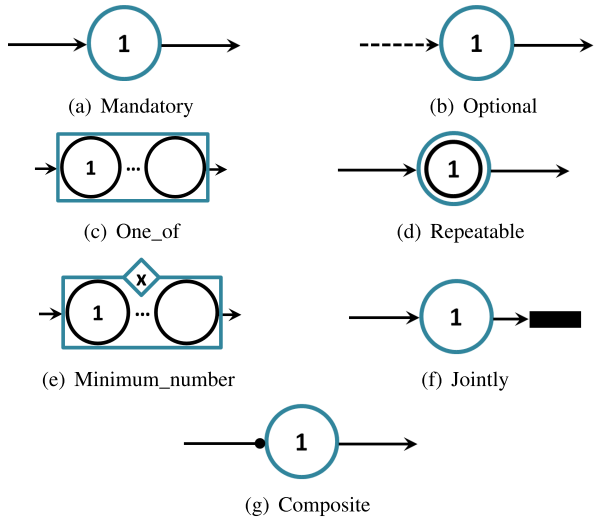

FIGURE 1. Visual icons for specifying the occurrence of events into sequences and compositions.

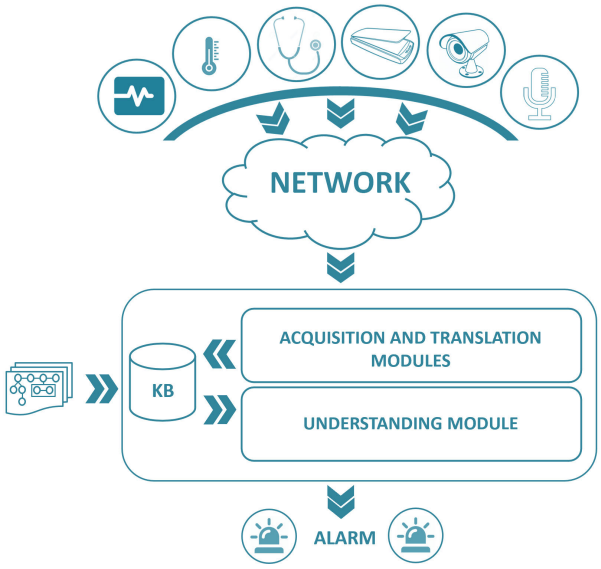

FIGURE 2. The system architecture.

to represent an *Optional* event a circle linked through a dashed directed arrow is used. A *One_of* set is specified by including the event circles in a rectangle shape; whereas an event included in a *Minimum_number* set is represented by including the event circles in a rectangle shape with a rhombus on the top, which contain the minimum threshold. Moreover, the *Jointly* occurrence of events is represented through event circles linked to the same black rectangle shape, and *Repeatable* events are modeled through double circles. Finally, an event can be composed of and depend on other ones, which must have been previously recognized. Finally, a circle linked through a directed arrow ending with a tiny circle is used to specify a *Composite* event.

The complete specification of example scenarios is described in Section V.

IV. THE PROPOSED SYSTEM

In this section, we describe the SPASM prototype, which implements the proposed framework. In order to detect events of anomalous scenarios, SPASM matches events originating from patient video records and IoT data against its stored knowledge of ''abnormal'' scenarios, described in terms of ECE Forms.

As shown in Figure 2, the system contains several types of input devices: audio/video devices and specific clinical IoT devices, such as thermometer, pulse oximeter, and Non-Invasive Blood Pressure (NiBP) measurement. These devices transmit data to the system's core across a network. The system's core two main layers, which group modules with the same goal: the acquisition and translation layer, and the understanding layer.

A. ACQUISITION AND TRANSLATION LAYER

The goal of modules involved in the acquisition and translation layer is to acquire the data and translate them in terms of properties of elements determining the context of the modeled scenarios. Modules represent ad-hoc and/or well-known algorithms that simply translate and store the data into a knowledge base, or analyze and synthesize them in order to produce a correct translation in terms of element properties.

As an example, the event detection process in a video is based on motion segmentation by means of automatic image analysis techniques and on object classification. Many algorithms can be used for motion detection [22]; we have employed the SGM (single Gaussian model) algorithm, proposed in the Pfinder system [23], which exploits a Gaussian model in order to classify the pixels of an image.[2]

B. UNDERSTANDING LAYER

The use of sequences/compositions of events representing relevant situations allows us to perform effective analysis and to logically infer updates of the context.

The modules involved in the understanding layer apply the current situation on the event sequences, by modeling the events that already occurred. When a scenario is identified, the system produces an alert signal. In fact, the defined scenario models are collected into a knowledge base, which can be used by means of three modules: *select*, *activate*, and *apply*.

With the *select* module the understanding of the current situation starts by selecting one or more event sequences from the knowledge base. This is performed by using the information coming from the acquisition and translation layer. Instead, the *activation* is the module which determines the

[2]SGM represents each pixel of an image by using an intensity-normalized color model, and classify pixels into the foreground/background class through a multi-way Gaussian classifier, trying to define blob clusters of foreground pixels. In particular, SGM compares pixels in the current frame to the background by computing the log-likelihood in color space, and by classifying a pixel as active when the likelihood is small and as background otherwise.

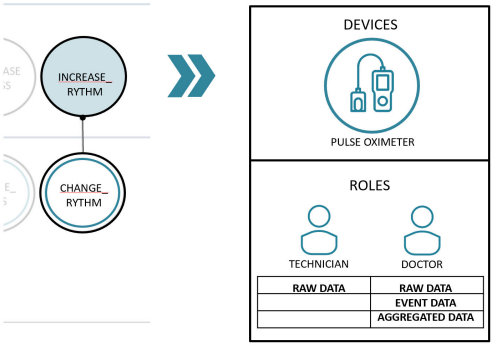

FIGURE 3. Event based access control method.

event sequence that should be used for processing the current situation. After the activation, an event sequence is *applied*, i.e., elements of context and events are instantiated from the situation being processed.

In particular, when a scenario model is used, it is possible to foresee the events that will occur according to the previously recognized ones. Thus, this leads to the detection of suspicious events and scenes in clinical situations.

C. ACCESS CONTROL METHODOLOGY

In the design of IoT healthcare systems, it is necessary to make a valuable effort on security aspects, in order to preserve human privacy and security. In fact, different kinds of attacks could be performed during the communication among IoT devices and/or with data consumers, or directly towards destination nodes [24]. For instance, Denial of Service (DoS) attacks aim to overburden the data transmission, in order to make a specific resource inaccessible. As another example, in reply attacks, the intruder starts sending messages when a transmitter stops sending data, after a considerable examination of the system's activities. To this end, SPASM also integrates an event-based access control mechanism that permits to dynamically select devices and users that can be involved during the processing and the activation of a specific critical scenario. It also exploits a visual editor providing the opportunity to visualize the automatically authorized devices for the interpretation of the event, eventually allowing/denying some of them, and finally admitting users for accessing specific levels of data processing, according to their role.

More specifically, in order to define access control policies, we use the eXtensible Access Control Markup Language (XACML) [25], which enables the definition of access control policies at different levels of detail, including the composition of policies, and the resolution of conflicts. Nevertheless, it is necessary to develop higher level languages from which XACML code could be automatically generated, since XACML is not a language simple to use [26]. To this end, the visual editor of SPASM permits to graphically visualize and customize access constraints for both devices and users.

SPASM automatically infers the devices that should be involved in the correct interpretation of an event, highlighting them into the visual editor (Figure 3). This enables the access of devices as *data transmitters*. In fact, even if a device can always send packets of data, the latter will be consumed if and only if there exists at least an event in the activated scenario that enables the device as a transmitter. In addition to automatically inferred devices, through the visual editor, it is possible to grant or deny the access of other devices during the understanding process of a critical scenario. On the other hand, for each event, it is possible to enable some users in the interpretation of patients' data, according to their roles. In particular, the access can be constrained at the following different levels of processing:

- *Raw data*, data transmitted by devices enabled as the transmitter for the interpretation of the event;
- *Event data*, event-based data and statistics concerning the activation of the event;
- *Aggregated data*, data and statistics concerning the interpretation of the current scenario.

More specifically, SPASM applies either default policies based on users' roles or policies customized at the event-level through its visual editor. In this way, authorizations can change depending on the criticality level of the current scenario in terms of already activated events.

In general, we assume several trust boundaries for the deployment of SPASM. In fact, although the proposed access control mechanism may lose its effectiveness without any control over the communication, the recent literature provides several communication standardized protocols for IoT applications, which also guarantee security during communications by means of encryption [27]. In particular, we assume that: i) SPASM is applied to a single room of Intensive Care Unit (ICU), where a proper set of IoT devices and a server are devoted to the online monitoring of a patient through SPASM; ii) when a patient is admitted to the room, SPASM is refreshed and re-initialized with the novel patient record, where all patient's personal data is obscured; iii) the credentials assigned to both devices and users during the registration phase are under a secure channel; iv) all the communications are made through a communication protocol which guarantees data encryption; v) the SPASM server is trusted and all the accesses to the knowledge base are safe.

V. A CLINICAL SCENARIO

In this section, an example scenario is described to illustrate the proposed framework. It describes a typical situation in which the patient is admitted to the hospital under observation, and s/he is monitored via audio/video devices (cameras, microphones), and clinical tools. The audio/video devices are designed to capture abnormal movements of the patient and/or specific physical conditions. As far as clinical IoT devices are concerned, they are normally used for the monitoring of patients in intensive care units, and they will be used to capture anomalous variations of the parameters involved (blood pressure, heart rate, temperature, etc.). Both the audio/video devices and clinical tools convey input data

TABLE 3. Patient vital signs.

(a) Initial vital signs

Parameter	Value
Heart rate	105/min
Blood pressure	130/69 mmHg
Respiratory rate	16/min
Body temperature	38,3 C
Oxygen Saturation	98%

(b) Degenerated vital signs

Parameter	Value
Heart rate	145/min
Blood pressure	110/51 mmHg
Respiratory rate	28/min
Body temperature	39 C
Oxygen Saturation	93%

to SPASM in order to enable it to detect emergency situations when they occur.

A. SCENARIO DETAILS

A 70 year old, male patient is admitted to the Emergency Department, in a separate, single bed area. The patient lies in his bed, and is monitored by audio/video devices and clinical tools that record his clinical parameters and behavior.

Initially, the patient has normal blood pressure, respiratory and heart rate, he is in a feverish state and his left leg is swollen and larger than the right one. The latter condition prompted his ED admission. The patient is able to speak, even if he is slightly grumpy and nervous. The anamnesis is positive for chronic cough and difficulty in breathing, due to COPD and thrombophlebitis at his left leg. Finally, the initial vital signs are shown in Table 3(a).

1) SYMPTOMS DEGENERATION

Later (in about one hour) the scenario changes. Clinical devices detect:

- further increase in body temperature,
- increased heart rate,
- increased respiratory rate,
- lowering of blood pressure.

The audio/video devices highlight:

- further increase in the left leg swelling,
- abnormal coloring of the left leg skin,
- abnormal and abrupt movements,
- alteration of the voice frequency,
- increase in the voice volume.

At this point of the scenario, the patient is more and more feverish, more tachycardic, his blood pressure falls, the patient breathes more quickly. Furthermore, the patient is extremely agitated, he starts moving sharply and abruptly, and tries to free himself from the monitor wires, he speaks faster and at a higher volume.

The blood test made earlier, but now disclosed to the physician, reports that the patient thrombophlebitis related ulcer is infected. The recorded vital signs after the symptoms degeneration are shown in Table 3(b).

The parameters and the patient's behavior reflect a high probability that this patient has contracted sepsis.[3]

However, medical personnel might initially underestimate symptoms like agitation and anxiety, associating them with a bad disposition of the patient. On the other hand, early detection of sepsis is vital, since time is a determinant of mortality.

Sepsis is a suitable field to apply the EBM approach integration. In 2004, the Surviving Sepsis Campaign published the international guidelines for the management of severe sepsis. Currently, the best clinical practice to benefit septic patients are basic care tasks [microbiological sampling and antibiotic delivery within 1 h, fluid resuscitation, and risk stratification using serum lactate], but performed timely. Future developments will focus on sepsis biomarkers and microarray techniques to rapidly screen for pathogens, risk stratification using genetic profiling, and the development of novel therapeutic agents targeting immunomodulation. The contribution of ITC is pivotal to sepsis care advance [28], [29].

2) COMPLICATIONS OF SEPSIS

Let us assume that the medical staff detects the symptom degeneration, hence they opt for making further rigorous examinations. More specifically, they perform a blood-gas test and apply an oxygen facemask. During the test, the patient raises his hand to his neck as a clear sign of labored breathing. Moreover, the monitor reports an alteration of vital parameters. In particular, the oxygen saturation parameter is no longer measurable (because of movement and/or low blood pressure, which reduces the signal). Consequently, the medical staff performs an electrocardiogram (EKG) that appears normal.

At this point, the medical staff performs an echocardiography and a lung ultrasound (LUS). The latter produces textual results, which highlight the presence of 4-5 B-type lines. The B-type are white lines with comet-tail shape, that are detected within the LUS. These comet-tail lines can be related to the presence of a pulmonary oedema. The absence of severe EKG abnormalities in the presence of a pulmonary oedema may be included in the sepsis scenario.

In this scenario, it is vital not only to effectively monitor the clinical parameters, but also to promptly detect all the symptoms and changes in patient behavior. However, in a typical emergency room (ER), often emergency physicians manage many critical patients at one time, and they are frequently interrupted. They work closely with emergency nurses and many other members of the healthcare team, which are often

[3] After years of study, the sepsis stands a major challenge to public health. Moreover, recently the incidence of sepsis has been increasing, and its mortality rate is still high. The current definition of severe sepsis requires the presence of organ dysfunction associated with infection. Septic shock is defined by the presence of sepsis associated with persistent hypotension after adequate volume replacement and the need for vasoactive drugs. Finally, a great variability with respect to phenotype, prognosis, and clinical outcomes is registered for patients classified as being in severe sepsis or septic shock [28]

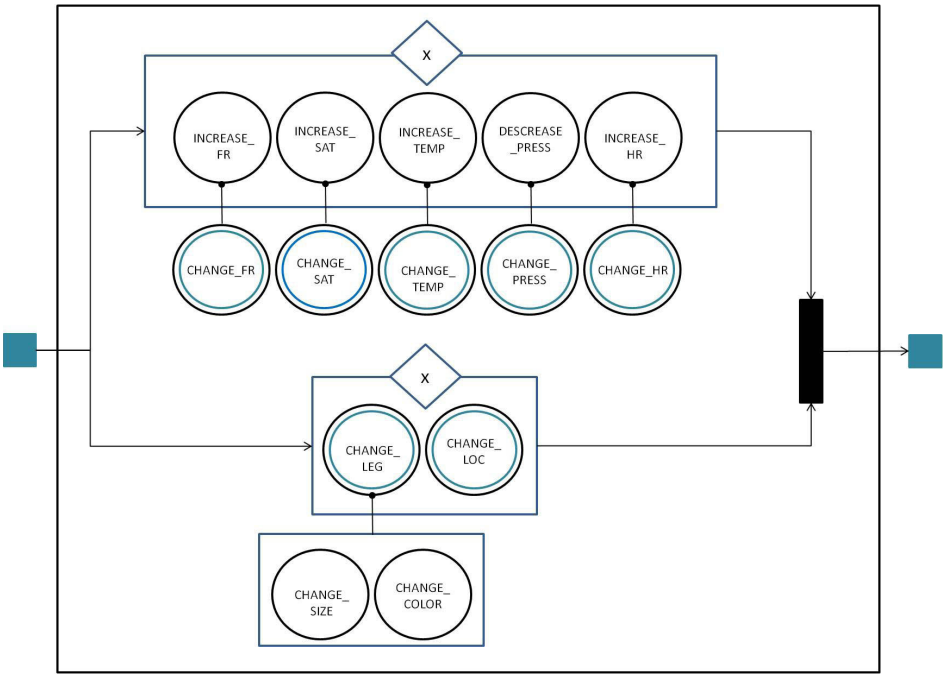

FIGURE 4. Model of the sepsis scenario.

understaffed, and might hence miss detecting some relevant events. In such and many similar scenarios, the proposed framework and system might be extremely useful to assist the healthcare team in surveying the patients, raising alerts, and providing suggestions. Thus, in what follows, we describe how to model this scenario through the proposed framework.

B. SCENARIO MODELING

The scenario presented in the previous subsection has been modeled in terms of elements of context and events through ECE Forms, as described in the following.

1) SEPSIS

Figure 4 shows a model for the sepsis scenario, which has been specified through the defined visual representation. It is applied to a set of elements representing the context of the scenario. In particular, in this scenario the relevant elements are: an *Actor* with his/her *legs*, laying *on the bed* (*PATIENT*), and the *Objects RIGHT_LEG*, *LEFT_LEG*, and *BED*. The latter has been specified as *CONSTANT*, since it cannot perform or be involved in any event modifying its properties. For each element, the basic properties are related to the specific observer monitoring it. In fact, the *XValue, YValue* of the element location and the *dimension* of its area are captured by a camera, and have been specified to all elements. However, only the element *PATIENT* presents properties related to the voice frequency (*Fvalue*), the cardiac rhythm (*CRvalue*), the respiratory frequency (*RFvalue*), the oxygen saturation (*OSvalue*), the arterial blood pressure (*APvalue1, APvalue2*), and the body temperature (*Tvalue*), captured by the microphone, the EKG monitor, the pulse oximeter, the sphygmomanometer, and the thermometer. Moreover, the *owner* property of the elements *RIGHT_LEG* and *LEFT_LEG* can be captured by checking the existence of the *(HAS, lleg, rleg)* entry conditions including these legs, and *BED* can be captured by checking the existence of the *IS_ON, bed)* entry condition including this bed. Finally, only the element *PATIENT* presents two *Entry Condition*s that are the previously cited *(HAS, lleg, rleg)* and *(IS_ON, bed)*.

The scenario is composed of two main groups of events included within *Minimum_Number* sets; they participate in a *Joinlty* set. The first group contains events detected through the microphone and medical devices, and represents the deterioration of symptoms of the patients in terms of increasing voice frequency, saturation, temperature, heart rate, and of decreasing blood pressure. Such events are composite ones, and depend on the change of the specific property events, which are even repeatable. The second group contains events detected by the camera and represents the symptoms degeneration of the patients in terms of his/her legs and of his/her location. Both events are repeatable, and the first one depends on a *One_of* set of events, which contains events managing the change of the leg color and/or the change of the leg size.

2) COMPLICATION OF SEPSIS

Figure 5 shows a model for the complication of sepsis scenario, which has been specified through the defined visual representation. It is applied to a set of elements representing the context of the scenario. Even in this scenario, the relevant elements are: an *Actor* with his/her *legs*, positioned *on the bed* (*PATIENT*), and the *Objects RIGHT_LEG*, *LEFT_LEG*, and *BED*. However, two properties have been added into the

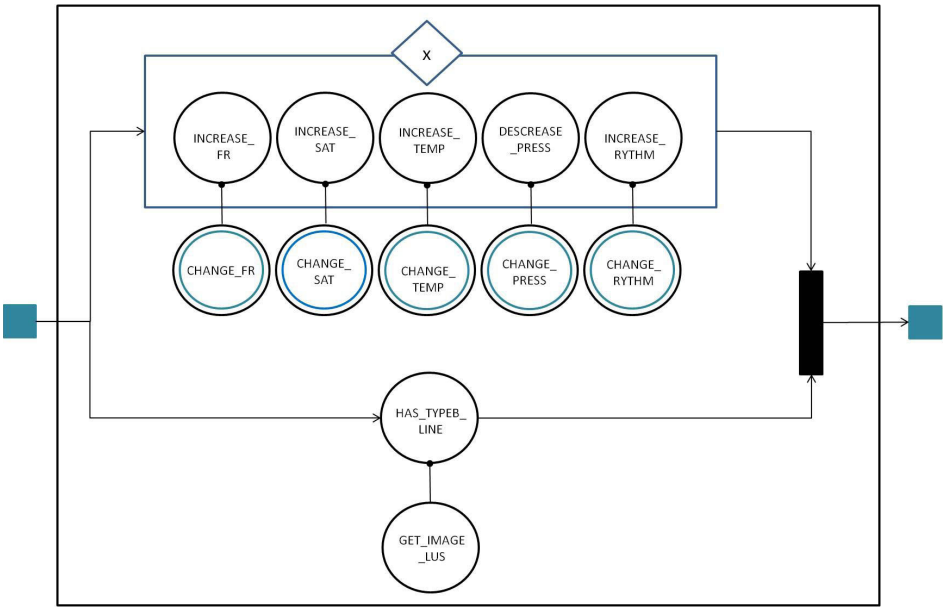

FIGURE 5. Model of the complication of sepsis scenario.

element *PATIENT*: the echo comet score (*ECSvalue*) and the emo gas analysis result (*EGAvalue*) obtained translating and synthesizing data of the observer *Electrocardiogram*.

The scenario is composed of one group of events included within *Minimum_Number* sets and another event participating in a *Joinlty* set. The group contains events detected through the microphone and medical tools, and represents the deterioration of symptoms of the patients in terms of increasing of voice frequency, saturation, temperature, cardiac rhythm, and of decreasing of the blood pressure. Such events are composite ones, and depend on the change of the specific property events; the latter are even repeatable. The other event detected by the electrocardiogram represents the symptoms degeneration of the patients in terms of the presence of at least four B-type lines. Such event depends on a simple event, which gets the *ECSvalue* detected through the analysis of the patient's electrocardiogram image.

VI. SYSTEM EVALUATION

In this section, we provide a preliminary evaluation of SPASM based on a typical ER scenario related to the detection of pneumonia and septic shock. Unfortunately, current regulations in healthcare prevent the possibility for a complete evaluation of the proposed system.

Several initiatives have been recently undertaken to establish what guidelines and principles can ethically guide digital innovation, particularly in the use of Artificial Intelligence (AI) to improve human lives. In particular, in 2019 the European Commission introduced the document ''Ethics Guidelines for Trustworthy AI'', which contains a list of seven requirements that AI systems should meet in order to be considered trustworthy [30]. While this witnesses the importance of AI systems and the interest for systematically adopting them in critical domains [31], there is still an extensive discussion on the interpretation of such guidelines, which prevents the effective exploitation of AI-based systems in healthcare and other critical environments. This is mainly due to the perceptions of users when they are involved in the process and should provide their consent (especially when the system-made decisions not only use their data, but also video records concerning them), like in the case of SPASM.

Thus, aiming to evaluate SPASM, in this section we present a hypothetical, though plausible ER scenario, and show how it would benefit from the use of the system of SPASM. In particular, we describe possible evolutions of the scenario when not using SPASM, and the expected developments when using it.

A 65 year old woman is admitted to the hospital with cough and fever (she had been suffering from these symptoms for 5 days). At a physical examination performed at 8:00 p.m., parameters are:

- Feverish (temperature: 38.5°C);
- tachycardic (heart rate: 97 bpm);
- hypotensive (blood pressure: 95/55 mmHg);
- Respiratory rate: 16 bpm;
- Chest: reduced breath sounds on the right lung, dull percussion tone at right lung base;
- Abdomen: Soft;
- Extremities: nothing.

A. SCENARIO EVOLUTION WITHOUT SPASM

A new patient record has been opened, in which patient vital parameters and results of the physical examination are registered. The doctor requests a Chest X-Rays, which shows a pneumonia with effusion, successively registered in the patient record.

The doctor goes to check the patient and observes an increase of the blood pressure, and that she is extremely agitated. S/he annotates this worsening in the patient record, applies a central venous access, and prescribes the infusion of 1000 ml saline plus the O2. Once again, the applied therapies are annotated in the patient record.

A nurse goes to check the patient, and takes note of her behavioral change, but this piece of information is not communicated to the new personnel arrived for the night shift, since in the meanwhile a dramatic car accident happened and a family of four was admitted to the ER: two children are bleeding, the father is dead, and the mother needs emergency brain surgery.

After 4 hours, the patient is in a coma, anuric, blood pressure and heart rate are unchanged. The sepsis progressed, in absence of proper antibiotic therapy.

B. SCENARIO EVOLUTION WITH THE SYSTEM

After opening the new patient record, and registering parameters and results of the physical examination, the system acquires it, together with monitoring information, and it outlines the context in terms of elements of context. In particular, elements of context ECE forms about the ''Patient'', ''Patient_Chest'', ''Patient_Abdomen'', and ''Patient_Extemities'' are filled. The doctor requests a Chest X-Rays, and once its report has been registered in the patient record, the natural language processing acquisition and translation module synthesizes the report, and new properties about pneumonia and effusion are included in the ''Patient'' and ''Patient_Chest'', in terms of admission pathologies and pathologies, respectively. Finally, all the scenario models concerning these characteristics are activated. In particular, according to the proposed event-based access control method, the patient records can only be visualized by medical personnel, such as nurses, clinicians, and so on. In this way, even if some other people, e.g. technicians, can access to raw data of some devices (see Figure 3), they cannot aggregate them with the patient data stored in his/her associated clinical record.

At 9:00 p.m., the patient status and early applied therapies are:

- hypotensive (blood pressure: 94/50 mmHg);
- status: very agitated;
- applied therapy: a central venous access (in order to administer large amount of IV fluids to correct the hypotension) was placed in the patient's right internal jugular vein;
- applied therapy: 1000 ml saline was infused;
- applied therapy: O2 is started by facial mask.

The system continues to acquire information from the camera and other monitoring tools, while the *agitation status* and the *increasing of blood pressure* events are detected and activated into the corresponding scenario models.

At 9.00 p.m. the doctor goes to check the patient, and after reading the system prompts becomes aware of the changes in the blood pressure and patient's behavior. Then, s/he prescribes the infusion of 1000 ml saline plus the O2, annotating it in the patient record, where the natural language processing acquisition and translation module synthesize it, triggering the writing of new prescription in the ''Patient'' form. It is worth to notice that the storage of new prescriptions is restricted to the role of ''Doctor''.

At 10.00 p.m., the patient status and parameters are:

- feverish (temperature: 39°C);
- tachipnoic (Repiratory rate: 30 bpm);
- status: quieter;

The system continues to acquire information from the camera and other monitoring tools, and the *change of status* and the *increase of respiratory* events are detected and activated into the corresponding scenario models. These events yield the ''Pneumonia and Septic Shock'' scenario model, hence the system raises an alarm, suggesting the antibiotic therapy for empiric treatment of community-acquired pneumonia and septic shock, following the reference in the EBM database, immediately after collecting specimen for microbiological tests. This would prevent the patient from going into a coma status.

This scenario shows how a system capable of processing a combination of alphanumeric data, video, diagrams, and text can effectively support the healthcare team in those monitoring activities which would suffer from the personnel shortage, potentially causing dangerous delays in emergency care. Moreover, the proposed event-based access control method is able to restrict to specific roles i) the visualization of data at different levels of detail, and ii) the possibility of carrying out actions, which could lead to the activation of some events.

In general, SPASM enables medical experts to build any possible model scenario, aiming to support the healthcare teams towards the recognition of a specific pathology and/or in general to monitor a specific kind of deterioration of the patient status. Nevertheless, although the applicability of SPASM on different real-world critical scenarios increases its scalability, it is important to properly test and verify the robustness of each defined scenario. To this end, it is necessary to evaluate how SPASM is able to recognize critical (modeled) scenarios.[4] In fact, in such a critical context, although the recall[5] (also named detection rate) would be the most important metric, since any missed clinical scenario can affect human life, also the precision[6] (also named positive predictive values) since it is important for clinicians to trust SPASM predictions. In general, the ability of SPASM to correctly recognize or not recognize critical scenarios over

[4]To evaluate results over a given set of evaluated scenarios, it is important to consider true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). In our context, true positives and true negatives represent correctly recognized and not-recognized critical (modeled) scenarios, respectively, false positives represent wrongly recognized scenarios, and false negatives represent missed critical scenarios.

[5]The recall denotes the fraction of correctly recognized scenarios over the number of critical scenarios to be recognized: TP/(TP+FN).

[6]The precision denotes the fraction of scenarios correctly recognized as critical with respect to the total number of scenarios recognized as critical (correctly and not correctly): TP/(TP+FP).

the total number of evaluated scenarios can be determined by means of accuracy.[7] Such a metric should be evaluated for each modeled scenario, and also to test the general functioning of SPASM. Moreover, the speed and the responsiveness of SPASM can be considered an important metric to evaluate. It is worth to notice that, although the robustness of SPASM mainly depends on the modeled scenarios, which require the involvement of domain experts to be defined, having modeled scenarios permits to make an autonomous monitoring tool also able to explain why a monitored real scenario has been recognized as critical. This not only permits to refine rules and models during the validation of scenarios, but it permits to tackle the automation bias problem.

VII. CONCLUSION

In this article, we have faced the problem of securing access to IoT-based systems to facilitate their exploitation in critical domains, such as healthcare. To this end, we have proposed the SPASM system relying on event-based, visually specified security policies and a knowledge representation framework enabling the analysis of recorded video scenes of patients and their clinical data collected through IoT devices, in order to timely recognize critical patients in ERs.

We have described how the use of SPASM in the context of a clinical scenario can enhance the timeliness of critical diagnosis like the sepsis one, while guaranteeing privacy and security of patients. In particular, access constraints can be graphically specified for both devices and users through a visual editor.

We provided a preliminary evaluation of the proposed system on a hypothetical although realistic scenario. Although ethical and practical difficulties related to ERs or Intensive Care Units (ICUs) prevented the possibility to perform real experiments in the healthcare domain, this virtual validation represents a first important step to follow the pathway of a new clinical application in a context where the patients cannot express their informed consent because of the severity of their clinical conditions. Moreover, installing any video recording is considered intrusive by the medical and para-medical personnel. A further consideration highlighting the difficulties in using novel digital technologies in the healthcare domain is that ethical considerations are not limited to security and privacy problems, even if they are evidently relevant, but they are extended to considerations about efficacy of treatments coming from EBM guidelines.

The potential advantage of having a secure tool that can assist continuous monitoring of the patient and, at the same time, combine clinical data collected through several IoT devices, is highlighted in one of the presented clinical scenario. The signs (the alterations in blood pressure, heart rate) and the symptoms reported by the patient, together with his/her behavioral change, are described by EBM literature and focused guidelines as significant indicators of a possible sepsis for which an immediate (6 hours) list of interventions is required.

In the future, other than evaluating the systems in other critical domains, we would like to evaluate its impact on the quality and costs of acute care compared with existing practice in a large clinical trial. Moreover, it would be useful to consider a distributed system architecture for SPASM, through which IoT devices are integrated into the communication and data transfer. Furthermore, proper solutions should be devised to prevent emerging attacks typical of distributed networks [32], [33].

[7] Accuracy = (TP+TN)/(TP+TN+FP+FN).

REFERENCES

[1] C. Bertolissi, M. Fernández, and S. Barker, "Dynamic event-based access control as term rewriting," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*. Springer, 2007, pp. 195–210.

[2] L. Caruccio, G. Polese, G. Tortora, and D. Iannone, "EDCAR: A knowledge representation framework to enhance automatic video surveillance," *Expert Syst. Appl.*, vol. 131, pp. 190–207, Oct. 2019.

[3] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," *IEEE Access*, vol. 6, pp. 25167–25177, 2018.

[4] R. Wu, W. Peters, and M. Morgan, "The next generation of clinical decision support: Linking evidence to best practice," *J. Healthcare Inf. Manage.*, vol. 16, no. 4, pp. 50–55, 2001.

[5] D. Fogli and G. Guida, "Knowledge-centered design of decision support systems for emergency management," *Decis. Support Syst.*, vol. 55, no. 1, pp. 336–347, Apr. 2013.

[6] M. Kumar, A. Sharma, and S. Agarwal, "Clinical decision support system for diabetes disease diagnosis using optimized neural network," in *Proc. Students Conf. Eng. Syst.*, May 2014, pp. 1–6.

[7] T. Zhao, "An ontology-based decision support system for interventions based on monitoring medical conditions on patients in hospital wards," M.S. thesis, Dept. Eng. Sci., Univ. Agder, Grimstad, Norway, 2014.

[8] Z. Y. Zhuang, C. L. Wilkin, and A. Ceglowski, "A framework for an intelligent decision support system: A case in pathology test ordering," *Decis. Support Syst.*, vol. 55, no. 2, pp. 476–487, May 2013.

[9] P. Delir Haghighi, F. Burstein, A. Zaslavsky, and P. Arbon, "Development and evaluation of ontology for intelligent decision support in medical emergency management for mass gatherings," *Decis. Support Syst.*, vol. 54, no. 2, pp. 1192–1204, Jan. 2013.

[10] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[11] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for naked healthcare environment," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[12] A. Salehi Shahraki, C. Rudolph, and M. Grobler, "A dynamic access control policy model for sharing of healthcare data in multiple domains," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2019, pp. 618–625.

[13] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.

[14] E. Bertino, K.-R. Choo, D. Georgakopoulos, and S. Nepal, "Internet of Things (IoT): Smart and secure service delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, 2016.

[15] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016.

[16] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.

[17] D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici, "A survey on secure communication protocols for IoT systems," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, 2016, pp. 47–62.

[18] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in *Proc. IEEE Int. Conf. Future IoT Technol.*, Jan. 2018, pp. 1–8.
[19] S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili, "A privacy-preserving approach to prevent feature disclosure in an IoT scenario," *Future Gener. Comput. Syst.*, vol. 105, pp. 502–519, Apr. 2020.
[20] P. D. Karp, "The design space of frame knowledge representation systems," SRI Int., SRI AI Center, Menlo Park, CA, USA, Tech. Note 520, 1992.
[21] I. Laptev, "On space-time interest points," *Int. J. Comput. Vis.*, vol. 64, nos. 2–3, pp. 107–123, Sep. 2005.
[22] J. C. Nascimento and J. S. Marques, "Performance evaluation of object detection algorithms for video surveillance," *IEEE Trans. Multimedia*, vol. 8, no. 4, pp. 761–774, Aug. 2006.
[23] C. R. Wren, A. Azarbayejani, T. Darrell, and A. P. Pentland, "Pfinder: Real-time tracking of the human body," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 780–785, Jul. 1997.
[24] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT smart health security threats," in *Proc. 19th Int. Conf. Comput. Sci. Its Appl. (ICCSA)*, Jul. 2019, pp. 26–31.
[25] OASIS. *Oasis Extensible Access Control Markup Language (XACML) V2.0 Specification*. Accessed: Nov. 24, 2020. [Online]. Available: http://www.oasis-open.org/committees/xacml/
[26] L. Caruccio, V. Deufemia, C. D'Souza, A. Ginige, and G. Polese, "A tool supporting end-user development of access control in Web applications," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 25, no. 02, pp. 307–331, Mar. 2015.
[27] B. H. Corak, F. Y. Okay, M. Guzel, S. Murt, and S. Ozdemir, "Comparative analysis of IoT communication protocols," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2018, pp. 1–6.
[28] S. Dugar, C. Choudhary, and A. Duggal, "Sepsis and septic shock: Guideline-based management," *Cleveland Clinic J. Med.*, vol. 87, no. 1, pp. 53–64, Jan. 2020.
[29] D. Hashimoto, E. Witkowski, L. Gao, O. Meireles, and G. Rosman, "Artificial intelligence in anesthesiology: Current techniques, clinical applications, and limitations," *Anesthesiology*, vol. 132, no. 2, p. 379, 2020.
[30] A. Hleg, "Ethics guidelines for trustworthy AI," *B-1049 Brussels*, 2019.
[31] L. Floridi, "Translating principles into practices of digital ethics: Five risks of being unethical," *Philosophy Technol.*, vol. 32, no. 2, pp. 185–193, Jun. 2019.
[32] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, 2018.
[33] W. Meng, W. Li, Y. Wang, and M. H. Au, "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling," *Future Gener. Comput. Syst.*, vol. 108, pp. 1258–1266, Jul. 2020.

LOREDANA CARUCCIO received the B.Sc. and M.Sc. degrees *(cum laude)* in computer science from the University of Salerno, in 2009 and 2012, respectively, and the Ph.D. degree in management and information technology in 2018. In 2017, she was a Visiting Student with the Hasso Plattner Institute, University of Potsdam. In 2020, she was an Adjunct Professor with the Department of Computer Science, Université Claude Bernard Lyon 1. She is currently an Adjunct Professor and a Postdoctoral Researcher with the Department of Computer Science, University of Salerno. Her research interests include data science, artificial intelligence, and web engineering. She regularly serves as a Reviewer in conferences and journals, such as *Data Science and Engineering* (Springer), *Information Sciences* (Elsevier), *Fuzzy Sets and Systems* (Elsevier), and IEEE Access. She is the Co-Chair of the 27th International DMS Conference on Visualization and Visual Languages (DMSVIVA).

ORNELLA PIAZZA is currently a full-time Associate Professor of anaesthesia and intensive care with the Department of Medicine, University of Salerno. She serves as a Professor of anaesthesia and intensive care for medical students and medical residents, dentistry students, radiographer, and student nurses at the School of Medicine, Salerno University. She has been the Head of the Division of Intensive Care and the Anaesthesia Department, Salerno University Hospital (Cava de' Tirreni), since 2015.

GIUSEPPE POLESE (Member, IEEE) received the Laurea degree *(cum laude)* in computer science from the University of Salerno, the M.Sc. degree in computer science from the University of Pittsburgh, USA, and the Ph.D. degree in applied mathematics and computer science from the jointed Universities of Salerno, Naples, and Catania. He was a Project Manager at Italian Airspace Company, Alenia. He is currently an Associate Professor with the University of Salerno, the Director of the Data Science and Technologies Laboratory, and the Coordinator of the master track in Data Science and Machine Learning of the master degree in computer science. He has been a Visiting Professor with the Computer Science Department, University of Pittsburgh (USA), and the Institute of Computational Science, University of the Italian Switzerland. His research interests include data science, artificial intelligence, information visualization, and web engineering. He is a member of ACM. He regularly serves as a Reviewer in journals and conferences in the fields of data science, big data, and information visualization. He is a member of the editorial board of the following international journals: *Information Systems* (Elsevier), the *ACM Journal of Data and Information Quality*, *Distributed and Parallel Databases* (Springer), *Multimedia Tools and Applications* (Springer), *International Journal of Software Engineering and Knowledge Engineering* (Kluwer), and *Translational Medicine @ UniSa*.

GENOVEFFA TORTORA (Senior Member, IEEE) was the Dean of the Faculty of Mathematical, Natural and Physical Sciences, University of Salerno, from 2000 to 2008. She is currently the Scientific Director of the Laboratory on Context-Aware Intelligent Systems, Department of Computer Science. She has been a Full Professor of computer science since 1990. She is the author or a coauthor of more than 290 articles published in scientific journals or proceedings of refereed conferences. She is a co-editor of three books. Her research interests include software engineering, visual languages and human–machine interaction, image processing and biometric systems, big data, data warehouses, data mining, and geographic information systems. She is a Steering Committee Member of the International Working Conference on Advanced Visual Interfaces, held in cooperation with ACM. She is the Program Chair and a Program Committee Member of several relevant international conferences. She is a Senior Member of the IEEE Computer Society and a member of ACM, European Association of Theoretical Computer Science (EATCS), and International Association of Pattern Recognition (IAPR). She is also a Reviewer of several international scientific journals and an Evaluator of research projects for Italian Ministeries, Regions, Universities, and a European Commission Member of the Board of Examiners for several researcher, associate professor, and full professor positions both at a national and at an international level. She is also an Editorial Board Member of high-quality international journals.