PHASE: Security Analyzer for Next-Generation Personalized Smart Healthcare System

Nur Imtiazul Haque and Mohammad Ashiqur Rahman
Analytics for Cyber Defense (ACyD) Lab, Florida International University, FL, USA
{nhaqu004, marahman}@fiu.edu

***Abstract*—With the advent of the connected healthcare systems, the contemporary healthcare system is going through a swift transformation to handle the ever-growing healthcare needs. The internet of medical things (IoMT) network and implantable medical devices (IMDs) are progressively being adopted in healthcare facilities for increasing efficiency and reducing treatment latency, thus giving rise to a smart healthcare system (SHS). Moreover, the acquisition of the personalized healthcare concept with SHS is boosting precise medication in real-time. However, the open network communication of IoMT sensor measurements collected from body sensor devices (BSDs) is vulnerable to measurement manipulation attacks since they are primarily encrypted or enciphered with lightweight cryptographic algorithms due to computational constraints. Hence, it is crucial to analyze the robustness of the SHS and real-time sensor measurements' vulnerability analysis to prevent mistreatment. This paper presents PHASE, a novel real-time security analysis framework for personalized rule-based SHS. Our framework can synthesize optimal attack vectors for measurement alteration attacks, each representing minimal required alterations to misinform the SHS controller with wrong patients' health status. The identified attack vectors can assess the vulnerability of the measurements in real-time with variable attacker's capability. We verify the effectiveness of the proposed framework using Pima Indians Diabetes, AIM-94, and Harvard Dataverse datasets.**

***Index Terms*—Healthcare security, internet of medical things, personalized smart healthcare system.**

I. Introduction

Healthcare is one of the prime human rights which controls the livelihood and quality of human lives. The healthcare market accounts for almost 20% expenditure for most countries of the world [1]. Recent statistics forecast the global healthcare market to reach $6.2 trillion by 2028. Such a massive cost for hospitalization, nursing, and treatment, along with huge latency in healthcare delivery, which often costs human lives, are mostly associated conventional healthcare system. The rise of the digital healthcare system (DHS) has cut a significant amount of cost, nursing, and treatment delay [2]. However, the ongoing pandemic period has drawn light to the fact that contemporary telehealth and mHealth services of DHS require more automation to deal with a transient increase in treatment demand [3]. During the pandemic, a substantial number of patients were delayed or denied healthcare services due to a significant disparity between hospital accommodations and demands [4]. The avoidance or delay in getting medical support contributed notably to the rise in COVID-19-related deaths. [5]. In this pandemic, nearly 48% of Americans affected with COVID-19 were either delayed or denied medical treatment. [6]. Treatment latency caused 11% of them to have worsening health conditions.

Global acceptance of automated smart healthcare systems (SHS) would have reduced such unexpected events by adopting and enabling automated remote patient monitoring and treatment [7]. The SHS concept redefines the modern healthcare system by merging an internet of medical things (IoMT)-enabled network and an automated control decision system to make it more personalized, automated, and effective [8]. In a typical SHS, patients are treated automatically via implantable medical devices (IMDs) or similar automated medical delivery systems [9]. A control signal, which is often generated by a cloud-based controller through patient's vital measurement processing, is used to trigger medical actuators (such as IMDs). The controllers employ knowledge derived from domain experts' years of expertise to identify the patient's status based on vital sign measurements obtained from the patient's body sensor devices (BSDs). Through the IoMT network, BSD measurements are relayed to the controller. Figure 1 shows such a system, where patients are being monitored and treated with an automated medicare delivery system accounting for minimal involvement of care providers.

Although the IoMT-enabled SHS can be a game-changer for an ameliorated healthcare system, the open IoMT network communication is growingly increasing the possible cyberattacks in a safety-critical SHS [10]. A recent study highlighted the viability of attacking healthcare sensor equipment, stating that more than two-thirds of IoMT devices are vulnerable to several hacks [11]. Moreover, the SHS is susceptible to many attacks, as found in recent literature including man-in-the-middle (MITM) attacks [12], malware (e.g., Medjack [13]), hardware Trojan [14], denial of service attack [15], Sybil attacks (using either hijacked IoMT [16] and so on. Between October 2018 and October 2019, adversarial attacks hit more than 50% of healthcare institutions [17]. According to a source, the University of Vermont Medical Center was cut off from the internet owing to a cyberattack, which caused a $64 million loss [18]. Statistics have identified the susceptibility of IoMT-enabled SHS, with 6.2 (out of 10) cybersecurity vulnerabilities in 15-20 connected/IoMT devices [19]. In light of these events, a measurement manipulation attack is not too far to take action. Hence, building robust SHS with preventive and reactive measures is mandatory.

The SHS is mostly augmented with personalized healthcare for improving patient treatment through obtaining knowledge

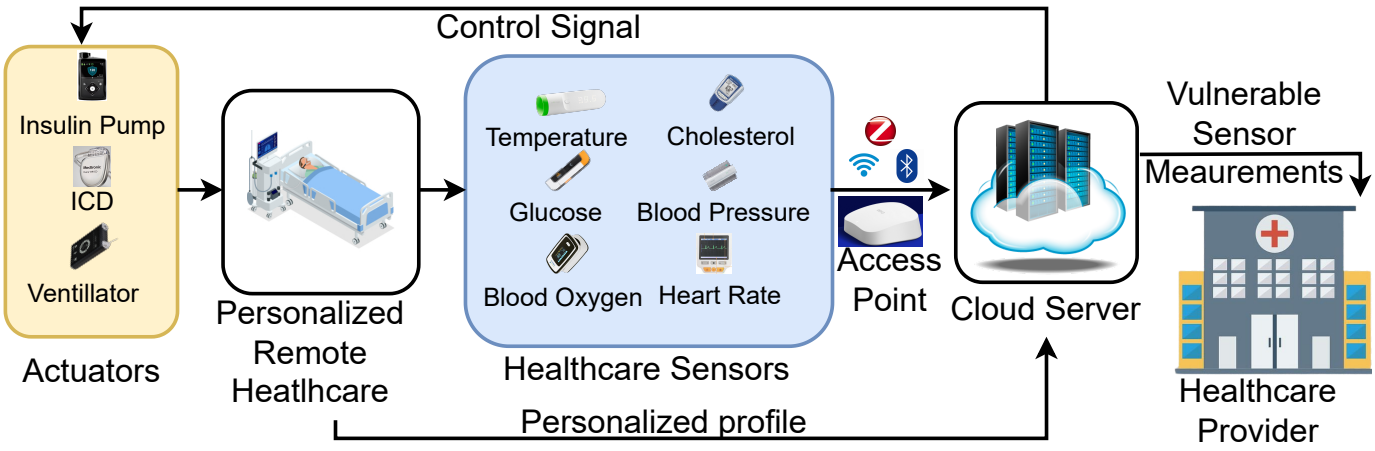

Fig. 1. An IoMT-enabled Personalized SHS.

about the individuals [20]. Personalized healthcare, also known as personalized medicine or precision medicine, is a rapidly developing area where doctors employ diagnostic tests to determine which medical treatments are appropriate for each patient. Despite treatment benefits, incorporating personalized healthcare can enhance the security of the SHS. In this work, we aim to demonstrate how adopting personalized healthcare along with an SHS can build a robust healthcare system. We propose **P**ersonalized **H**ealth **A**nalyzer for **S**ecutity **E**nhancement (PHASE) framework that can perform real-time security analysis of a personalized SHS. Our considered SHS incorporates a rule-based knowledge base (KB), where the rules related to the patient status identification, medication decisions, and healthcare policies are acquired through years of experience with the healthcare providers and healthcare data analysts. We consider a sophisticated attacker with access to a massive amount of healthcare data that can partially or fully learn the data distribution of the healthcare rules. The proposed framework uses a satisfiability modulo theorem (SMT)-based optimizer to produce optimal attack vectors (i.e., required measurements to be injected into actual measurements for altering the patient's label) with the intent to evade the controller verification. However, using the knowledge acquired from personalized patient data analysis, our proposed framework can reveal several attacks. A knowledgeable attacker having complete knowledge of the SHS architecture and measurement verification process can still launch stealthy attacks by misinforming the SHS controller. Thus, the patient will be mistreated. We consider the critical measurements that can result from measurement manipulation attacks as vulnerable sensor measurements. The PHASE framework can identify vulnerable sensor measurements in real-time and notify the healthcare provider. Accordingly, our framework employs robustness and reliability while reducing treatment latency, cost, and the need for direct involvement of healthcare providers. We will use the term SHS to refer to a personalized SHS throughout the paper for brevity.

Cyber threat detection and threat analysis have received a growing interest in the recent researches [21]–[26]. However, unlike traditional efforts, the PHASE framework does not require learning attack patterns through a learning algorithm. There is no anomaly dataset that can detect all possible anomalies due to the constant emergence of various novel attacks. We use three different datasets - PIMA Indians diabetes dataset, AIM-94 dataset [27], and Harvard Dataverse [28] blood pressure datasets for the experimentation and framework evaluation. The framework overview and comprehensive discussion are provided in Sections III and IV respectively. Section V presents the experimental and data processing overview. The concluding remarks are provided in Section VI.

II. Related Work

The security analysis of the healthcare system, particularly next-generation SHS, has grown significant interest recently. The security of the IoMT sensor measurements cannot be hardened with a strong cryptographic algorithm due to their computation and power constraints. However, one group of research focuses on strengthening the security of SHS through lightweight encryption tehniques [29]–[31]. Nevertheless, the proposed solutions are susceptible to several threats. Hence, there is a dire requirement to analyze the security and propose defense of the SHS prior to and post-deployment.

The security analysis of SHS or similar domains has been mostly researched through formal analysis tools [32], [33]. One of the mentionable works for SHS threat analysis is proposed by Haque et al. [34]. They have developed an efficient algorithm for analyzing the machine-learning-based SHS against measurement manipulation attacks. However, the proposed comprehensive framework is responsible for pre-deployment attack vector and attack impact identification, whereas the PHASE framework can identify vulnerable measurements in real time. Another pre-deployment vulnerability assessment tool of a similar domain for a rule-based system is analyzed in BIoTA framework [35]. Several works consider threat analysis using or on an machine learning (ML)-based model [36], [37]. Nevertheless, the ML-based SHS control model is out of scope for this work. Moreover, several

regulations-based security analysis techniques [38]–[40] and graph-based security analysis has also been explored with recent researches [41]–[44]. However, none of these works are capable of identifying vulnerable measurements at real-time for measurement manipulation attacks.

Our proposed PHASE framework can make the SHS robustness against stealthy measurement manipulation attacks. Hence it can be considered a defense tool as well. Different types of anomaly detection systems or intrusion detection systems have been developed in the prior works for SHS or similar domains [45]–[47]. The proposed anomaly detection systems have experimented with efficient ensembling of state-of-the-art ML algorithms and proposed novel solutions using bio-inspired optimization approaches to defend (i.e., detection based defense) against zero-day attacks. However, knowledgeable attackers can still exploit the proposed anomaly detection systems with novel zero-day attacks. We will explore the vulnerability of those research in our future works.

III. Framework

This section provides an overview of the proposed framework. The working principle of the PHASE framework is shown in Fig. 2. The framework has three main components -

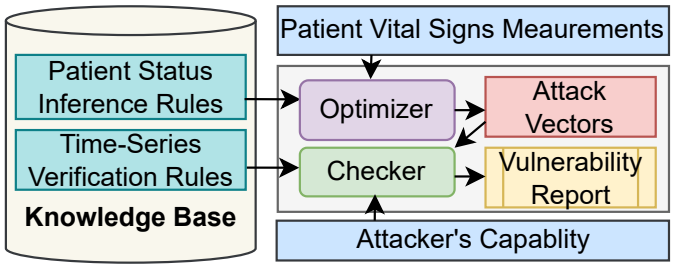

Fig. 2. The workflow of PHASE framework.

KB, optimizer, and checker. The KB is the core component of the PHASE framework. Two types of rules are stored in the KB - patient status inference rules and time-series verification rules. The patient status inference rules are obtained from the healthcare domain experts and scientific research reports to map the patients' vital signs with particular health status. On the other hand, the time-series verification rules contain temporal relationships of the vital signs measurements. The latter helps identify abnormal sensor measurements due to fault or malicious intent. The optimizer takes patient status rules from the KB and patient's vital sign measurements as input and produces an attack vector. The attack vector is represented by a minimal set of measurements to be added with the actual vital sign measurements for altering the patient's status. The generated optimal attack vectors are passed to the checker for assessing the vulnerability of current patient vital sign measurements. The checker also takes the attacker's capability, patient vital status inference rules, time-series verification current vital sign measurements into account to report whether the current set of measurements are vulnerable or not. The healthcare and cloud service providers will be notified immediately when the PHASE framework reports the patient's sensor measurement to be vulnerable. We consider the measurements those as vulnerable measurements from which attack vectors can be obtained. The vulnerable measurements need special treatment to avoid hazards. **Threat Model** In our security analysis framework, we are considering measurement manipulation attacks. Because the sensors in an SHS IoMT network mostly possess less computational power, they can't use robust encryption to protect data integrity. As a result, attackers get a scope to modify measurement data. The attacker is presumed to have access to one or more sensor measures and the ability to manipulate them. The attacker can change sensor measurements to cause the KB to make a bad inference decision, causing the controller to send an incorrect control signal, resulting in the wrong drug being delivered. The measurement changes are thought to have been carried out by a sophisticated attacker acquainted with KB inference rules. Our considered measurement manipulations are restricted to the sensor level. The attack model implies that the SHS's controllers and actuators are secured/protected from direct compromise. Our attack model discovers only attack vectors that are reachable with the attacker's capability.

TABLE I
Modeling Notations

Symbol	Description	Type
$\mathcal{M}$	Set of patient vital sign measurements.	Set
$\mathcal{M}_a$	a-th patient vital sign measurement.	Real
$\mathcal{L}$	Set of patient statuses.	Set
$\mathcal{K}^{inf}$	Set of patient status inference rules of the KB.	Set
$\mathcal{K}_i^{inf}$	i-th KB inference rules represented by a tuple that maps inference rules, $\mathcal{K}_i^{inf,r}$ with corresponding label, $\mathcal{K}_i^{inf,l}$	Tuple
$\mathcal{K}^{ver}$	Set of time-series verification rules of the KB.	Set
$\mathcal{K}_j^{ver}$	j-th KB verification rules represented by a tuple that maps patient vital sign measurements, $\mathcal{K}^{ver,m}$ with minimum and maximum measurement prediction $\mathcal{K}_j^{ver,min}$ and $\mathcal{K}_j^{ver,max}$ respectively.	Tuple
Δ	Attack vector.	Vector
$\Delta_{t,a}$	a-th measurement of attack vector at t-th time instance.	Real
$\mathcal{A}$	Attacker's accessibility vectors.	Vector
$\mathcal{A}_a$	Attacker's accessibility to a-th measurement.	Bool

IV. Technical Details

The framework introduced in section III will be thoroughly discussed in this section. As discussed earlier, the framework mainly consists of three different components, which are formally described as follows. The discussion will use the modeling notations tabulated in Table I and the procedures shown in Algorithm 1.

A. Knowledge Base (KB)

The KB is the key element for inferring the treatment demand through patient status identification. Moreover, the KB module holds verification rules that help detect abnormal vital

sign measurements. The SHS knowledge is stored in the KB in the form of rules. There are two different types of rules in the KB.

Patient Status Inference Rules The patient status inference rules portray the relationships between the vital sign measurements and corresponding patient status. Line 2 of Algorithm 1 shows the acquisition of labels for a patient's current vital sign measurements using the $Inference$ function. The Sat function is used in this process, which checks whether the current vital sign measurements are consistent with the measurements of the i-th inference rule from the KB, $\mathcal{K}_i^{inf,m}$ or not. The $Inference$ function outputs the label in the KB, $\mathcal{K}_i^{inf,l}$ for which the current vital sign measurements and knowledge base measurements comply.

Time-series Verification Rules Drastic alteration in consecutive time-slot measurement is unnatural and/or abnormal. Hence, the KB also stores a possible alteration range of measurements in succeeding time-slot. The range varies based on the patient's biological and disease profile. Hence the time-series verification rules that map the possible minimum ($\mathcal{K}_j^{ver,min}$) and maximum ($\mathcal{K}_j^{ver,max}$) following time-slot measurements with current vital sign measurements are collected through careful time-series data (i.e., measurements) analysis from the patient in consideration.

B. Optimizer

The optimizer leverages patient status inference rules from the KB to generate optimal attack vectors that can be attained with minimal vital measurement alteration. Line 6-7 shows the attack vector generation process through the optimizer. The $AttackVectorGeneration$ function takes vital sign measurements ($\mathcal{M}_t$), KB inference rules ($\mathcal{K}^{inf}$), and targeted patient status ($\hat{l}$) as input. From the algorithm, it can be seen that the patient's vital measurements are labeled as l using the KB inference rules. The optimizer produces the optimal attack vector by solving a minimization problem, i.e., the adversarial sample generated with the attack vector gets labeled as the targeted label ($\hat{l}$). Note that the absolute value of attack vectors is taken in the case of the optimization objective, which assures the acquisition of attack vectors through addition and/or subtraction from actual measurements that maintain minimum distance.

C. Checker

After KB rules and attack vector generation, the vulnerability of the measurements is checked with the checker. The checker uses both time-series verification and confidence rules in the checking process. The primary task of the checker is to generate a vulnerability report for vital sign measurements. The patient vital sign measurements and the KB time-series verification rules are taken as input for vulnerability assessment of the current sensor measurements. At first, the measurements from both the current and the previous time-slots are passed through the $Inference$ function to obtain the labels for current patient status ($label$) (Line 11). Then the adversarial sample is generated for all target patient status other than current status by adding the current vital sign measurements with the attack vectors (Line 13-14). The attack vectors are generated with the optimizer bypassing the vital sign measurements, KB inference rules, and target patient status. If the adversarial sample is within the minimum-maximum range for the KB verification rules associated with current vital measurements and the attacker has accessibility to alter required measurements, then the sample is labeled as a vulnerable sample (Line 15-16) for that specific target patient status. Otherwise, the sample is labeled as "not vulnerable" for that target patient status (Line 18) and added to the vulnerability report accordingly. Finally, the PHASE-generated vulnerability report is assessed for decision-making. If there exists any vulnerability, the measurements are further inspected by the healthcare providers and data analysts; otherwise, control signals are generated using the measurements to actuate the IMDs.

Algorithm 1: SHS Real-time Security Analysis with PHASE.

1 **Function** `Inference`($\mathcal{M}$, $\mathcal{K}^{inf}$)**:**
2 $label \leftarrow \mathcal{K}_i^{inf,l}$:$Sat(\mathcal{K}_i^{inf,m}, \mathcal{M}_t)$
3 **return** $label$**;**
4
5 **Function** `AttackVectorGeneration`($\mathcal{M}_t$, $\mathcal{K}^{inf}$, $\hat{l}$)**:**
6 $l \leftarrow Inference(\mathcal{M}_{t,a}, \mathcal{K}^{inf})$;
7 $\Delta_t \leftarrow \min \Delta_t : \forall_{a \in \mathcal{M}} Inference(\mathcal{M}_a + |\Delta_{t,a}|) \leftarrow \hat{l}$
8 **return** $attackVector$**;**
9
10 **Function** `VulnerabilityReportGeneration`($\mathcal{M}$, $\mathcal{M}$ $\mathcal{K}^{inf}$, $\mathcal{K}^{ver}$, $confThreshold$)**:**
11 $label \leftarrow Inference(\mathcal{M}_a, \mathrm{K}^{inf})$;
12 **for** *each* $\hat{l}$ *in* $\mathcal{L}$ *such that* $\hat{l}$*!=label* **do**
13 $\Delta \leftarrow$ AttackVectorGeneration($\mathcal{M}$, $\mathcal{K}^{inf}$, $label$)
14 $adversarialSample \leftarrow \mathcal{M} + \Delta$;
15 **if** $\mathcal{K}_j^{ver,min} \leq$*adversarialSample*$\leq \mathcal{K}_j^{ver,min}$ *:* $Sat(\mathcal{K}_j^{ver,m}, \mathcal{M})$ *and* $\forall_{a \in A} Sat(adversarialSample, \mathcal{K}_j^{ver}))$ **then**
16 $report.add($ $\leftarrow$"Vulnerable for target label, $\hat{l}$");
17 **else**
18 $report.add$("Not Vulnerable for target label, $\hat{l}$");
19 **end**
20 **end**
21 **return** $report$**;**

V. Experiments and Results

This section provides the experimentation to show the analysis of the performance of PHASE using state-of-the-art healthcare datasets for diabetes prediction. We consider an SHS that generates the necessary insulin delivery control signal to actuate an automated insulin pump. Suppose the patient sensor measurements are vulnerable to measurement manipulation attacks. In that case, the proposed framework will also detect that and notify the healthcare provider to take immediate steps. The data collection, experimental setup, and experimental results are discussed followingly.

TABLE II
ATTACK VECTOR ANALYSIS FOR VARIOUS CASES

Case No	Measurement Type	Blood Pressure	Glucose	Insulin
1	Benign	66	114	79
	Attacked	66	155	79
	Verification (Min)	62	109	None
	Verification (Max)	82	123	
2	Benign	70	93	0
	Attacked	70	166.56	31
	Verification (Min)	62	35	None
	Verification (Max)	86	384	
3	Benign	73	187	200
	Attacked	73	110.56	200
	Verification (Min)	73	70	None
	Verification (Max)	73	310	
4	Benign	78	154	8
	Attacked	78	123.5	8
	Verification (Min)	73	102	None
	Verification (Max)	84	182	

A. Data Collection

To evaluate the PHASE framework's performance, we consider measurements from a state-of-the-art dataset- the Pima Indians diabetes dataset. Although the dataset is not a time-series patient diabetic status dataset, we leverage the dataset for rule acquisition and KB modeling. The Pima Indians dataset contains several features that are used for medical prediction (i.e., patients' age, insulin level, BMI, blood pressure, glucose, number of pregnancies, diabetes pedigree function) and a target variable (i.e., diabetes status). Among the features, blood pressure, glucose, and insulin levels are the vital sign measurements that are considered for attack vector generation. We gather the personalized healthcare information from two time-series datasets - the Harvard Dataverse dataset (blood pressure) and the AIM-94 dataset (insulin and glucose). These datasets are used for vulnerability analysis of the measurements collected from the Pima Indians diabetes datasets.

B. Environmental Setup and Experimental Tools

We conducted the experimentation on Dell Precision 7920 Tower workstation with Intel Xeon Silver 4110 CPU @3.0GHz, 32 GB memory, 4 GB NVIDIA Quadro P1000 GPU. The attack vectors are identified using a Z3 SMT optimizer [48]. The rules are collected using a decision tree inference model [49] that learned the inference rule from the PIMA Indians diabetes dataset. The verification rules are interpolated using a linear regression model [50].

C. Attack Vector Analysis

Here, we discuss the attack vector analysis from the datasets in consideration. Table II shows PHASE generated attack vectors for 4 different cases. The demonstrated measurements are only vital signs measurements. We ignore the other dataset features (e.g., patient's age, number of pregnancies) out of attack scope. In the 1st case (patient status: Normal) and the 4th case (patient status: diabetic), PHASE-generated attack vectors did not pass the verification test. Hence, these attack vectors are not considered as vulnerable. However, for the 2nd case, the PHASE optimizer-generated attack vector bypassed the verification module and is capable of altering the normal patient status to a diabetic one. In the 3rd case, the attack vectors also evaded the verification rules and altered the diabetic patient's status to normal. Hence, the attack vectors from the 2nd and 3rd cases are considered to be vulnerable. The healthcare providers will be notified to perform further analysis of these scenarios to avoid wrong medication or treatment.

TABLE III
VULNERABILITY MEASUREMENT WITH DIFFERENT ATTACKER'S CAPABILITY (ACCESSIBILITY)

Attacker's Accessibility to Sensor Measurements	Measurements	Vulnerable Samples
3 Measurements	BP, Glucose, Insulin	190
2 Measurements	BP, Glucose	162
	BP, Insulin	118
	Glucose, Insulin	74
1 Measurement	BP	57
	Glucose	68
	Insulin	29

D. Determining the number of vulnerable samples

The primary task of the PHASE framework is to identify vulnerable sensor measurements. Based on our analysis, we figure that 24.74% (190 out of 768) of the measurements in the Pima Indians dataset are vulnerable measurements. However, it does not signify that almost 1/4th of measurements of the day require dealing with healthcare providers. For a reason, patient status (i.e., diabetes symptoms or not) seldom varies frequently for a regular diabetic patient. Even for the critical patient with the considered patient profile, sensor measurements are highly probable (i.e., 0.75) to be not vulnerable. Moreover, the analysis of vulnerable sensor measurements can be a good tool for the healthcare providers to schedule patient importance based on counting the vulnerable sensor measurements with an existing health history. Table III shows the vulnerable samples count with different measurement accessibility.

E. Measurements Importance Analysis

The proposed framework also provides a guide to identifying the most crucial measurements to protect against measurement manipulation attacks. Fig. 3 shows various measurements' importance through their participation in the attack vectors. For instance, the glucose measurement contributes the most to the identified attack vectors. In both samples, considered attack vectors and attack vectors associated with vulnerable samples, the participation is above 50% for the glucose measurement. Hence, glucose is considered the most

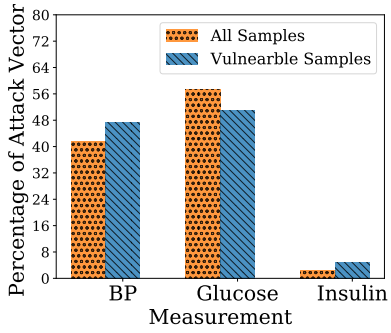

Fig. 3. Different measurement participation in PHASE generate attack vectors.

crucial measurement, protection of which will create a robust blood pressure monitoring and treatment of SHS. The insulin measurement is the least contributing towards the patient status prediction as reported by the PHASE-generated attack vector analysis. The vulnerable samples are generated considering attackers have accessibility to all measurements.

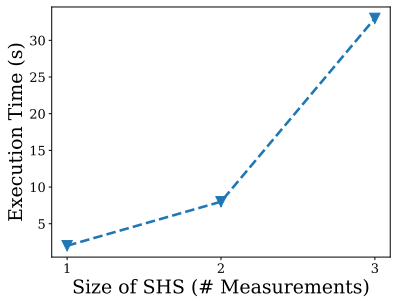

Fig. 4. Scalability analysis of the proposed framework.

F. Scalability Analysis

We assess the scalability of the PHASE framework through execution time analysis varying the considered SHS size. Although we had three vital sign measurements (i.e., blood pressure, glucose, and insulin level), we consider three different sizes of SHS; where in the first one, we portray rules only from glucose measurements, and in the second case, we depict rules from an SHS consisting of glucose and blood pressure measurements. In contrast, for the final case, we contemplate rules from all three measurements. Fig. 4 shows the execution time needed for the PHASE optimizer. The required execution times for 1, 2, and 3 measurements SHS were 2.21 s, 8.13 s, and 33.17 s, respectively. The vulnerability checking time is negligible ($<$1 s) for all considered cases. Although the figure shows a sharp increment in execution time, when SHS size increases to 3 measurements from 2 measurements, the proposed framework should be able to identify vulnerable run-time measurements for a large SHS (i.e., containing 10 measurements). Hence, the framework seems to be scalable in the smart healthcare concept. The framework appears to be scalable since the sampling time of the AIM-9 time-series dataset is 1 hour or more. However, the sampling time for control signal generation is significantly low (i.e., a few seconds) for some sensor measurements. In that case, the PHASE framework will be unable to label vulnerable vital sign measurements in real-time.

VI. Conclusion

We propose the PHASE framework for real-time security analysis of personalized SHS. The framework can generate sophisticated attack vectors with minimal alteration of measurements in real-time to alter the patients' status. Moreover, the deployed checker that uses verification rules to detect abnormalities can reveal the attack vectors. We evaluate the proposed framework with several metrics. Our experimental analysis shows that more than 75% of the PIMA INDIANS diabetes dataset data is robust against measurement manipulation attacks when PHASE-generated verification rules are applied. In this work, we acquire the KB rules through data analysis from different state-of-the-art datasets. We plan to collaborate with domain experts to model the KB rules in future work. The verification rules are represented with minimum and maximum values. The future extension will consider predicted measurement confidence for reducing the vulnerable samples and thus contribute to enhancing the robustness of the SHS. Moreover, the verification rules used in the work will be modified in the upcoming work for further reduction in vulnerable samples.

References

[1] Michelle P. Scott. Why u.s. healthcare spending is rising so fast. https://www.investopedia.com/u-s-healthcare-spending-rising-fast-5186172, 2022. Accessed: 2022-05-10.

[2] Bhagyashree Mohanta, Priti Das, and Srikanta Patnaik. Healthcare 5.0: A paradigm shift in digital healthcare system using artificial intelligence, iot and 5g communication. In *2019 International Conference on Applied Machine Learning (ICAML)*, pages 191–196. IEEE, 2019.

[3] Ronald S Weinstein, Elizabeth A Krupinski, and Charles R Doarn. Clinical examination component of telemedicine, telehealth, mhealth, and connected health medical practices. *Medical Clinics*, 102(3):533–544, 2018.

[4] Mark É Czeisler, Kristy Marynak, Kristie EN Clarke, Zainab Salah, Iju Shakya, JoAnn M Thierry, Nida Ali, Hannah McMillan, Joshua F Wiley, Matthew D Weaver, et al. Delay or avoidance of medical care because of covid-19–related concernsâunited states, june 2020. *Morbidity and mortality weekly report*, 69(36):1250, 2020.

[5] Delay or avoidance of medical care because of covid-19ârelated concerns â united states, june 2020. https://www.cdc.gov/mmwr/volumes/69/wr/mm6936a4.htm, 2020. Accessed: 2021-04-21.

[6] Elizabeth Lawrence. Nearly half of americans delayed medical care due to pandemic. https://khn.org/news/nearly-half-of-americans-delayed-medical-care-due-to-pandemic/, 2020. Accessed: 2021-04-21.

[7] Haluk Demirkan. A smart healthcare systems framework. *It Professional*, 15(5):38–45, 2013.

[8] Gulraiz J Joyia, Rao M Liaqat, Aftab Farooq, and Saad Rehman. Internet of medical things (iomt): Applications, benefits and future challenges in healthcare domain. *J. Commun.*, 12(4):240–247, 2017.

[9] Yeun-Ho Joung. Development of implantable medical devices: from an engineering perspective. *International neurourology journal*, 17(3):98, 2013.

[10] Understanding the iot digital attack surface and threat mitigation. https://www.tokenex.com/blog/understanding-the-iot-digital-attack-surface-and-threat-mitigation, 2018. Accessed: 2022-02-22.

[11] Hp study reveals 70 percent of internet of things devices vulnerable to attack. https://www.hp.com/us-en/hp-news/press-release.html?id=1744676.YhUL0pZOm5c, 2014. Accessed: 2022-02-22.

[12] Vahab Pournaghshband, Majid Sarrafzadeh, and Peter Reiher. Securing legacy mobile medical devices. In *International Conference on Wireless Mobile Communication and Healthcare*, pages 163–172. Springer, 2012.

[13] Darlene Storm. Medjack: Hackers hijacking medical devices to create backdoors in hospital networks. https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html, 2015. Accessed: 2020-01-08.

[14] T. Wehbe, V. Mooney, A. Javaid, and O. Inan. A novel physiological features-assisted architecture for rapidly distinguishing health problems from hardware trojan attacks and errors in medical devices. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 106–109, 2017.

[15] Rashmi V Deshmukh and Kailas K Devadkar. Understanding ddos attack & its effect in cloud environment. *Procedia Computer Science*, 49:202–210, 2015.

[16] Ahmad Almogren, Irfan Mohiuddin, Ikram Ud Din, Hisham Al Majed, and Nadra Guizani. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet of Things Journal*, 2020.

[17] Ponemon Institute. *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*, October 2019. https://www.keeper.io/hubfs/PDF/2019

[18] Laira Dyrda. Inside uvm medical center's ransomware attack: 11 details. https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html, 2020. Accessed: 2021-07-05.

[19] 5 common cybersecurity vulnerabilities in the iomt. https://securityscorecard.com/blog/common-cybersecurity-vulnerabilities-in-the-iomt, 2021. Accessed: 2022-02-22.

[20] Ganjar Alfian, Muhammad Syafrudin, Muhammad Fazal Ijaz, M Alex Syaekhoni, Norma Latif Fitriyani, and Jongtae Rhee. A personalized healthcare monitoring system for diabetic patients by utilizing ble-based sensors and real-time data processing. *Sensors*, 18(7):2183, 2018.

[21] Ibrahim Alrashdi, Ali Alqazzaz, Raed Alharthi, Esam Aloufi, Mohamed A Zohdy, and Hua Ming. Fbad: Fog-based attack detection for iot healthcare in smart cities. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0515–0522. IEEE, 2019.

[22] Leandros A Maglaras, Jianmin Jiang, and Tiago Cruz. Integrated ocsvm mechanism for intrusion detection in scada systems. *Electronics Letters*, 50(25):1935–1936, 2014.

[23] AKM Iqtidar Newaz, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A Selcuk Uluagac. Healthguard: A machine learning-based security framework for smart healthcare systems. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pages 389–396. IEEE, 2019.

[24] Samuel G Finlayson, John D Bowers, Joichi Ito, Jonathan L Zittrain, Andrew L Beam, and Isaac S Kohane. Adversarial attacks on medical machine learning. *Science*, 363(6433):1287–1289, 2019.

[25] Mehran Mozaffari-Kermani, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. Systematic poisoning attacks on and defenses for machine learning in healthcare. *IEEE journal of biomedical and health informatics*, 19(6):1893–1905, 2014.

[26] Samuel G Finlayson, Hyung Won Chung, Isaac S Kohane, and Andrew L Beam. Adversarial attacks against medical deep learning systems. *arXiv preprint arXiv:1804.05296*, 2018.

[27] Jeroen Eggermont, Joost N Kok, and Walter A Kosters. Genetic programming for data classification: Partitioning the search space. In *Proceedings of the 2004 ACM symposium on Applied computing*, pages 1001–1005, 2004.

[28] John Schwenck. Blood Pressure Data, 2020.

[29] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang. A medical healthcare system for privacy protection based on iot. In *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, pages 217–222, 2015.

[30] Nidhi Sharma and Ravindara Bhatt. Privacy preservation in wsn for healthcare application. *Procedia computer science*, 132:1243–1252, 2018.

[31] Ashwini Kore and Shailaja Patil. Cross layered cryptography based secure routing for iot-enabled smart healthcare system. *Wireless Networks*, pages 1–15, 2022.

[32] Mujahid Mohsin, Zahid Anwar, Ghaith Husari, Ehab Al-Shaer, and Mohammad Ashiqur Rahman. Iotsat: A formal framework for security analysis of the internet of things (iot). In *2016 IEEE conference on communications and network security (CNS)*, pages 180–188. IEEE, 2016.

[33] Mujahid Mohsin, Zahid Anwar, Farhat Zaman, and Ehab Al-Shaer. Iotchecker: A data-driven framework for security analytics of internet of things configurations. *Computers & Security*, 70:199–223, 2017.

[34] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, Md Hasan Shahriar, Alvi Ataur Khalil, and Selcuk Uluagac. A novel framework for threat analysis of machine learning-based smart healthcare systems. *arXiv preprint arXiv:2103.03472*, 2021.

[35] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, Dong Chen, and Hisham Kholidy. Biota: Control-aware attack analytics for building internet of things. In *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE, 2021.

[36] Zhengping Luo, Shangqing Zhao, Zhuo Lu, Yalin E Sagduyu, and Jie Xu. Adversarial machine learning based partial-model attack in iot. In *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*, pages 13–18, 2020.

[37] Chenglin Yang, Adam Kortylewski, Cihang Xie, Yinzhi Cao, and Alan Yuille. Patchattack: A black-box texture-based attack with reinforcement learning. In *European Conference on Computer Vision*, pages 681–698. Springer, 2020.

[38] Ioannis Stellios, Panayiotis Kotzanikolaou, and Christos Grigoriadis. Assessing iot enabled cyber-physical attack paths against critical systems. *Computers & Security*, 107:102316, 2021.

[39] Zeinab Bakhshi, Ali Balador, and Jawad Mustafa. Industrial iot security threats and concerns by considering cisco and microsoft iot reference models. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 173–178. IEEE, 2018.

[40] Nikolay Akatyev and Joshua I James. Evidence identification in iot networks based on threat assessment. *Future Generation Computer Systems*, 93:814–821, 2019.

[41] Gemini George and Sabu M Thampi. A graph-based decision support model for vulnerability analysis in iot networks. In *International Symposium on Security in Computing and Communication*, pages 1–23. Springer, 2018.

[42] Shuqin Zhang, Minzhi Zhang, Hong Li, and Guangyao Bai. Threat analysis of iot security knowledge graph based on confidence. In *International Symposium on Emerging Technologies for Education*, pages 254–264. Springer, 2021.

[43] Lina Zhu, Zuochang Zhang, Guoen Xia, and Caoqing Jiang. Research on vulnerability ontology model. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, pages 657–661. IEEE, 2019.

[44] Ralph Ankele, Stefan Marksteiner, Kai Nahrgang, and Heribert Vallant. Requirements and recommendations for iot/iiot models to automate security assurance through threat modelling, security analysis and penetration testing. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–8, 2019.

[45] Nur Imtiazul Haque, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, M Hadi Amini, and Sheikh Iqbal Ahamed. Biocad: Bio-inspired optimization for classification and anomaly detection in digital healthcare systems. In *2021 IEEE International Conference on Digital Health (ICDH)*, pages 48–58. IEEE, 2021.

[46] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, and Hossain Shahriar. Ensemble-based efficient anomaly detection for smart building control systems. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 504–513. IEEE, 2021.

[47] Ashish Singh, Kakali Chatterjee, and Suresh Chandra Satapathy. Trids: an intelligent behavioural trust based ids for smart healthcare system. *Cluster Computing*, pages 1–23, 2022.

[48] Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient smt solver. In *International conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340. Springer, 2008.

[49] Anthony J Myles, Robert N Feudale, Yang Liu, Nathaniel A Woody, and Steven D Brown. An introduction to decision tree modeling. *Journal of Chemometrics: A Journal of the Chemometrics Society*, 18(6):275–285, 2004.

[50] Sanford Weisberg. *Applied linear regression*, volume 528. John Wiley & Sons, 2005.