IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received March 23, 2019, accepted April 2, 2019, date of publication April 12, 2019, date of current version April 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2910087

Ontology-Based Security Recommendation for the Internet of Medical Things

FAISAL ALSUBAEI[1,2], ABDULLAH ABUHUSSEIN[3], AND SAJJAN SHIVA[1], (Fellow, IEEE)

[1]Department of Computer Science, The University of Memphis, Memphis, TN 38152, USA
[2]College of Computer Sciences and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
[3]Information Systems Department, St. Cloud State University, St. Cloud, MN 56301, USA

Corresponding author: Faisal Alsubaei (flsubaei@memphis.edu)

ABSTRACT Security and privacy are among the key barriers to adopting the Internet of Medical Things (IoMT) solutions. IoMT adopters have to adhere to security and privacy policies to ensure that patient data remains confidential and secure. However, there is confusion among IoMT stakeholders as to what security measures they should expect from the IoMT manufacturers and whether these measures would comply with the adopter's security and compliance requirements. In this paper, we present a recommendation tool that models IoMT concepts and security issues in addition to successively recommending security measures. The presented tool utilizes semantically enriched ontology to model the IoMT components, security issues, and measures. The developed ontology is equipped with context-aware rules to enable reasoning in order to build a recommendation system that empowers users to make well-educated decisions. The recommendation tool classifies IoMT security threats faced by IoMT stakeholders and automatically recommends security controls that have to be enforced for each threat. We have experimented the proposed tool with respect to the completeness and effectiveness of its output (i.e., security issues and recommended security measures). The results show that the tool was effectively able to recommend necessary security measures.

INDEX TERMS IoMT, Internet of Medical Things, healthcare, recommendation, security, privacy, IoT, stakeholder-centric, medical, health, ontology.

I. INTRODUCTION

The Internet of Medical Things (IoMT) has gained a great deal of adoption lately due to its many advantageous features, such as facilitating the management of diseases and drugs, improving treatment methods and the patient experience, and reducing costs. About 70% of healthcare organizations have already adopted IoMT [1]. In fact, one-third of IoT devices are found in the healthcare industry [2].

The haste to embrace IoMT technologies in the medical field without having strong security in mind poses a high risk. A warning from the Federal Bureau of Investigation (FBI) revealed that IoMT solutions are highly vulnerable [3]. In addition, utilizing a large number and wide variety of IoMT devices wirelessly transmitting sensitive medical data to the cloud introduces new risks to healthcare systems [4]. Moreover, a deficiency of security awareness among users (e.g., patients and medical professionals) can facilitate attacks on IoMT systems [5]. Such attacks include asset destruction, denial-of-service (DoS), medical data theft or manipulation, and therapy manipulation. The disastrous consequences of these attacks do not only disrupt the whole medical system (e.g., ransomware attacks) but also put the patients' lives at risk [6].

Ensuring the security of the IoMT is an urgent issue worthy of further investigation and development. Security cannot be planned for, managed, monitored, or controlled if issues are not identified. Due to the rapid increase of IoMT solutions and the constant development of IoMT technologies, security assurance poses problems for IoMT adopters. These problems exist especially when choosing proper and robust security measures. Therefore, our contribution in this paper is an IoMT security recommendation tool that consists of two main functionalities. (1) It identifies potential security issues that could affect an IoMT scenario. (2) Based on these issues, it recommends a list of security measures. In addition, it provides IoMT adopter with a means to ensure the effectiveness of these measures. This tool helps IoMT stakeholders to comprehend IoMT risks that may be confusing due to practical limitations, such as unknown security vulnerabilities and

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

technical complexity. As a result, this increases IoMT users' awareness and promotes accountability and transparency between IoMT adopters and solution providers.

The rest of this paper is organized as follows. Section II briefly discusses the components of IoMT. Section III discusses the motivation for this work. Section IV summarizes the related work. Section V presents the problem formalization. Section VI explains the recommendation process that includes the IoMT scenarios and the recommendation results. Section VII provides a use case scenario of the tool. Section VIII presents the evaluation of the proposed tool. Section IX presents the limitations of the proposed tool and future work. Finally, section X concludes this paper with some final remarks.

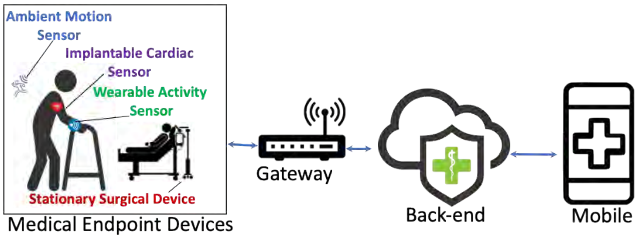


FIGURE 1. IoMT typical components.

II. BACKGROUND

The typical IoMT system archetypes include endpoints, gateway, back-end, and mobile (Figure 1). They are defined as follows [7]:

- **Endpoints:** The Global System for Mobile Communication Association (GSMA) defined endpoints as physical computing devices that perform a task such as sensing as a part of an Internet-connected product or service, including wearable fitness devices [8]. The U.S. Food and Drug Administration (FDA) defined a medical device as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease [9]. It also defined connected medical devices as medical devices that are connected to the Internet, hospital networks, and other medical devices 10]. In this work, we also include devices that are not medical in nature but that can be used in IoMT systems, such as ambient sensors used in ambient assisted living (AAL).
- **Gateway:** Networking devices that aggregate data and enhance the connectivity of weak endpoints by acting as a bridge network to the back-end.
- **Back-end:** Most contemporary IoT systems use cloud-based platforms to provide centralized back-end management capabilities, such as backups, data storage, ecosystem administration, reports and analytics, and web interfaces.
- **Mobile:** Mobile applications are utilized in many IoMT systems to provide back-end management, control of endpoints, and analytics.

III. MOTIVATION

This paper discusses our work to resolve the challenges encountered in IoMT that arise from (1) the boundless diversity in IoMT solutions and (2) the multiple-stakeholder dilemma.

A. THE BOUNDLESS DIVERSITY IN IoMT

IoMT solutions are not limited to hospital devices. Solutions for outpatients, such as over-the-counter and in-home medical devices, are also becoming increasingly prevalent. This great quantity and diversity of IoMT solutions has made the associated security issue increasingly critical and difficult to trace and control [11]. This is mainly attributed to the following factors: (1) as IoT is an emerging field, healthcare manufacturers have rushed to embrace IoT technologies only focusing on the functionality and overlooking crucial aspects such as built-in security. (2) There is a lack of standards in IoT in general and IoMT specifically. Despite the FDA's efforts to standardize medical devices, including connected devices, only 10% of these devices are classified under the FDA Class III. This includes devices designed to support or sustain life, such as pacemakers [6]. This lack of standards allows solution providers to design their own proprietary security measures, which are not always compatible with the existing standards and systems, thus introducing risks. (3) The extreme heterogeneity of IoMT solutions that often comprise different types of devices, such as wearable, ambient, implantable, and stationary devices, in large numbers. Each type of device poses its own security risks. (4) There is a wide range of IoMT use cases each requiring different sets of solutions, including cloud-based, mobile-controlled, and gateway-dependent. (5) IoMT solution providers often have different offerings of the same security measure, such as network monitoring, encryption, and bandwidth. These factors increase the complexity of IoMT solutions, introduce security challenges, and increase the attack surface. This boundless diversity motivates the need for a systematic, detailed, and expendable approach to accurately recommend scenario-specific security considerations.

B. THE MULTIPLE-STAKEHOLDER DILEMMA

The diversity of stakeholders also introduces new challenge dimensions to IoMT security. This is attributed to the following. (1) Different IoMT stakeholders often have different security objectives. For instance, patients normally care about the privacy of their medical data more than others. Hence, the recommendation process must consider these differences. However, since IoT and the cloud are new concepts, some stakeholders may not know how their security priorities are applied in such complex systems in real life [12]. In a recent survey, only 15% of medical professionals were aware of potential security issues in IoMT systems and took serious measures to prevent them [13]. (2) IoMT adopters' unfamiliarity with security solutions and risks often leads them to overlook the security countermeasures and focus more on other aspects, such as functional features, price, and performance. (3) In addition, due to the variety of IoMT solutions and their components, IoMT adopters can obtain complex and overlapping solutions. For example, a hospital system administrator can obtain a cloud-based IoT platform that controls connected medical sensors in an IoMT patient-monitoring system. In this system, medical professionals can use mobile applications to analyze the patients' collected data. However, every stakeholder in such complex scenarios needs to assess the security and make a decision based on their perspective. If this is not considered when recommending security, there will be a lack of consensus among stakeholders regarding the accountability of security in the IoMT solution [14]. This dissension leaves adopters unsure about which security measures are relevant to their solutions [15].

Due to these factors, IoMT stakeholders often have no option but to accept the default security offered in the solutions. Consequently, there is a need for a conceptual framework under which challenges to recommending security measures may be resolved in some uniform and comprehensive manner. This suggests the need for presenting a tool to identify security issues and recommending security contingencies. In addition, it enables adopters to understand these issues and to verify that the risks are identified, managed, and controlled. It also enables adopters to ensure that security measures reflect their particular requirements, which depend not only on the scenario, but on the adopter's assets and tolerance to risks.

IV. RELATED WORK

Many standards and guidelines have been published by specialized organizations to highlight the security risks and controls in IoT. In its discussion of the security of IoT, the Cloud Security Alliance (CSA) described both challenges, including attack surfaces, and implementation suggestions [16]. The Open Web Application Security Project (OWASP) maintains a regularly updated security analysis of IoT that includes vulnerabilities, attack surfaces, and framework assessments, among others [17]. In addition, European data protection authorities have discussed the protection of privacy and data in IoT and have provided some implementation guidelines to meet legal frameworks [18]. The GSMA has published a list of security questions that can be used in assessing the protection of IoT [19]. Although these works constitute important contributions to the issue at hand, they do not provide solutions specific to the unique medical environment that consider the increased sensitivity of data and criticality of operations in IoMT environments.

Moreover, many researchers have presented general security guidelines for IoMT. Laplante *et al.* presented a structured approach for describing IoMT while providing an abstract overview of security requirements within it [20]. Similarly, Islam *et al.* provided an attack taxonomy as part of their general survey that can be used to determine the technical security requirements needed to assess IoMT solutions [21]. Williams and Woodward identified general issues that contribute to a potentially insecure IoMT environment, such as consolidated reporting, context expertise, governance, regulations, resilience measures, standards, and technical controls [22]. Even though these works give useful hints to IoMT adopters so they can better understand the IoMT security issues, they do not provide an automated solution to support decision making.

In addition, Savola *et al.* presented security considerations for IoMT that include an analysis of risk-driven security metrics for elderly and disabled people from the perspective of the service provider and end users. According to every stakeholder, they identified the main risks and their impact along with a list of security considerations for each risk [23]. However, this work focuses on a limited set of use cases, such as patient monitoring, and does not scale well to broader use cases, such as medication management systems, among others [24]. In like manner, many organizations have published security guidelines for medical devices. The FDA issued a guide named *Postmarket Management of Cybersecurity in Medical Devices* [25]. The International Organization for Standardization (ISO) has many released and under-developed standards [26]. Similarly, the Naval Medical Logistics Command (NMLC) has provided a risk assessment questionnaire for medical devices that is used in the U.S. military [27]. However, these efforts target device manufacturers and do not consider other stakeholders, such as medical professionals. They also provide abstract and generalized security recommendations that primarily focus on one part of IoMT environments (endpoints) to the exclusion of others, such as mobile and back-end.

In our work, we propose a recommendation tool that draws upon all of the previously mentioned works. These works and others were systematically analyzed and combined to thoroughly cover the security considerations for all IoMT scenarios. For every IoMT scenario, the recommendation tool identifies a list of scenario-specific security issues along with their countermeasures. It also recommends a scenario-specific list of attributes (questions) to assure security in the measures. This tool educates the adopters about the risks associated with their potential IoMT solution. It also alleviates their efforts in choosing secure solutions, as they need only to refer to one list of security considerations that contains the most relevant measures to their IoMT scenario.

V. PROBLEM FORMALIZATION

This section describes the problem in abstract mathematical and algorithmic (see Algorithm 1) forms as follows:

- *Stakeholder (set):* Let $T = \{t_1 = \mathit{System\ administrator}, t_2 = \mathit{Patient}, t_3 = \mathit{Medical\ professional}\}$ be the set of the most important stakeholders in IoMT systems, which is described in the next section.
- *Solution (set):* Let $S = \{s_1 = \mathit{Device}, s_2 = \mathit{Service}, s_3 = \mathit{Platform}\}$ be the set of IoMT

Algorithm 1 The recommendation

```
    e: an IoMT scenario
Input: $Stakeholder_e, Solutions_e, Architectures_e$
Output: $Issues_e, Measures_e, Attributes_e$
for all $Solution$ in $Solutions_e$ do
  if $Solution$ in $Solutions_{Stakeholder_e}$ then
    if $Solution_{Components}$ not in $Components_e$ then
      add $Solution_{Components}$ to $Components_e$
    end if
    if $Issues_{Solution}$ not in $Issues_e$ then
      add $Issues_{Solution}$ to $Issues_e$
    end if
    for all $Architecture$ in $Architectures_e$ do
      if $Architecture$ in $Solution_{Architectures}$ then
        if $Component_{Architecture}$ not in $Components_e$
        then
          add $Component_{Architecture}$ to $Components_e$
          if $Issues_{Architecture}$ not in $Issues_e$ then
            add $Issues_{Architecture}$ to $Issues_e$
          end if
        end if
      end if
    end for
  end if
end for
for all $Component$ in $Components_e$ do
  if $Issues_{Component}$ not in $Issues_e$ then
    add $Issues_{Component}$ to $Issues_e$
  end if
end for
for all $Issues$ in $Issues_e$ do
  for all $Measure$ in $Measures_{Issue}$ do
    if $Measure$ not in $Measures_e$ then
      add $Measure$ to $Measures_e$
    end if
    for all $Attribute$ in $Attributes_{Measure}$ do
      if $Attribute$ in $Attributes_{Stakeholder_e Requirement}$ then
        add $Attribute$ in $Attributes_e$
      end if
    end for
  end for
end for
return $Issues_e, Measures_e, Attributes_e$
```

solutions types, which is described in the next section. $\forall t \in T, \exists S_t \subset S$that includes only the solutions relevant to the stakeholder t.

- *Architecture (set):* Let $R = \{r_1 = Gateway - dependent, r_2 = Gateway - independent, r_3 = Wearable, r_4 = Implantable, r_5 = Stationary, r_6 = Ambientr_7 = Mobile - controlled, r_8 = Web - controlled, r_9 = Cloud - based, r_{10} = On - premise\}$ be the set of the deployment architectures in IoMT solutions, which is described in the next section. $\forall s \in S, \exists R_s \subset R$ that includes only the architectures relevant to the solution s.
- *Component (set):* Let $C = \{c_1 = Endpoint, c_2 = Gateway, c_3 = Mobile, c_4 = Back - end\}$ be the set of the typical IoMT components, which were described in section 2. $\forall r \in Rands \in S, \exists C_r, C_s \subset C$ that include only the component(s) relevant to the architecture r and solution s, respectively.
- *Requirement (set):* Let $Q = \{q_1, q_2, \dots q_n\}$ be the set of stakeholder security requirements, which is described in the next section. This includes data confidentiality, physical security, and Regulatory Compliance, among others. $\forall t \in T, \exists Q_t \subset Q$ that includes only the most important security requirements for stakeholder t.
- *Issue (set):* Let $I = \{i_1, i_2, \dots i_n\}$ be the set of security issues that threaten all IoMT solutions, which is described in the next section. This includes unauthorized access, DoS, and data breach, among others. $\forall r \in R, s \in S, c \in C, \exists I_r, I_s$, and $I_c \subset I$ that includes only the issue(s) relevant to the architecture r, solution s, and component c, respectively.
- *Measure (set):* Let $M = \{m_1, m_2, \dots m_n\}$ be the set of all security measures to address (i.e., detect, prevent, and/or respond to) the potential issues in IoMT solutions as described in the next section. Such measures include secure data storage, intrusion prevention, and authentication, among others. $\forall i \in I, \exists M_i \subset M$ that includes only the measures that address the issue i.
- *Attribute (set):* Let $A = \{a_1, a_2, \dots a_n\}$ be the set of all attributes to assure the security of the measure. $\forall m \in M, q \in Q, \exists A_m$, and $A_q \subset A$ that includes only the attributes relevant to the measure m and requirement q, respectively. For example, the attributes to verify the effectiveness of the "Authentication" measure, include: *- Does every medical device use a unique password or cryptographic identity? Do medical devices require users to authenticate themselves to access or perform any task?*
- **The recommendation**: $\forall Scenario\ e = \{t_e \in T, S_e \subset S_{te}, R_e \subset R_{Se}\}, \exists I_e = I_r^e \cup I_s^e \cup I_c^e, M_e = M_I^e, A_e = A_M^e \cup A_{Qte}^e$

Example: x is a scenario of a patient monitoring solution where a *patient* uses a *mobile*-connected *wearable device* that collects clinical-grade readings such as electrocardiogram (ECG) and blood pressure. The mobile application provides many *services* for patients, such as analyzing and sharing medical data, which is also stored in the *cloud*, with doctors. In this scenario, $t_x = patient$, $q_t^x = \{Data\ confidentiality, Data\ integrity, Data\ availability, Operation\ availability\}, S_x \subset S_t, = \{Device,\ Service\}, R_x \subset R_s = \{Cloud - based, Mobile\ controlled\}, C_x = C_r^x + C_s^x = \{Backend,\ Mobile,\ Endpoint\}, I_x = I_r^x + I_s^x + I_c^x = \{Physical\ tampering, Unauthorized\ access, Denial\ of\ service, etc.\}, M_x = M_I^x = \{Physical\ security, Authentication, Intrusion\ Prevention, etc.\}, A_x = A_{Mx}^x$.

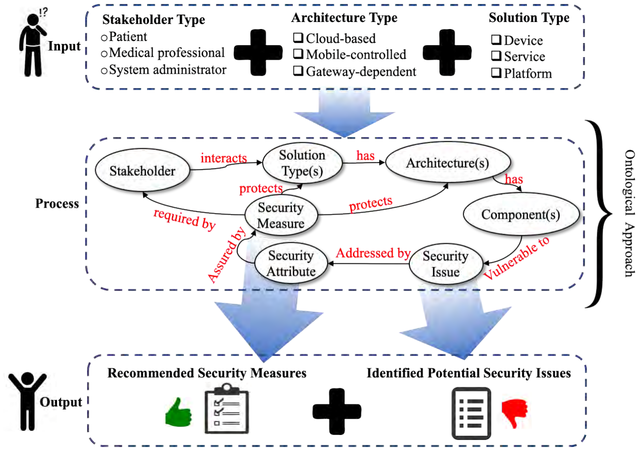


FIGURE 2. The recommendation tool structure.

VI. THE RECOMMENDATION TOOL

The recommendation tool (Fig. 2) is a Python-based web application that accepts an IoMT scenario as input, identifies its potential security issues and recommends their countermeasures. The tool also provides a list of attributes (questions) for each countermeasure to verify its effectiveness. The recommendation approach utilized in this tool includes the following qualities:

- **Ontology-Inspired:** This means using an approach that reinstates the autonomy and singularity of objects while maintaining that objects exist independently of their qualities. The ontology-inspired approach models and accesses knowledge into a structured description of IoMT-representative features of a real-world entity and relations. This methodological arrangement of properties is employed to delineate the different use cases of IoMT solutions and to facilitate extensions and upgrades in the future.
- **Stakeholder-Centric:** IoMT stakeholders have different roles when interacting with solutions as well as different security requirements and responsibilities. Thus, this work considers three main IoMT stakeholders: patients, medical professionals, and system administrators. Patients utilize connected medical devices, such as wearables, to easily and continually monitor their health or for diagnostic purposes, such as imaging devices used in hospitals. They can also utilize devices like drug pumps as a part of their treatment to enhance it. Medical professionals, such as physicians, nurses, pharmacists, and medical lab technicians, analyze the data generated by IoMT endpoints or operate them in order to collect data, such as heart rate. System administrators are individuals with technical expertise, including IT and programming, whose main duties are architecting, operating, monitoring, and controlling IoMT systems.
- **Scenario-Based:** Hypothetical scenarios are employed to aid researchers in working through complex problems. Scenarios for interacting with IoMT solutions consist of a stakeholder, solution type(s), and architecture(s). IoMT solutions can take many forms classified as follows: devices that can be wearable sensors, such as heart monitors; implantable devices, like embedded cardiac function monitors; ambient sensors, like door sensors; or stationary devices, like computerized tomography scanners. Most devices offer embedded connectivity capabilities, while others do not, consequently requiring a dedicated networking gateway. In addition, IoMT services, which often are web or mobile applications, are used to extend device capabilities beyond sensing to provide medical analytics and offer enhanced integration with other systems. Moreover, IoMT platforms, which are primarily cloud-based, are used to facilitate the use of smart devices and applications. IoMT platforms provide centralized back-end management capabilities, such as backup, data storage, ecosystem administration, reports and analytics, and web interfaces. Usually, IoMT solutions are combinations of these types. For example, AIRSTRIP ONE is a platform that provides a mobile service to allow medical professionals to receive instant alerts and view analytics of the data collected from the devices [28]. BL Healthcare provides a home monitoring solution that integrates all of the aforementioned solution types into one [29].
- **In Line With Available Guidelines:** This tool adheres to IoMT characteristics and security guidelines from specialized organizations such as the FDA, OWASP, GSMA, ISO, and others.

A. THE TOOL INPUT: IoMT SCENARIO

As shown in Fig. 2, each scenario consists of a stakeholder who interacts with at least one IoMT solution that has at least one architecture. Our recommendation tool considers known and real scenarios. In other words, not any combination of the scenario parameters can form a valid scenario. For example, patients do not use an IoT platforms. Hence, such scenarios are not considered, and the recommendation tool prompts a message to indicate that. However, the tool records and analyzes newly selected scenario entries to be considered in the future if needed. This input constructs the set of ontology rules that are discussed in the following section to determine the security issues and their measures.

B. THE PROCESS: ONTOLOGY

We have conducted a comprehensive study to review and catalog the potential threats faced by IoMT stakeholders and have determined the security controls. Based on this study, we have developed an ontology (Fig. 3) describing the IoMT scenarios and their pertinent security issues and controls. The main components of an ontology are concepts, relations, instances, and axioms. The ontology components are described as follows:

- **Concepts** represent a set or a class of entities in the IoMT model. The main classes of the proposed ontology are *stakeholder*, *solution type*, *architecture*, *security issues*, *security measures*, and *security attributes*.

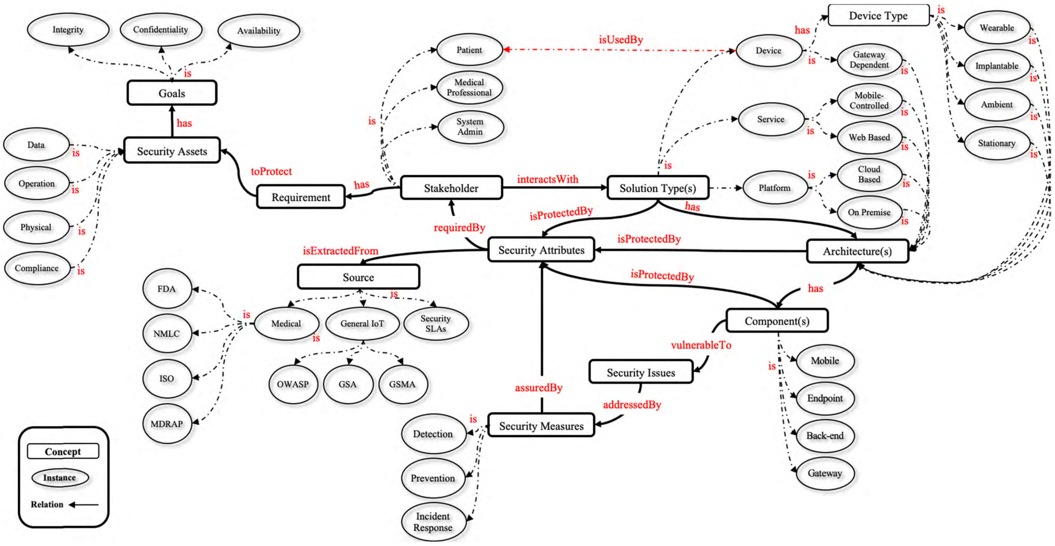


FIGURE 3. The IoMT security ontology.

A description of our ontology classes is presented in section 5.

- **Instances** are the things represented by a concept. In the proposed IoMT ontology, '*stakeholder*' is a concept whereas '*patient*' is an instance of the concept.
- **Relations** describe how concepts interact among themselves. For example, a stakeholder interacts with an IoMT solution. Relations can also be used to represent instances of concepts. To illustrate, IoMT device types are wearable, implantable, ambient, or stationary.
- **Axioms** are assertions used to constrain values for concepts or instances. These are represented by properties that show on the relation arrows. For example, the following axioms talk about two concepts in our IoMT ontology, '*stakeholder*' and '*solution type*', where one property is *interactsWith*and three instances are patient, medical professional, and system admin.

$$\mathit{Instance\ Of}\ (\mathit{patient},\ \mathit{stakeholder}\ )$$

$$\mathit{Interacts\ With}\ (\mathit{solutionType},\ \mathit{stakeholder})$$

$$\mathit{Instance\ Of}\ (\mathit{device},\ \mathit{solutionType}\ )$$

$$\mathit{isUsedby}\ (\mathit{patient},\ \mathit{device\ AND\ service})$$

The first axiom shows that a patient is an instance of stakeholder, whereas the third axiom shows that device is a type of solution type. The second axiom shows that every instance of stakeholder interacts with at least one instance of solution type. The fourth axiom shows that only device and service instances are used by patients. Axioms are also used to assert special relationships among concepts and their instances. For example, in our ontology, the components that are related to the solutions that a stakeholder interacts with form the attack surface. This is how the ontology identifies the security issues and recommends measures for every component. Some special rules such as the relationship between the security issues and measures are not shown in the ontology (Fig. 3) due to space limitations. Moreover, it is also important to consider the details of each component because this improves the identification of specific security issues and their countermeasures. For example, implantable devices often are not vulnerable to physical tampering. Similarly, cloud-specific issues, such as unauthorized access due to virtual machine (VM) jumping, and their countermeasures should not be recommended unless the solution is cloud-based.

TABLE 1. IoMT stakeholders' security requirements.

Security requirement	Patient	Medical professional	System administrator
Data confidentiality	[30] [31] [32] [33] [34] [30] [35]	[36] [37]	[36]
Data integrity	[30]	[36]	[36]
Data availability	[34] [38]		[36]
Data accountability			[36]
Operation confidentiality			[36]
Operation integrity		[36]	[36]
Operation availability	[30]	[36] [37]	[36]
Operation accountability		[36] [37]	[36]
Regulatory compliance		[37]	[36]
Physical security		[37]	[36]

Patients' and medical professionals' security concerns about the use of technology in general as well as IoT in particular, have been well investigated in the past. Table. 1 summarizes the stakeholders' main security requirements. In addition to these findings, we also considered the technical/security knowledge among the stakeholders. As shown in Table. 1, patients' main concerns are data confidentiality, integrity, and availability and operation availability. While system administrators are responsible for maintaining IoMT systems, all security requirements are crucial.

C. RECOMMENDATION OUTPUT

The output of the recommendation tool consists of two lists (see Fig. 2), which are: (1) scenario-specific security issues and (2) scenario-specific security measures. The latter also includes the attributes to verify the measures' effectiveness in addressing the issues. Both are described in the following subsections.

TABLE 2. Representation of the ontology traversal.

Property	Scenario x	
Stakeholder	Patient	
Solution	Wearable device + Service	
Architecture	Cloud-based + Mobile-controlled	
Sample of identified security issues and recommended measures		
Component	Issues	Measure
Endpoint	Eavesdropping	• Secure connectivity • Web security
Mobile	Unauthorized access	• Authentication • Intrusion prevention
Back-end	Data Breach	• Cloud service isolation • Secure data storage • Privacy

1) SECURITY ISSUES

The IoMT solutions are vulnerable to various security issues. The list of IoMT security issues was carefully identified, collected, and categorized in our previous work [39]. Using a revised and expanded version of the list, this tool identifies only the security issues that are related to the scenario. These issues are categorized based on their attack surface (the IoMT component), and one issue can affect multiple components. Table. 2 shows a sample representation of the ontology traversal for scenario x that was previously mentioned in section 5. Since the tool is based on a systematic ontological design, the list of IoMT security issues can be easily revised and updated to ensure its relevance to current IoMT security issues.

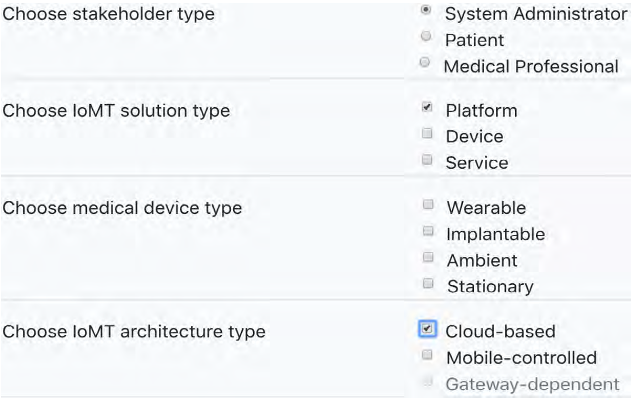
2) SECURITY MEASURES AND ATTRIBUTES

As shown in Table. 2, security measures are also recommended for each issue in order to improve adopters' understanding of how to address (i.e., detect, prevent, and/or respond to) the issues. Multiple security measures can be used to secure one component from at least one issue. The full list of security measures that includes 43 security measures for all IoMT components was carefully identified, collected, and categorized in our previous work [40]. As shown in Table. 3, the tool also provides security attributes for each of the recommended security measures in order to effectively determine its quality. The attributes are organized in a hierarchy, in which level 1 (Table. 3, first column) denotes IoMT components, level 2 (second column) denotes the security measures that protect the component from potential security issues, and level 3 (third column) includes the attributes to verify the security measures' effectiveness.

These attributes are in the form of yes/no questions so that adopters can easily answer and integrated into a quantitative assessment method. The scenario-specific attributes are carefully selected from the large pool of security considerations discussed in our previous work [40]. These attributes are created by systematically reviewing the related works and analyzing security requirements and combining them into a detailed list of questions that address any IoMT scenario. The sources used to curate the attributes (mentioned in section IV) include but are not limited to: (1) Medical-specific sources, such as security considerations provided by the FDA [10], ISO [26], NMLC [27], and the Medical Device Risk Assessment Platform [41], among others. (2) General IoT security considerations provided by OWASP [17], CSA [16], GSMA [19], and others [18]. (3) Available documentation that describe the security in popular IoMT solutions of every type. As IoMT evolves rapidly, the list of attributes will be updated as needed.

TABLE 3. Sample list of recommended attributes for selected measures.

Component	Measure	Attribute
Endpoint	Secure connectivity	Do medical devices support end-to-end encrypted communications?
Mobile	Authentication	Do mobile devices or their applications support biometrics authentication (e.g. fingerprint, face recognition)?
Back-end	Cloud service isolation	Does the back-end cloud hypervisor defend against network/data vulnerabilities (e.g., VM jumping), which can be caused by sharing of physical resources?



Choose stakeholder type
● System Administrator
○ Patient
○ Medical Professional

Choose IoMT solution type
☑ Platform
☐ Device
☐ Service

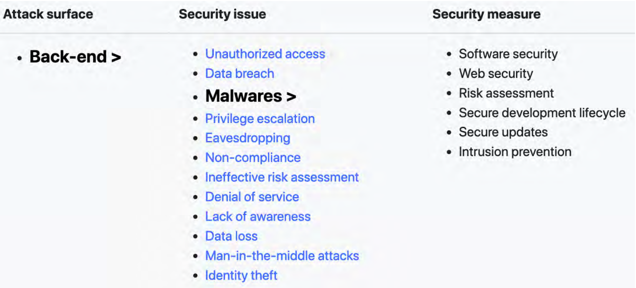
Choose medical device type
☐ Wearable
☐ Implantable
☐ Ambient
☐ Stationary

Choose IoMT architecture type
☑ Cloud-based
☐ Mobile-controlled
☐ Gateway-dependent

FIGURE 4. The new recommendation page showing user input for scenario *y*.

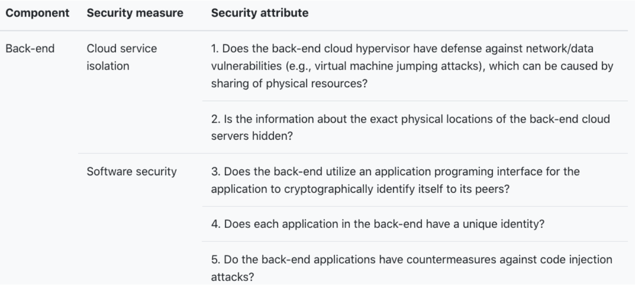
VII. CASE STUDY

In the previous section, we presented an abstract scenario x that is relevant to many real IoMT solutions, such as *AliveCor* [42] and *QardioCore* [43], both of which are considered over-the-counter health monitoring solutions. In this section, we provide a real-world use case to demonstrate how our tool can be used to recommend security using different scenarios. Fig. 4 shows the page corresponding to a new recommendation, where the user enters a new scenario y, where $y = \{administrator, platform, cloud\text{-}based\}$. In this scenario, the stakeholder is an administrator of IoMT cloud-based platforms like *Kaa*. which is an IoT cloud-based platform that allows healthcare systems to establish cross-device connectivity and implement smart features into medical devices



Attack surface	Security issue	Security measure
• Back-end >	• Unauthorized access • Data breach • **Malwares >** • Privilege escalation • Eavesdropping • Non-compliance • Ineffective risk assessment • Denial of service • Lack of awareness • Data loss • Man-in-the-middle attacks • Identity theft	• Software security • Web security • Risk assessment • Secure development lifecycle • Secure updates • Intrusion prevention

FIGURE 5. A sample of the security issues and measures for scenario *y*.



Component	Security measure	Security attribute
Back-end	Cloud service isolation	1. Does the back-end cloud hypervisor have defense against network/data vulnerabilities (e.g., virtual machine jumping attacks), which can be caused by sharing of physical resources?
		2. Is the information about the exact physical locations of the back-end cloud servers hidden?
	Software security	3. Does the back-end utilize an application programing interface for the application to cryptographically identify itself to its peers?
		4. Does each application in the back-end have a unique identity?
		5. Do the back-end applications have countermeasures against code injection attacks?

FIGURE 6. A sample of the recommended attributes for scenario *y*.

and related software systems [44]. As shown in Fig. 5, back-end is the only component in this scenario. The identified issues in this scenario include malwares, denial of service, unauthorized access, and others. The recommended security measures associated with these issues include software security secure development lifecycle, risk assessment cloud service isolation, intrusion prevention, and others. Fig. 5 shows a sample list of attributes that can be used to ensure the effectiveness of the measures.

Our tool helps users to know the security issues that might affect these solutions and how they can be addressed. For example, in scenario *y*, the tool identified the security issue found in *Kaa* (vulnerability number 15 in Table 4) in which malwares can be executed by injecting malicious code. The tool also recommended the measures (e.g., software security, etc.) that address this issue along with detailed attributes to ensure the effectiveness of measures. On the other hand, solution providers may use the recommended attributes as a checklist to ensure the security of their products. In addition, the tool can help in forensic investigations where an attack can be traced back to its cause and affected components. This helps in discovering the weakness of a system (e.g., Kaa's insecure software) that were exploited and/or in order to be addressed.

VIII. EVALUATION

The goal of the presented tool is to help users to comprehend the security issues that might arise from adopting IoMT solutions in order to prevent severe consequences. To verify tool efficiency in helping users to achieve these goals, we need to evaluate the completeness and effectiveness of the tool output (i.e., security issues and recommended measures). In the following subsections, we evaluate the effectiveness of the presented tool using two different methods (i.e., Vulnerability-based and Expert-based).

A. VULNERABILITY-BASED EVALUATION

Since this tool can be considered an expert system, evaluation methods used in such systems can also be applied here. Some expert systems like medical diagnoses, have had detailed and structured protocols established in order to evaluate their quality objectively. However, there is lack of such protocols for the cybersecurity in general and the IoMT security in specific. Therefore, to verify the extensiveness of the tool objectively, we tested its ability to identify and address all known IoMT real-life security issues. We gathered a list of reported IoMT-related vulnerabilities as of October 2018 from NIST's National Vulnerability Database (NVD) [45] and CVE Details [46] for the last three years to ensure their recentness. The keywords used in this extensive search are IoT, IoMT, medical, health, medical device, and healthcare. Upon filtering all found vulnerabilities to exclude those that are irrelevant to IoMT, such as non-medical endpoints, we found 40 distinct vulnerabilities (Table. 4). Then, we analyzed the details of each vulnerability and assigned it to at least one possible scenario based on its stakeholder, solution type, and the architecture type. As a result, we categorized these vulnerabilities under 11 distinct scenarios. Then, for every vulnerability, we checked whether its known security issue(s) had been identified by the tool for its related scenario. We found that our tool was able to successfully highlight all of the security issues as well as the missing or inadequate security measures. The tool was also able to recommend necessary security attributes that are directly related to the vulnerabilities. Table. 4 shows the results of our analysis for each vulnerability along with its corresponding scenario, Common Vulnerabilities and Exposures (CVE) ID, identified potential issue(s), recommended security measure(s) and their attribute(s) that pertain(s) to the vulnerability. It is very likely that every vulnerability is addressed by more than one security measure and by more than one attribute. Since our tool was able to work with diverse scenarios and address their different issues, this shows that it can scale well to different scenarios and unknown vulnerabilities. This also demonstrates the tool's extensibility and ability to work with different use cases.

To verify the effectiveness of the tool in capturing missing or inadequate security measures, we analyzed two commercial IoMT solutions that are known to have/had serious security issues. Smiths Medical Medfusion 4000 syringe infusion pump is stationary medical endpoint that is used to deliver small doses of medication in acute care settings [47]. This pump can be programmed wirelessly through PharmGuard, a Medication Safety Software that helps reduce pump programming errors and associated adverse drug events by encouraging the use of drug libraries with hard and soft limits. This IoMT solution was found vulnerable to at least eight serious security issues (vulnerabilities 1 to 8 in Table. 4).

TABLE 4. **IoMT vulnerabilities and their recommendation results.**

Scenario				Vulnerability			Sample of relevant tool output	
#	Stakeholder	Solution	Architecture	#	CVE ID	Issue	Measure	Attribute
1	Medical professional	Device, Service	Stationary	1	2017-12718	Malwares	Software security	Is the written code of endpoints thoroughly inspected to ensure that it is protected from reverse engineering and vulnerabilities like buffer errors?
				2	2017-12720	Unauthorized access	Authentication	Do medical devices require users to authenticate themselves to access or perform any task?
							Access control	Do medical devices implement effective access controls (e.g., attribute-based, discretionary, mandatory, rule-based, role-based)?
				3	2017-12721	Man-in-the-middle attacks	Secure connectivity	Does the gateway renegotiate and verify communication security keys each time it reconnects to the communication network?
				4	2017-12722	Unauthorized access	Memory protection	Do medical devices enforce memory protection using memory management units or memory protection units?
						Denial of communication	Secure connectivity	Does the communication protocol used by medical devices devalue the effects of DoS attacks to deal with and recover from disruptions to its communications?
							Software security	Is the written code of endpoints thoroughly inspected to ensure that it is protected from reverse engineering and vulnerabilities like buffer errors?
				5	2017-12723	Data breach	Secure data storage	Are all data stored in medical devices (configurations, sensor readings, authentication credentials, and cryptographic keys) securely encrypted?
				6	2017-12724	Unauthorized access	Authentication	Do medical devices ensure that default or hard-coded passwords are not used?
				7	2017-12725			
				8	2017-12726			
2	Patient	Device, Service	Stationary	9	2015-1011	Unauthorized access	Authentication	Do medical devices ensure that default or hard-coded passwords are not used?
				10	2015-1012	Data breach	Secure data storage	Are all data stored in medical devices (configurations, sensor readings, authentication credentials, and cryptographic keys) securely encrypted?
				11	2015-3955	Malwares	Software security	Is the written code of endpoints thoroughly inspected to ensure that it is protected from reverse engineering and vulnerabilities like buffer errors?
				12	2015-3957	Data breach	Secure data storage	Are all data stored in medical devices (configurations, sensor readings, authentication credentials, and cryptographic keys) securely encrypted?
				13	2015-3958	DoS	Secure connectivity	Does the communication protocol used by medical devices devalue the effects of DoS attacks to deal with and recover from disruptions?
				14	2015-3459	Unauthorized access	Authentication	Do medical devices require users to authenticate themselves to access or perform any task?
							Access control	Do medical devices have effective access controls (e.g., attribute-based, discretionary, mandatory, rule-based, role-based)?
3	Administrator	Platform	Cloud-based	15	2017-7911	Malwares	Software security	Do the back-end applications have countermeasures against code injection attacks?
				16	2017-11496	Malwares	Software security	Are the back-end applications designed to mitigate buffer errors using the operating system's mechanisms?
				17	2017-11497			
				18	2017-11498			
				19	2016-9353	Data breach	Secure data storage	Are the back-end authentication credentials (usernames, passwords, device ids) hashed and salted before stored?

TABLE 4. ***(Continued.)*** **IoMT vulnerabilities and their recommendation results.**

4	Medical professional	Device	Stationary	20	2017-14002	Unauthorized access	Authentication	Do medical devices ensure that default or hard-coded passwords are not used?
				21	2018-5457	Privilege escalation	Software security	Do the endpoint applications require super-user privileges only during initial access to resources? Is endpoint unprivileged software denied access to privileged resources such as configuration files, drivers, and other objects?
				22	2018-7518	Data breach	Secure data storage	Are all data stored in medical devices (configurations, sensor readings, authentication credentials, and cryptographic keys) securely encrypted?
				23	2018-7526	Unauthorized access	Access control	Do the medical devices have effective access controls (e.g., attribute-based, discretionary, mandatory, rule-based, role-based)?
				24	2018-7510	Data breach	Secure data storage	Are all data stored in medical devices (configurations, sensor readings, authentication credentials, and cryptographic keys) securely encrypted?
				25	2018-4845	Privilege escalation	Access control	Are the administrative capabilities hidden and isolated from publicly accessible applications or application programming interfaces?
				26	2018-4846	Unauthorized access	Authentication	Do medical devices ensure that default or hard-coded passwords are not used?
5	Medical professional	Device	Stationary, Gateway-dependent	27	2017-6018	Malwares	Web security	Does the web interface of medical devices have countermeasures against open redirect attacks?
6 7	Medical professional Patient	Device	Implantable, Gateway-dependent	28	2017-5149	Man-in-the-middle attacks	Secure connectivity	Does the gateway renegotiate and verify communication security keys each time it reconnects to the communication network?
8 9	Medical professional Patient	Device	Stationary, Mobile-controlled	29	2017-12701	Malwares	Software security	Do the medical devices have countermeasures against code injection attacks?
10	Administrator	Device, service, platform	Stationary	30	2018-5454	Malwares	Software security	Are all back-end debugging and test technologies disabled?
				31 32 33 34	2018-5458 2018-5462 2018-5464 2018-5466	Unauthorized access	Authentication Web security	Does the back-end sign the public facet of the signing key with the organizational root? Does the back-end web interface use valid certificates that are signed by a certificate authority? Does the back-end web interface have countermeasures against authentication bypass?
				35 36	2018-5468 2018-5472	Privilege escalation	Software security	Do back-end applications always run as a privileged user only when needed?
				37	2018-5470	Privilege escalation Malwares	Software security	Do back-end applications always run as a privileged user only when needed? Do the back-end applications have countermeasures against code injection attacks?
				38	2018-5474	Malwares	Software security	Do the back-end applications have countermeasures against code injection attacks?
11	Medical professional	Device, service	Wearable	39 40	2017-9657 2017-9658	Denial of communication	Intrusion prevention	Can the medical devices detect devices leaving or joining a communication network? Can medical devices detect a significantly abnormal network traffic fingerprint of other devices?

Similarly, Hospira LifeCare Patient-Controlled Analgesia (PCA) is another infusion system that was vulnerable to many security issues (vulnerabilities 9-14). The vulnerabilities for both devices are discussed in detail in advisories issued by the U.S. Community Emergency Response Team (CERT) [48], [49] for each device respectively. Using our tool to check the security in these solutions would reveal that these solutions have weak authentication and insecure software. This information may help future adopters in making better decisions like choosing a more secure alternative or wait until the vulnerabilities are patched. This helps users to avoid severe consequences, such as improper treatment, that are

TABLE 5. Classification of recommendations.

	Relevant	Irrelevant
Recommended	*a*	*b*
Not Recommended	*c*	*d*

associated with these unpatched solutions, as highlighted in the Common Vulnerability Scoring System (CVSS) as medium to high for the pumps [48], [49].

B. EXPERT-BASED EVALUATION

Another way to objectively evaluate the tool is by comparing it to existing similar recommendation systems. However, to the best of our knowledge, the presented tool is first of its kind in this domain that is specific to the IoMT security. Therefore, we surveyed experts in the field of cybersecurity to evaluate the tool's accuracy, recall, and precision. This approach is well-known and widely used to evaluate the effectiveness of context-based recommendation systems [50]. Accuracy represents the quality of nearness to the truth by the recommendation system, Recall represents the coverage of useful items the tool can recommend, and Precision represents the tool's capacity for showing only useful measures and minimizing the useless ones. The tool was evaluated by a group of participants consisting of seven graduate students majoring in cybersecurity. Students deemed qualified on the basis of being graduate students and having recently completed three cybersecurity graduate courses. Participants were asked to pick an IoMT solution of their choice and suggest a set of security measures necessary to protect users from risks. To validate the effectiveness of the tool, the results from the procedure followed by participants were processed to find the number of relevant/irrelevant and recommended/not-recommended security measures as described in Table. 5 where *a* represents the number of security measures recommended by the tool and participants; *b* represents the number of security measures that were recommended by the tool, but not the participants; *c* represents the number of security measures that were recommended by participants, but were not recommended by the tool; and *d* reflects the number of security measures that were not recommended by either the tool or participants. Numbers *a* and *d* count as the correct decisions. (i.e., when the tool recommends relevant measures and does not recommend irrelevant measures). As shown in Table. 6, the evaluation metrics were computed for the seven cases where the tool's and experts' recommendations were compared using the following equations:

$$Accuracy = (a+d)/(a+b+c+d) \tag{1}$$

$$Recall = a/(a+c) \tag{2}$$

$$Precision = a/(a+b) \tag{3}$$

The results from Table. 6 show that tool accuracy averaged 94.7%. This indicates that the ratio of successful tool recommendations to total recommendations is high. Columns *b* and *c* show the number of occurrences where the tool has not recommended relevant security measures or the number of occurrences where tool's recommendations were irrelevant respectively. The worst cases were 4 and 7 where three and five irrelevant security measures were recommended in column *b*. Also, we noticed that when the number of relevant recommendations (column *a*) increased, the number of recommended irrelevant measures (column *b*) also increased. This is most likely due to the complexity of the chosen scenario, which made expert recommendations more prone to human errors (i.e., overlooking some measures). Although column *b* indicates incorrect cases as reflected in the precision column, these cases do not expose the IoMT solution to risks. However, these cases indicate additional protection at the adopter's expense.

TABLE 6. Computing the tool evaluation metrics.

Case	*a*	*b*	*c*	*d*	Accuracy	Recall	Precision
1	28	0	1	14	97.7%	96.6%	100%
2	18	1	1	23	95.3%	94.7%	94.7%
3	22	1	2	18	93%	91.7%	95.7%
4	32	3	1	7	90.7%	97%	91.4%
5	14	0	0	29	100%	100%	100%
6	23	1	0	19	97.7%	100%	95.8%
7	38	5	0	0	88.4%	100%	88.4%
				Average	**94.7%**	**97.1%**	**95.1%**

Moreover, in case 3, the tool did not recommend two measures although they were relevant. This is clearly reflected in the recall value of 91.7%. The rest of the cases indicate that in both columns *b* and *c*, either zero or one incorrect recommendation. Although they are not significantly high, the incorrect recommendation in column *c* identifies missing security measures that can be added to the tool to improve protection and deterrence. This can be effortlessly done since the tool is ontology-based and allows for expandability.

1) THREATS TO VALIDITY

Students may not be the best candidates to represent experts in the field. Although each of the students deemed qualified on the basis of being a graduate student and having recently completed at least three cybersecurity graduate courses, the study results may be affected by the students' knowledge prior joining the graduate program and/or the cybersecurity courses. This falls into the category of conclusion threat. Moreover, since the students may not have performed the experiment truthfully or consistently across the entire population, the study may also be subject to instrumentation threat.

IX. LIMITATIONS AND FUTURE WORK

This tool aims to identify security issues and considerations for any IoMT scenario from three different stakeholders' perspectives. These stakeholders, as aforementioned, are patients, medical professionals, and system administrators. It can be argued that there are some other stakeholders, such as accountants, who are not considered in this work. However, we only focused on the stakeholders that directly interact with IoMT solutions. Some stakeholders, especially medical professionals and patients might find that the information provided here is difficult to understand. However, despite our efforts to simplify and shorten the recommendation lists, this work encourages stakeholders to learn more about the IoMT security issues and considerations. We proposed an all-encompassing recommendation tool that is relevant to all IoMT scenarios. However, there might be some cases where some updates are required as the IoMT solutions evolve. Therefore, since our work is designed with expandability in mind, we will continue to review and improve our work regularly to ensure that it is up-to-date.

Our future work includes further developing this tool and implementing an IoMT catalog to save and retrieve IoMT descriptions when future users request them. We also will consider implementing a platform to crowdsource entering IoMT descriptions to save future users time and effort. Further, we will continue to update the security issues and considerations to include emerging changes in IoMT technologies and security breaches and will investigate possible additional stakeholders and new scenarios.

X. CONCLUSION

In this paper we presented a security recommendation tool for IoMT solutions. The input for this tool is an IoMT scenario that specifies the type of stakeholder, solution, and architecture. Based on the scenario, the tool identifies a list of security issues and recommends security measures to address them. It also recommends a list of security attributes that can be used to determine the level of protection provided in the measures. This work assists IoMT adopters in choosing and enforcing security in IoMT solutions based on their security objectives. In some cases, system administrators are the only ones responsible for making security-related decisions, but this work educates other stakeholders about security in IoMT, thus encouraging them to be more involved in making decisions. Furthermore, this tool helps to create security awareness and promotes accountability and transparency among IoMT stakeholders. On the other hand, solution providers can utilize this tool to assess and verify the security in their products. It also helps them to compete transparently with the other providers. Another interesting utilization of this work is to enable providers to learn the security concerns of the other stakeholders by simply tracing their roles through the ontology. Moreover, the tool can help in forensic investigations where an attack can be traced back to its cause and affected components. Finally, legislators and standardization bodies can utilize it to understand the issues to better offer laws and regulations. The ultimate goal is to improve security of IoMT solutions, and we hope this work can help to push towards achieving this goal.

REFERENCES

[1] HIPAA Journal. *87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019*. Accessed: Nov. 20, 2017. [Online]. Available: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/

[2] Intel. *A Guide to the Internet of Things Infographic*. Accessed: Oct. 13, 2017. [Online]. Available: https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[3] *Internet Crime Complaint Center (IC3) | Internet of Things Poses Opportunities for Cyber Crime*. Accessed: Accessed: Oct. 17, 2017. [Online]. Available: https://www.ic3.gov/media/2015/150910.aspx

[4] P. Waurzyniak, "Securing manufacturing data in the cloud," *Manuf. Eng. Mag.*, pp. 69–77, Jul. 2016.

[5] HIPAA Journal. (2018). *Lack of Security Awareness Training Leaves Healthcare Organizations Exposed to Cyberattacks*. Accessed: Sep. 30, 2018. [Online]. Available: https://www.hipaajournal.com/lack-of-security-awareness-training-healthcare-cyberattacks/

[6] J. H. Hamlyn-Harris. *Three Reasons Why Pacemakers Are Vulnerable to Hacking*. Accessed: Dec. 7, 2017. [Online]. Available: http://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362

[7] F. Alsubaei, A. Abuhussein, and S. Shiva, "An overview of enabling technologies for the Internet of Things," in *Internet of Things A to Z*. Hoboken, NJ, USA: Wiley, 2018, pp. 77–112.

[8] Internet of Things. *IoT Security Guidelines for Endpoint Ecosystems*. Accessed: Oct. 17, 2017. [Online]. Available: https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/

[9] CD and R Health. *Classify Your Medical Device—Is The Product A Medical Device?*. Accessed: Oct. 19, 2017. [Online]. Available: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm

[10] CD and R Health. *Digital Health-Cybersecurity*. Accessed: Oct. 19, 2017. [Online]. Available: https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

[11] *Medical Devices Are the Next Security Nightmare*. Accessed: Oct. 14, 2017. [Online]. Available: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[12] C. Boulton. (Aug. 2016). IoT security suffers from a lack of awareness. CIO. Accessed: Sep. 29, 2017. [Online]. Available: https://www.cio.com/article/3104116/internet-of-things/iot-security-suffers-from-a-lack-of-awareness.html

[13] Synopsys. *Synopsys and Ponemon Study Highlights Critical Security Deficiencies in Medical Devices*. Accessed: Mar. 16, 2018. [Online]. Available: https://www.prnewswire.com/news-releases/synopsys-and-ponemon-study-highlights-critical-security-deficiencies-in-medical-devices-300463669.html

[14] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A systematic, organizational perspective," *J. Med. Internet Res.*, vol. 20, no. 5, 2018, Art. no. e10059.

[15] J. Msv. Security is fast becoming the Achilles heel of consumer Internet of Things. Forbes. Accessed: Sep. 29, 2017. [Online]. Available: https://www.forbes.com/sites/janakirammsv/2016/11/05/security-the-fast-turning-to-be-the-achilles-heel-of-consumer-internet-of-things

[16] Cloud Security Alliance. (Apr. 2015). *New Security Guidance for Early Adopters of the IoT*. Accessed: Sep. 7, 2017. [Online]. Available: https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

[17] *OWASP Internet of Things Project—OWASP*. Accessed: Mar. 10, 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Medical_Devices

[18] *[Press Release WP29] Opinion on the Internet of Things | CNIL*. Accessed: Sep. 7, 2017. [Online]. Available: https://www.cnil.fr/en/press-release-wp29-opinion-internet-things

[19] Internet of Things. (Feb. 2016). *GSMA IoT Security Guidelines–Complete Document Set*. Accessed: Sep. 7, 2017. [Online]. Available: https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/

[20] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the Internet of Things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, Sep. 2018.

[21] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[22] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, Jul. 2015.

[23] R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, "Risk-driven security metrics development for an e-health IoT application," in *Proc. Inf. Secur. South Afr. (ISSA)*, Aug. 2015, pp. 1–6.

[24] I. Laranjo, J. H. Macedo, and A. Santos, "Internet of Things for medication control: E-health architecture and service implementation," *Int. J. Rel. Qual. E-Heal.*, vol. 2, no. 3, pp. 1–15, Jul. 2013.

[25] Food and Drug Administration. (2016). *Postmarket Management of Cybersecurity in Medical Devices*. Accessed: Oct. 19, 2017. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[26] *Medical Equipment in General*. Accessed: Oct. 19, 2017. [Online]. Available: https://www.iso.org/ics/11.040.01/x/

[27] Naval Medical Logistics Command. (2016). *Medical Device Risk Assessment Questionnaire Version 3.0*. Accessed: Oct. 19, 2017. [Online]. Available: http://www.med.navy.mil/sites/nmlc/Public_Docs/Solicitations/RFP/MDRA%203.0-20160815RX.PDF

[28] *AirStrip ONE|AirStrip*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.airstrip.com/airstrip-one

[29] *BL Healthcare*. Accessed: Nov. 6, 2018. [Online]. Available: https://blhealthcare.com/

[30] L. Van Velsen, S. Wildevuur, I. Flierman, B. Van Schooten, M. Tabak, and H. Hermens, "Trust in telemedicine portals for rehabilitation care: an exploratory focus group study with patients and healthcare professionals," *Med. Inform. Decis. Making*, vol. 16, p. 11, Jan. 2016.

[31] W. Wilkowska and M. Ziefle, "Privacy and data security in E-health: Requirements from the user's perspective," *Health Inform. J.*, vol. 18, no. 3, pp. 191–201, Sep. 2012.

[32] A. A. O'Kane, H. M. Mentis, and E. Thereska, "Non-static nature of patient consent: Shifting privacy perspectives in health information sharing," in *Proc. Conf. Comput. Supported Cooperat. Work*, 2013, pp. 553–562.

[33] D. Pal, S. Funilkul, N. Charoenkitkarn, and P. Kanthamanon, "Internet-of-Things and smart homes for elderly healthcare: An end user perspective," *IEEE Access*, vol. 6, pp. 10483–10496, Feb. 2018.

[34] M. Ziefle, C. Rocker, and A. Holzinger, "Medical technology in smart homes: Exploring the user's perspective on privacy, intimacy and trust," in *Proc. IEEE 35th Annu. Comput. Softw. Appl. Conf. Workshops*, Jul. 2011, pp. 410–415.

[35] N. Magdi, "Factors affecting adoption of eHealth in Egypt," M.S. thesis, School Eng. Inf. Sci., Middlesex Univ., London, U.K., 2013.

[36] M. Maksimović, V. Vujović, and B. Perišić, "A custom Internet of Things healthcare system," in *Proc. 10th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Aveiro, Portugal, Jun. 2015, pp. 1–6.

[37] M. Ziefle, L. Klack, W. Wilkowska, and A. Holzinger, "Acceptance of telemedical treatments—A medical professional point of view," in *Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments*, vol. 8017, S. Yamamoto, Ed. Berlin, Germany: Springer, 2013, pp. 325–334.

[38] J. Larson, "Medical device security considerations: Case study," presented at the RSA Conf., San Francisco, CA, USA, Feb-2017.

[39] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[40] F. Alsubaei, A. Abuhussein, and S. Shiva, "A framework for ranking IoMT solutions based on measuring security and privacy," in *Proc. Future Technol. Conf. (FTC)*, vol. 880, K. Arai, R. Bhatia, and S. Kapoor, Eds. Cham, Switzerland: Springer, 2019, pp. 205–224.

[41] *MDRAP | Home Page*. Accessed: Oct. 19, 2017. [Online]. Available: https://mdrap.mdiss.org/

[42] *AliveCor*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.alivecor.com/

[43] Qardio. *Smart Wearable ECG EKG Monitor–QardioCore*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.getqardio.com/en/qardiocore-wearable-ecg-ekg-monitor-iphone/

[44] Kaa IoT Platfor. *IoT Healthcare Solutions-Medical Internet of Things for Healthcare Devices and Smart Hospitals*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.kaaproject.org/healthcare

[45] *NVD - Home*. Accessed: Nov. 6, 2018. [Online]. Available: https://nvd.nist.gov/

[46] *CVE Security Vulnerability Database. Security Vulnerabilities, Exploits, References and More*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.cvedetails.com/

[47] *Smiths Medical Global Homepage: Portex Medex Deltec Level1 BCI CADD Pneupac Surgivet Graseby Jelco Medfusion Wallace*. Accessed: Nov. 6, 2018. [Online]. Available: https://www.smiths-medical.com/

[48] *Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (Update A) | ICS-CERT*. Accessed: Apr. 8, 2018. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02A

[49] *Hospira LifeCare PCA Infusion System Vulnerabilities (Update B) | ICS-CERT*. Accessed: Feb. 13, 2019. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B#footnoten_st097fb

[50] F. Ricci, L. Rokach, B. Shapira, and P. B. Kantor, Eds., *Recommender Systems Handbook*. Boston, MA, USA: Springer, 2011.

FAISAL ALSUBAEI received the B.S.Eds. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2008, and the M.Sc. degree in computer science, with a concentration in security and computing, from RMIT University, Australia, in 2011. He is currently pursuing the Ph.D. degree in computer science with The University of Memphis.

He was a Software Engineer with Shaker and Associates Pty Ltd., Australia. He has been a Lecturer with the University of Jeddah, Saudi Arabia, since 2012, and is currently on sabbatical leave. His research interests include security and privacy in the Internet of Medical Things (IoMT), and cloud computing. He is a Microsoft Certified Technology Specialist, a Microsoft Certified Professional, and a Cisco Certified Entry Networking Technician. He is a member of the Australian Computer Society and Linux Users of Victoria.

ABDULLAH ABUHUSSEIN received the B.Sc. degree in computer science, in 1999, the M.Sc. degree in information systems management from Ferris State University, in 2002, and the Ph.D. degree in computer science from The University of Memphis.

In 2017, he joined the Department of Information Systems, Herberger Business School, St. Cloud State University, as an Assistant Professor. In his Ph.D. research, he focused on pragmatic cloud security assessment framework and stakeholder's perspective in cybersecurity. He is teaching courses on security, software engineering, and cloud computing as a Lecturer with various educational institutions. His research interests include cloud computing, cloud security, security economics, the Internet of Things (IoT), software engineering, social engineering, security and privacy, and security metrics. He holds a number of refereed publications in related venues, presented papers in various conferences, and served as a Reviewer for some journals, including the IEEE TRANSACTIONS ON CLOUD COMPUTING.

SAJJAN SHIVA joined The University of Memphis, in 2002, as the Director of the Computer Science Division, and transitioned it into the Department of Computer Science, in 2005. He was the Founding Chair, in 2015. He was with the Computer Science Faculty, The University of Alabama in Huntsville, and Alabama A&M University. He was the Manager of Software Quality Assurance with Teledyne Brown Engineering; a Senior Software Engineer and an Executive Manager (Technical) with Intergraph Corporation; and a Technical Advisor with the Computer Technologies Division, U.S. Army Space and Strategic Defense Command. He has consulted with industry and government organizations in the areas of software engineering, computer architecture, artificial intelligence, and expert systems. His current interests include game theoretic cybersecurity and secure software engineering.

Dr. Shiva is a Life Member of ACM. He received research funding from NSF, NASA, the U.S. Department of Defense, and ONR.