A Secure IoT-based Modern Healthcare System with Fault-tolerant Decision Making Process

Prosanta Gope, *Member IEEE*, Youcef Gheraibia, Sohag Kabir, and Biplab Sikdar, *Senior Member IEEE*

***Abstract*—The advent of Internet of Things (IoT) has escalated the information sharing among various smart devices by many folds, irrespective of their geographical locations. Recently, applications like e-healthcare monitoring has attracted wide attention from the research community, where both the security and the effectiveness of the system are greatly imperative. However, to the best of our knowledge none of the existing literature can accomplish both these objectives (e.g., existing systems are not secure against physical attacks). This paper addresses the shortcomings in existing IoT-based healthcare system. We propose an enhanced system by introducing a Physical Unclonable Function (PUF)-based authentication scheme and a data driven fault-tolerant decision-making scheme for designing an IoT-based modern healthcare system. Analyses show that our proposed scheme is more secure and efficient than existing systems. Hence, it will be useful in designing an advanced IoT-based healthcare system.**

***Index Terms*—IoT, Healthcare, machine learning, fault tolerance, sensor fusion**

I. Introduction

With the development of diverse types of consumer electronics products and devices, people's lives have changed dramatically. The devices are connected by advanced communication technologies to the Internet and form the Internet of Things (IoT) to exchange information. Nowadays, IoT devices are widely deployed for various applications such as smart home, smart city, body sensor networks (BSN), smart grid, and vehicular ad-hoc networks. The term IoT is commonly used to refer to systems consisting of uniquely identifiable objects, that are autonomous in nature and able to connect to the Internet to present and exchange real-world information in a digital form. Its vision is that in the future, everything (i.e., including live objects) would be accessible, sensed, and interconnected inside the global, dynamic, living structure of the Internet.

The development of IoT depends on a number of new technologies such as wireless sensor networks (WSNs), cloud computing and information sensing. In IoT-based information systems, a low-cost data acquisition system is necessary to effectively collect and process the data and information at IoT end nodes (IEN). In this context, WSNs play an important role, since they consist of a large number of IENs to cover a wide application field (such as IoT-based modern healthcare system) by acquiring and reporting data about different phenomena and events of interest, anytime and everywhere. On the other hand, security is also an imperative requirement to guarantee the availability and functionality of IoT. However, guaranteeing security for IoT is challenging since miscellaneous IoT devices, communication interfaces, and applications lead to many different security requirements and also increase the cost of deploying the corresponding security protections. IoT security solutions have not been standardized thoroughly due to the wide range of applications with vastly different security requirements. The requirements of security in an IoT application should be considered through the following three aspects: hardware, communication, and system model. Here, hardware security considers the physical security of the IoT devices while communication security of IoT applications considers confidentiality and integrity of communication between IoT entities (e.g., end devices, network infrastructures, service providers, information processing systems) and application data in storage. The security of each IoT application may vary according to the system model. For instance, in some applications (e.g. VANET, mobile communication, IoT-based healthcare system) the privacy of the involved entities should be taken into consideration, while in some other IoT-based applications like cloud-based IoT applications, secure data access permissions and key-management are required to be considered.

A. Related works on IoT-based healthcare systems

In the recent years, a substantial amount of researches have been performed for IoT-based human activity recognition and monitoring using wearable sensors' data. In this section we briefly reviewed some of the existing approaches. A list of recent researches on activity detection using different types of sensors and classification methods, and under different data acquisition protocols have been provided in [16]. Mukhopadhyay [5] reviewed different technologies and systems available for human activity monitoring based on wearable sensors. Altun *et al.* [17] provided a comparison of different classification techniques used for classifying human activities based on the data from the sensors in body sensor networks, whereas different classifications techniques for human activity recognition based on wearable sensors were reviewed in [18]. A similar study has been performed in [19]. In [20], Mannini *et al.* used support vector machine to classify physical activities based on a single accelerometer attached either to the ankle or wrist. In [21], an approach was proposed based on a one-

P. Gope is with the Department of Computer Science, University of Sheffield, UK (Email: p.gope@sheffield.ac.uk)

Y. Gheraibia is with the Department of Computer Science, University of York, UK (Email: youcef.gheraibia@york.ac.uk)

S. Kabir is with the Department of Computer Science, University of Bradford, UK (E-mail: s.kabir2@bradford.ac.uk)

B. Sikdar is with the National University of Singapore, (Email: bsikdar@nus.edu.sg)

Corresponding author: Dr. Prosanta Gope

TABLE I
COMPARISON BETWEEN EXISTING IOT-BASED HEALTH-CARE SYSTEMS IN TERMS OF DESIRABLE PROPERTIES (DP)

Schemes	**DP1**	**DP2**	**DP3**	**DP4**	**DP5**	**DP6**	**DP7**
Malan et al. [1] (Codeblue)	No	No	No	No	No	No	No
Ng et al. [2] (Ubimon)	No	No	No	No	No	No	No
Wood et al. [3] (Alarmnet)	Yes	No	No	No	Yes	No	Yes
Ko et al. [4] (Medisn)	Yes	No	No	No	No	No	No
Mukhopadhyay et al. [5]	No	No	No	No	No	No	Yes
Gope et. al. [6] (BSN-Care)	Yes	Yes	Yes	Yes	Yes	No	No
Wang et al. [7] (Healthedge)	No	No	No	No	No	No	No
Yeh et al. [8]	Yes	No	No	Yes	No	No	No
Kong et al. [9]	No	No	No	No	No	No	Yes
Yang et al. [10]	No	No	No	Yes	Yes	No	No
Sowjanya et al. [11]	Yes	Yes	Yes	Yes	No	No	No
Kumar et al. [12]	Yes	Yes	Yes	Yes	Yes	No	No
Binu et al. [13]	Yes	Yes	Yes	Yes	No	No	No
Shuai et al. [14]	Yes	Yes	Yes	Yes	No	No	No
Sengupta [15]	Yes	Yes	Yes	Yes	No	No	No
Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes

DP1: Authentication; **DP2:** Privacy of the User; **DP3:**Secure Localization; **DP4:** Resistance to Replay and Forgery Attacks; **DP5**:Data Security; **DP6:** Physical Security of the Sensor Nodes; **DP7:** Multi-sensor-based decision-making system

class support vector machine and a kernel nonlinear regression for abnormal human activity detection. Bao and Intille [22] developed algorithms for physical activities detection based on data collected using five biaxial accelero-meters. They showed that among different classifiers the decision tree classifiers provided best performance in their experiment. Maurer *et al.* [23] showed a real time physical activity recognition system which can identify activities based on data from multiple sensors worn on different body positions. Wang *et al.* [24] proposed a hierarchical model for activity detection where activity is detected using a two step process. In the first step, physical gestures of a person is detected at the sensor node level. This information is used in the second level to identify complex physical activities. The authors in [25], [26] used both supervised and unsupervised settings for human activity detection based on data from wearable sensors. Zhang and Sawchuk [27] proposed a method for human activity recognition based on sparse representation-based framework. They showed that if the dimension of the features is equal to or greater than 40 then their approach performs better than other classification methods such as nearest neighbor, support vector machine, and naive Bayesian classifier. Recent research on human activity recognition include [28], [29].

B. Problem statement and motivation

A remote health monitoring system is a modern IoT-based healthcare system where a patient's vital body state can be monitored remotely. Traditionally the detection systems were only found in hospitals and were characterized by large and complex circuitry which required high power consumption. Continuous advances in the semiconductor technology industry have led to sensors and microcontrollers that are smaller in size, faster in operation, low in power consumption and affordable in cost. In recent times, several systems have been proposed [1]–[10] to address the existing issues in remote health monitoring. The systems have a wireless communication feature that sends the sensor information wirelessly to a remote server. However, only a few of them have considered security (as shown in Table I). For instance, the works presented in [1], [2], [7] were not able to provide any concise solution to meet the desirable properties. On the other hand, [5], [9] can take into account data from multiple sensors while making a decision, but they are not able to satisfy other desirable properties. The approach proposed in [3] addressed the authentication and data security issues while featuring a multi-sensor-based decision-making scheme. Among the recent works, each of [8] and [10] has featured only two desirable properties. Both of these approaches are resistant to replay and forgery attacks, but the former can provide secure authentication functionality and the latter can provide data security. Recently, a few more interesting authentication protocols such as [11]–[15], [30] have been proposed for ensuring security in IoT-based healthcare systems. Among them, only [12] has considered the data security (both privacy and integrity) features. From Table I, it is clear that only the scheme proposed in [6], i.e., a secure IoT-based modern healthcare system (BSN-Care) using body sensor networks can ensure most of the desirable security features such as secure localization, privacy, and integrity of the BSN data through lightweight cryptographic solutions. However, like the other existing schemes, the BSN-Care system cannot ensure the physical security of the sensor nodes. In addition, BSN-Care has some shortcomings in the decision making process which can make the system inefficient. BSN-Care is a single parameter-based health monitoring system where the decision is taken based on the reading of a particular sensor. While the system collects heartbeat detection system data, fall detection system data, temperature data and few other parameters, only

one the data sets is then availed for remote detection via a local processing unit (LPU). This leads to the following issues in the BSN-Care system:

- **Ambiguous decision-making process:** Decision is made based on the data from a single sensor, which can be misleading in many cases. For instance, in the existing BSN-Care system the blood pressure (BP) sensor is responsible for monitoring the blood pressure of a patient. In this context, the BP sensor sends its reading to the BSN-Care server (via LPU). After receiving the reading, if the server finds any abnormality (such as high blood pressure), then it takes necessary action based on rules defined in the action table (see Table II). Now, there could be several reasons for getting a high blood pressure reading from the BP sensor. For example, one possibility could be that the patient is sick while another possibility could that the patient is doing some routine exercise like running. However, in the current BSN-Care system, it will be a difficult job to the BSN-Care server to differentiate these two different circumstances.
- **Faulty Sensor Nodes:** If for some reason the data from the BP sensor is unavailable due to equipment or network failure, then the BSN-Care system would not be able to make a decision.
- **Lack of physical security:** In general, IoT devices are small, simple, low cost, and are often installed in locations where an adversary may capture them easily. Therefore, physical security of IoT devices is a major concern. For example, keys stored in the device memory may be read off a physically captured device and then used by an adversary to launch an attack. Similarly, the sensor nodes and the LPU device in a BSN-based system are not tamper-proof. Hence, they are susceptible to compromise. Unfortunately, none of the existing IoT-based healthcare systems ensure physical security of the sensor nodes.

It should be noted that although the BSN-care system has some shortcomings, it can fulfill most of the security requirements, which are imperative in designing any IoT-based health-care systems. On the other hand, there are some IoT-based systems such as [5] and [3] that have considered a multi-sensor based decision making process. However, they have not considered the desired security properties as shown in Table I. This article seeks to address all the aforesaid weaknesses in IoT-based healthcare systems. In this regard, this paper extends the capability of the BSN-Care system by proposing an enhanced system that introduces a secure PUF-based authentication scheme along with a fault-tolerant decision-making process. The major contribution of this article can be summarized as follows:

- A secure anonymous authentication and key-agreement scheme using physical unclonable functions, which allows the LPU to securely transfer the sensor data to the server.
- A machine-leaning-based fault tolerant decision making scheme which can take into account data from multiple sensors in order to make a right decision in the presence of uncertainty and missing data. The mathematical notations used in this article are defined in the Table III.

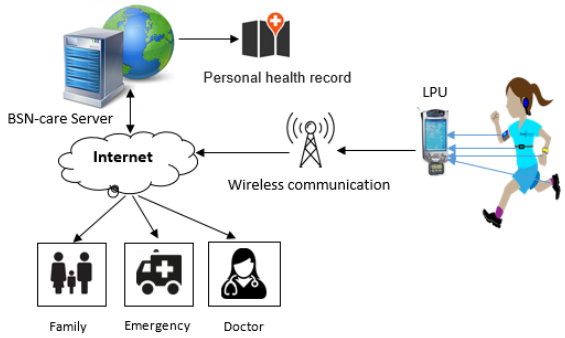

Fig. 1. BSN-Care System [6]

TABLE II
ACTION TABLE IN BSN-CARE BASED ON SINGLE SENSOR DATA [6]

BSN BP data	Action	Response
BP $\leq$ 120	No action	Null
120<BP$\leq$160	Inform Family Members	FR:T/F
BP>160 and FR:F	Inform Local Physician	PR:T/F
BP>160, FR:F and PR:F	Inform Emergency	ER:T/F
FR: Family response; **PR:** Physician response; **ER:** Emergency response		

TABLE III
MATHEMATICAL NOTATION

Notation	Definition
P_u	PUF attached with the device
C_i/R_i	Challenge/response for i-th session
X	Medical records
K	Kernel function
ω, b	Hyperplane
δ	Relaxation parameter
ξ	Number of total records
ψ	Positive changes between variable values
Φ	Negative changes between variable values
α_i	The influence of example i
Arc_X	Average rate of changes for X

II. PROPOSED AUTHENTICATION SCHEME

Before presenting the proposed protocol, we first present a brief introduction to PUFs in this section. A PUF can be regarded as a unique physical feature of a device, just like the biometric features of human beings such as fingerprints. The most notable property of a PUF is that it cannot be reproduced using cryptographic primitives, rather, it requires a physical basis. Thus, the idea behind using a PUF in IoT systems is

that just like human beings, every device will have a unique fingerprint in the form of a PUF and this fingerprint cannot be reproduced or cloned. In another way, a PUF is defined as "a function that maps a set of challenges to a set of responses based on an intractably complex physical system" [31], [32]. Therefore, a PUF can be considered as a function, which takes a challenge in the form of a string of bits and produces a response in the form of a string of bits. We represent a PUF as a function P as follows: $R = P(C)$, where R is the response of a PUF, while C is the challenge given to the PUF. In this paper, we make the following assumptions regarding the system:

- An IoT device (such as sensors and LPU) consists of an embedded system equipped with a PUF. Any physical tampering with the PUF such as an attempt to separate it from the embedded system will destroy the PUF.
- The IoT device micro-controller and the PUF are assumed to be a system on chip (SoC). Therefore, based on SoC security [33], [34], the communication between them is considered to be secure, in the sense that it will be difficult for an adversary to intercept the *on-chip communication* between the device and the PUF and break the SoC security within polynomial time.

We now describe our PUF-based authentication scheme. There are two phases in our proposed scheme: setup phase and the authentication phase. In the setup phase, the LPU sends its enrollment request to the BSN-Care server. After successful enrolment, the LPU gets certain secret credentials which will help the server to authenticate the LPU during the authentication process. If the authentication is successful, then the LPU will be able to securely transfer the information to the server via a communication medium, run by a third-party organization.

A. Registration Phase

For the registration process of the proposed scheme, the LPU and server need to execute the following steps:

Step R1: The LPU sends its identity ID_u to the server for a setup request through a secure channel.

Step R2: The server generates a challenge C_i for the i-th round and sends it to the LPU. It also generates a set of challenges $C_{syn} = \{c_1, \cdots, c_n\}$, which are used later for addressing desynchronization or DoS attacks.

Step R3: The LPU uses its PUF (P_u) and extracts the PUF outputs $R_i = P_u(C_i)$, and $R_{syn} = P_u(C_{syn})$ and subsequently sends $\{(R_i, R^x_{syn})\}$ to the server through the secure channel.

Step R4: Next, the server generates a unique pseudo identity PID^i_u and a set of fake ids $FID = \{\mathrm{fid}_1, \cdots, \mathrm{fid}_n\}$ and sends them to the LPU. Finally, the server needs to store $\{(PID^i_u, FID), ID_u, (C_i, R_i), (C_{syn}, R_{syn})\}$. On the other hand, the LPU only needs to store $\{(PID^i_u, FID)\}$.

B. Authentication Phase

Conceive that the LPU has been assigned to collect sensor data from the patient. In this phase of the proposed scheme, both the LPU and the server can authenticate each other and establish a session key for secure communication. The detailed description of the phase is as follows:

Step AU1: The LPU generates a random number N_u and then submits his/her current pseudo identity PID^i_u , and N_u to the BSN-Care server.

Step AU2: Upon receiving the authentication request, the server first locates the pseudo identity PID^i_u and subsequently selects the *challenge-response pair* (CRP) (C_i, R_i), from its database. Next, the server generates a nonce N_s, a unique pseudo identity for the $(i+1)$-th round PID^{i+1}_u, and subsequently, calculates $PID^* = PID^{i+1}_u \bigoplus R_i$ and $Res_{Serv} = h(R_i||PID^*||N_u)$. Hereafter, the server composes a response message $\{PID^*, N_s, C_i, Res_{Serv}\}$ and sends the message to the LPU.

Step AU3: After receiving $\{PID^*, N_s, C_i, Res_{Serv}\}$, the LPU first extracts the PUF outputs $R_i = P_u(C_i)$, and then computes and verifies the hash-response Res_{Serv}. If the verification is unsuccessful, the LPU aborts the execution of the protocol. Otherwise, the LPU derives $PID^{i+1}_u = PID^* \bigoplus R_i$, $C_{i+1} = h(C_i||R_i)$, $R_{i+1} = P_u(C_{i+1})$, $EL = LAI_u \bigoplus h(R_i||N_s)$, $R^*_{i+1} = h(ID_u||R_i) \bigoplus R_{i+1}$, $SK = h(N_u||R_i||N_s)$, $Res_{Lpu} = h(EL||R^*_{i+1}||SK)$, and subsequently composes a message $\{R^*_{i+1}, Res_{Lpu}, EL\}$ and sends the message to the server.

Step AU4: Upon receiving the response message from the LPU, the server first computes $SK = h(N_u||R_i||N_s)$, and then checks the response parameter Res_{Lpu}. If the verification is successful, then the server decodes $LAI_u = EL \bigoplus h(R_i||N_s)$ and validates LAI_u with the location of the LPU . After successful validation, the server computes $C_{i+1} = h(C_i||R_i)$, $R_{i+1} = h(ID_u||R_i) \bigoplus R^*_{i+1}$. Finally, the server replaces $\{PID^i_u, (C_i, R_i)\}$ with $\{PID^{i+1}_u, (C_{i+1}, R_{i+1})\}$.

Note that, for addressing DoS or synchronization attacks in our proposed scheme, we utilize the concept of synchronous *CRP* pairs (C_{syn}, R_{syn}) and the set of fake ids $FID = \{\mathrm{fid}_1, \cdots, \mathrm{fid}_n\}$. In cases where the server cannot identify the pseudo identity PID^i_u or if the LPU fails to receive any response message with the parameters $\{PID^*, N_s, C_i, Res_{Serv}\}$, then the LPU needs to choose one of the unused fake identities fid_j from the set of fake ids, i.e., FID and the server needs to select one of the unused synchronous *CRP* pair $(c_x, r_{syn}) \in (C_{syn}, R_{syn})$. Once both the LPU and server mutually authenticate each other by using fake identity fid_j and unused synchronous *CRP* pair (c_x, r_x), the server will delete (c_x, r_{syn}) from its database and both the LPU and the server delete the fake identity fid_j from their memory. Details of this phase are shown in Fig. 2. It should be noted that even though we have focused on the authentication between the LPU and the server, the proposed authentication scheme can also be applied between the sensor nodes and the LPU to mutually authenticate each other and share a session key. On the other hand, for ensuring both the privacy and integrity in our proposed system, when the sensor nodes send data to the LPU unit then they need to use OCB authenticated encryption mode [35] with fresh nonce N and the shared session key *SK*. Similarly, when the LPU sends its periodical updates to the server then the LPU also needs to use OCB mode. In this way, the recipient can check the privacy, integrity, and the freshness of the received data.

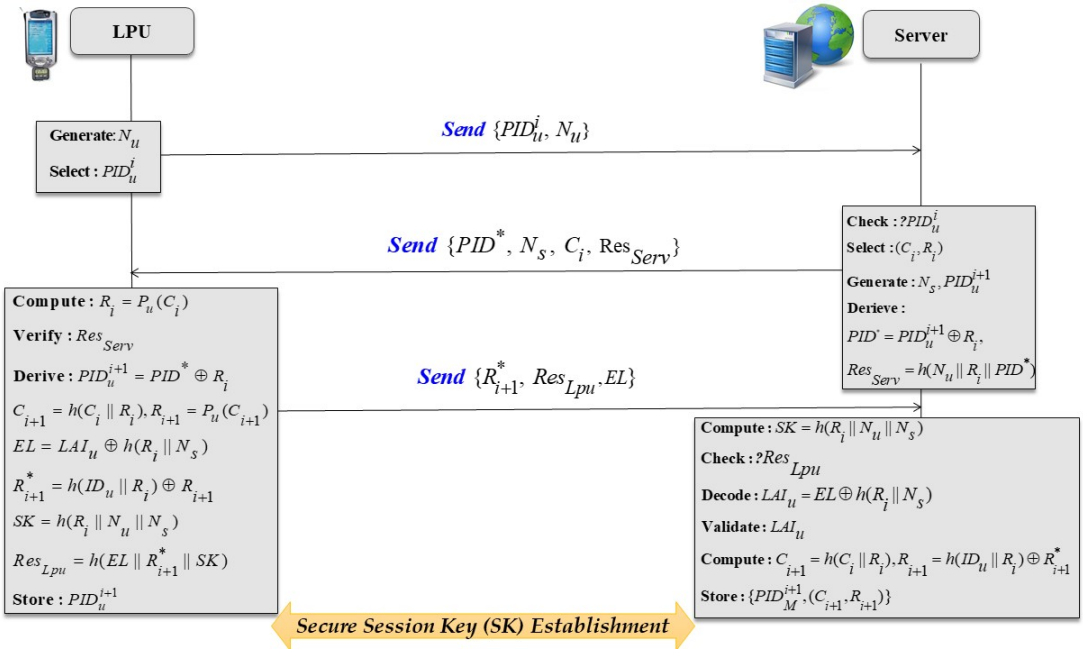

Fig. 2. Proposed PUF-based Anonymous Authentication Scheme.

III. Proposed Fault-Tolerant Decision Making Scheme

A graphical representation of the proposed IoT-based healthcare system with the fault-tolerant decision making support is shown in Fig. 3. The proposed mechanism enhances the basic architecture of the existing BSN-Care system [6] to enable it for fault-tolerant decision making. The approach is data-driven, i.e., it will work based on the data received by the BSN-care server from the local processing unit (LPU) using cellular network such as LTE-A/CDMA, etc. Interested readers can refer to the original BSN-Care article [6] for more detailed information about data collection process. In BSN-Care, the decision about potential actions is made based on the data from a single sensor. In the proposed decision making approach, under the condition of abnormal behaviour (e.g., failure of BP sensor), data from other sensors such as temperature and motion sensors are taken into account in addition to the data from BP sensor to make a decision. This will help to address the false positive and false negative decisions taken by BSN-care. Moreover, it will also handle the scenario when the data from a sensor in not available to make a decision by BSN-Care.

To achieve the fault-tolerant decision making capability, the proposed system uses a machine learning approach. In particular, it uses support vector machines to learn the normal behaviour of the patient from the sensory data (this step is not shown in Fig. 3). These training data are collected from the server. Details of normal behaviour characterization are given in section III-A. After the initial normal behaviour model is formed, whenever a new record is sent from the sensors to the server, unlike the classical decision making process of BSN-Care, the proposed framework would perform a number of tasks to reach to a robust decision. Note that running a machine learning algorithm would require high computation power that the sensors/nodes may not afford to have. Therefore, in this paper, we consider that all the heavy computations are performed in the server.

Whenever a new record is sent from the server to the decision making module, it first checks to see if the record is complete, i.e., there is no data missing from a sensor. If the record is complete, it is checked against the normal behaviour model of the patient to detect anomaly. A detailed description of the anomaly detection process is provided in section III-A. If no anomaly is detected, the record is saved in a central repository and a decision about the action is made based on predefined rules. Note that, to keep the normal behaviour model of the patient updated, it is regenerated after a certain number of new normal record has arrived. This number could be defined by user. In this paper, we regenerated the model after receiving 12 normal records.

If an anomaly is detected in the new record, correlations are generated among the different parameters in the record. The process of generating correlation measures is described in Section III-C. Based on these correlations and the action suggested by the traditional BSN-Care system, the proposed approach will either make a decision to take an emergency action or keep the action suggested by the traditional BSN-Care system, but add more helpful information with this.

At the beginning, if the newly arrived record is identified to be incomplete (i.e., having missing data), then a separate temporary behavioural model (represented as red color behavioural model in Fig. 3) is created by considering this incomplete record. After that, the missing data are predicted and imputed to the incomplete record following the process described in Section III-B. In this way, the record is made complete, and afterwards it is processed for decision making process in the same way as it was done for a complete

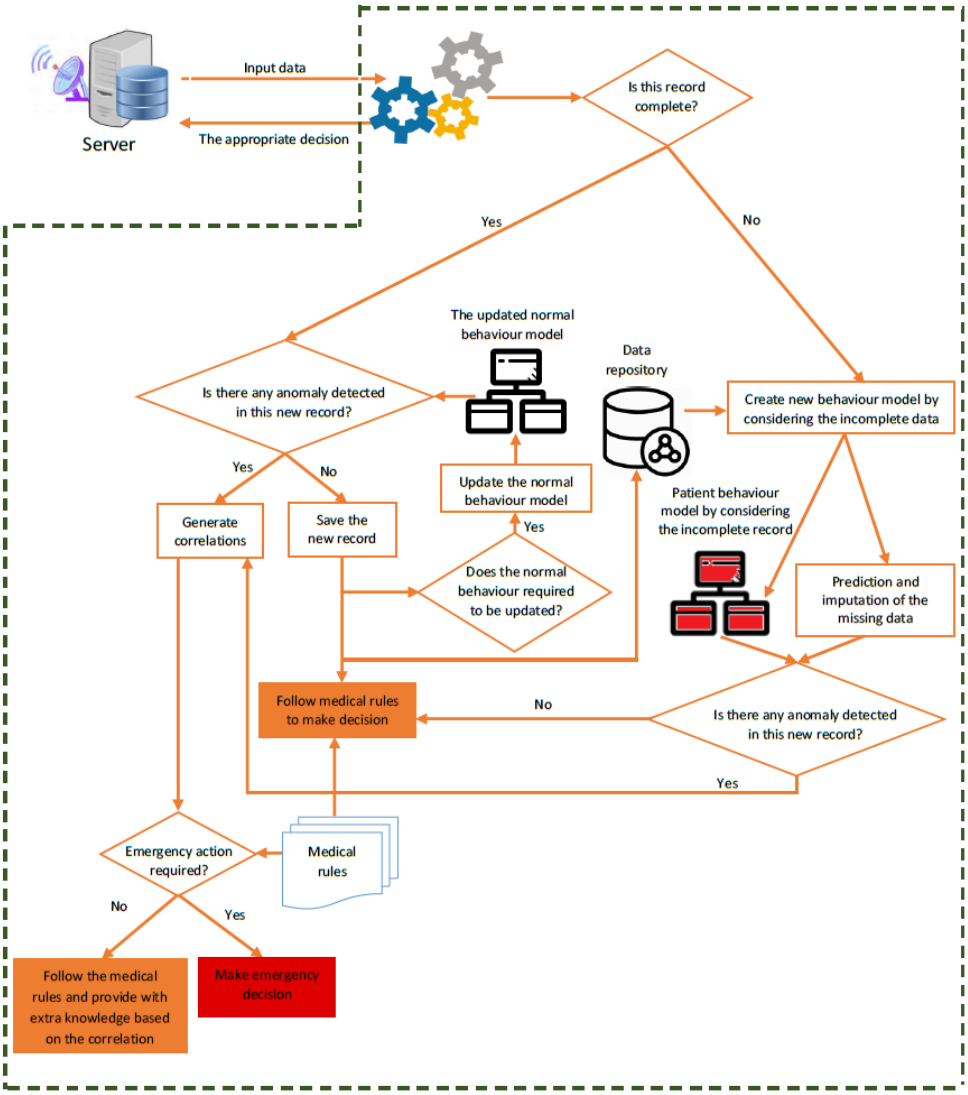

Fig. 3. Flow chart of the proposed decision making process

record. However, in this case, the reference model used during anomaly detection is the temporary model created considering the incomplete data, not the normal behaviour model.

A. Anomaly Detection Process

In the proposed system, the first step to detect any anomaly in the patient's behaviour is to generate a model for the normal behaviour of the person after obtaining a set of incoming records from the real system. Thus, the framework has to wait for a sufficient number of records to model the normal behaviour. The initial incoming data from the system is considered to be normal, i.e., all data are labelled with one class *'Normal'*. The normal behaviour characterization process is formulated as one-class classification problem using only data from the assigned class. The One Class Support Vector Machine (OC-SVM) classifier [36] has been used to generate the normal behaviour. We use a semi-supervised classification strategy, which uses a modified classification to formulate the normal behaviour and detect any deviation from that behaviour.

The OC-SVM problem for the normal behaviour generation from the data collected by the system can be formulated as follows. Let $X = \{x_1, x_2, x_3, \cdots, x_n\}^m$ be a set of instances with label *'Normal'* representing the streaming data coming continuously in real time from the system. n is the number of parameters of the system (data captured from the different sensors in the system) and m is the number of instances at a time instant t.

Let $K : R^n \rightarrow H$ be the kernel function that transforms the input data to the features space H. To form the normal behaviour model, the OC-SVM used in this paper aims to minimise the distance between points on the same class as follows:

$$\min_{\omega,b,\delta,\rho} F(\omega, b, \delta, \rho)^n = \frac{1}{2}\|\omega\|^2 + \frac{1}{vn}\sum_{i=1}^{n}\delta_i - \rho \qquad (1)$$

$$\text{Subject to}: \left(\omega^T K(x_i)\right) \geq \rho - \delta_i, \;\; i = 1, \cdots, n \qquad (2)$$

where $\delta_i \geq 0$ is the relaxation parameter that is used to balance

the experienced risk minimisation. ω and b are parameters used for deciding the separating line (hyperplane) that defines the decision distance that separates points assigned to the normal behaviour from other points. $v \in \ ]0,1]$ and vn sets upper bounds on the out-of-class training examples and lower bound on the number of training used as support vector.

The problem of finding the optimal hyperplane, which facilitates the separation between classes of data, is formulated as follows:

$$\min_{\alpha} Q(\alpha) = \frac{1}{2}\sum_{i,j}^{n} \alpha_i \alpha_j K(x_i, x_j) \tag{3}$$

$$\text{Subject to :} 0 \leq \alpha_i \leq \frac{1}{vn}, \sum_{i}^{n} \alpha_i = 1 \tag{4}$$

where α_i is the influence of example i. The decision function is given by:

$$f(x) = sign\left((\omega, K(x)) - \rho\right) \tag{5}$$

where the $sign$ function is the derivative of the absolute value function (-1, +1). ρ is given by

$$\rho = \sum_{j=0}^{n} \alpha_i K(x_i, x_j). \tag{6}$$

B. Missing Data Prediction Algorithm

Missing data is a well-known problem in sensor-based systems and refers to instances when no data is available for one or more variables in a given observation interval. The proposed approach for imputing missing data in this paper is based on two steps. In the first step, we use the nearest neighbour algorithm to select the nearest record that matches the incomplete data record. Note that prior to applying the nearest neighbour algorithm, we reduce the dimension of the complete record to match the dimension of the missing record. The values of the missing variables are not taken directly from the nearest record as a prediction of the missing data because the data used in the system are healthcare data where any change can make a difference in the decision-making process. The proposed data imputation process uses the average rate of change (Arc) values that represent the rate of growth or reduction of two variables together. Arc can be calculated as:

$$V_j = \sum_{i=0}^{\xi-1} (x_{i+1} - x_i) \ \ j = 0, \cdots, \xi - 1 \tag{7}$$

$$Arc_{i+} = \frac{\sum_{k=0}^{\psi} V_k}{\psi} \ if \ (V_k \geq 0) \ \ i = 1, \cdots, \xi \tag{8}$$

$$Arc_{i-} = \frac{\sum_{k=0}^{\Phi} V_k}{\Phi} \ if \ (V_k < 0) \ \ i = 1, \cdots, \xi \tag{9}$$

where:

- V_j is the sum of the difference between two consecutive values.
- ξ, ψ and Φ are the number of total records, positive, and negative changes between variable values, respectively.
- Arc_{i+} is the average rate of change of positive differences.
- Arc_{i-} is the average rate of change of negative differences.

Algorithm 1 Missing data prediction

Require: The person's data history and new record with missing data

Ensure: Prediction of missing data

1: Extract data instances without missing data and reduce their dimension to match the dimension of the missing record
2: Determine the closest matching record with Euclidean distance
3: Generate correlation between variables for the original data
4: Calculate the average rate of changes (Arc) for the missing variable and the highly correlated variable to the missing parameter
5: Predict the missed value from the nearest neighbour and the Arc

The missed value will be calculated based on the nearest record and the Arc positive or negative changes. The algorithm calculates the missing values by using the following equations according to the changes, i.e., whether the values of the new records are going up or down:

$$X_{Miss} = X_{NR} + \left(Arc_{X+} * \frac{|Y_{MR} - Y_{NR}|}{Arc_{Y+}}\right) \tag{10}$$

$$X_{Miss} = X_{NR} + \left(Arc_{X-} * \frac{|Y_{MR} - Y_{NR}|}{Arc_{Y-}}\right) \tag{11}$$

where:

- X_{miss} is the missing value of variable X. Y is the highly correlated variable to X and Y_{MR} is the value of Y in the record where the value of X is missing.
- X_{NR}, Y_{NR} are the values of the variables X and Y in the nearest record to the record with missing value.
- Arc_X is the average rate of changes for variable X.
- Arc_Y is the average rate of changes for variable Y.

C. Correlation Measures

In the proposed decision making scheme, when an anomaly is detected in the newly arrived dataset, correlations between different parameters within the dataset are measured to identify the potential causes of the anomaly. By using correlation measures we can identify how a parameter is correlated with other parameters, i.e., how the changes in one parameter is related to the changes in other parameters. While it is known that correlation does not imply causality [37], experts or machine learning algorithms with prior knowledge can interpret this correlation in a specific scenario. For example, let X and Y be the readings from the motion and blood pressure sensor of the proposed system. A strong observed correlation between X and Y can be interpreted as that the motion of a person influences the blood pressure of the person, or blood pressure influences motion, or motion and blood pressure influence each other or a third variable influences both motion and blood pressure. In this paper, we use Pearson

correlation coefficient to measure the correlation between two variables. The Pearson correlation coefficient r_{xy} for random variables X and Y is given by:

$$r_{xy} = \frac{\sum_{i=1}^{n}\left(X_i - \overline{X}\right)\left(Y_i - \overline{Y}\right)}{\sqrt{\sum_{i=1}^{n}\left(X_i - \overline{X}\right)^2}\sqrt{\sum_{i=1}^{n}\left(Y_i - \overline{Y}\right)^2}}. \quad (12)$$

IV. Illustrative Example

The server receives data from sensors at regular intervals. The collected data is then transferred to the machine learning agent to decide on the best course of action. Table IV shows an example of the data received from the sensors at 12 consecutive time instances, which is the number used by this example to start building the normal behaviour model of the person. The system keeps using the static medical rules to decide the required action for the received data until it can build the normal behaviour model. In this experimentation, four scenarios are evaluated based on the incoming data from sensors and the availability of data.

TABLE IV
Training Dataset

Time Instance	Temperature (°C)	BP	Motion
T1	37	80	0.2
T2	37	85	0.2
T3	37	85	0.3
T4	37	87	0.3
T5	37	89	0.4
T6	37	115	1.2
T7	37.25	89	0.4
T8	37.25	95	0.5
T9	37.25	119	1.6
T10	37.25	98	0.6
T11	37.25	105	0.7
T12	37.25	106	0.8

A. Scenario 1

T13	37.25	108	2.2

The first scenario considers the case where an abnormal behaviour is detected, but the medical rules say that no action is required for this data. This scenario can be considered as false negative in the sense that the BSN care indicates a person does not have a health condition when the person actually may have it. As no alarm is raised in this case, the person may face serious consequences due to the lack of timely action. As seen in the collected data from the sensors, the BP is 108. According to the rules defined in Table II, this BP value is inside the normal range of blood pressure, and therefore no action is advised. However, consider the situation that the machine learning agent detects an anomaly in this particular instance of the data because this dataset falls outside the normal behavior model of the person. In this case, the machine learning agent will generate correlations between the BP value and with the other sensors' data using previous records. Fig. 4 shows the correlations among different variables and it can be seen that the positive correlation between the blood pressure and the movement is very high ($r_{BP,Motion} = 0.96$). This means it is expected that if the movement of the person increases then the BP of the person should also increase, and vice versa. The data for this particular scenario depicts a considerable increase in the value received from the motion sensor, i.e., an increase in movement, but the BP has not increased accordingly. That means the BP value is not harmonized with the movement. This kind of abnormality may be caused by different reasons. In the more serious case, it could be caused by deterioration in the person's health condition. Other causes may be that either the BP sensor or the motion sensor, or both, are giving faulty readings. Considering the worst case scenario, in this case, the machine-learning algorithm will make an emergency decision to check the person and also the suspected faulty sensors.

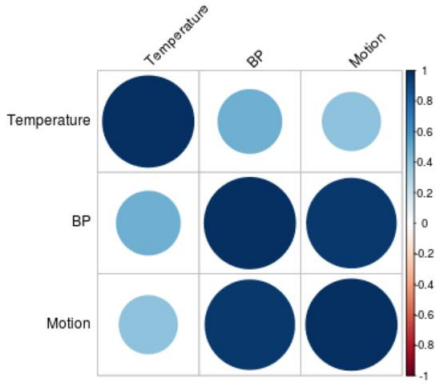

Fig. 4. Correlations among the variables used in the BSN care example.

B. Scenario 2

T13	37.25	125	2.2

The second scenario is similar to the first scenario where an abnormal behaviour is detected, but in this case we assume that there is a medical rule saying that an action is required for these data. In this case, the machine learning algorithm will generate correlations based on the new abnormal behaviour and the previously collected data. In this case the positive correlation between the blood pressure and the movement is very high ($r_{BP,Motion} = 0.96$). Unlike the first scenario, in this scenario, the BP value is harmonized with the movement, i.e., both BP and movement values increased together. Therefore, a possible explanation for this scenario is that due to the increase in the motion of the person, his/her blood pressure increases. As a result, the machine learning agent will generate the final decision based on the medical rules with extra knowledge (correlation) which can be useful for decision interpretation by doctors or family members.

C. Scenario 3

T13	37.25	X	2.2

The third scenario is different from the two previous scenarios. This scenario considers the case where the server receives

incomplete data. This situation of incomplete record can happen if a sensor malfunctions or fails to send data. In this case, the machine learning agent will construct a new normal behaviour model of this person while excluding the failed sensors. In this example, the agent will thus construct a new normal behaviour of the temperature and motion attributes. After that, the incomplete record will be tested to check if it fits the requirement of the new normal behaviour or not. The next step of the algorithm is to construct the correlation between sensors with and without missing data. The correlation is calculated based on previously collected data.

The next step of the algorithm is to predict the missing data based on the generated correlation and the nearest neighbours algorithm. The decision making process will be based on the medical rules of the predicted value of the failed sensors. For this example, record T9 is the nearest neighbour to T13. The algorithm will thus use the value of the BP of this record as reference to predict the BP of the new record. The algorithm will then calculate the average rate of changes (*Arc*) for the BP and the correlated parameter (in this example the motion). The positive Arc for the BP is 7.11 and the negative is -17, and for the motion the positive $Arc = 0.26$ and negative $Arc = -0.9$. The increase in the motion for the new record compared to the nearest neighbour (T9) is 0.8 and the estimated BP value for the new record is 140. To complete the record this newly computed value is imputed into the record. The record is then treated as an complete record and decision is made accordingly as described earlier. The accuracy of missing data imputation is sensitive to different factors. The performance of the missing data imputation algorithm can be measured in different ways. In this paper, we measured the accuracy using a set of metrics to check the capability of the algorithm to classify the each instance in the appropriate class. These metrics are based on the TP (True Positive), TN (True Negative), FP (False Positive) and FN (False Negative) values. We calculated the accuracy, True Positive Rate (TPR) (sensitivity) and False Positive Rate (FPR) (specificity) of the algorithm based on the following expressions:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{13}$$

$$TPR = \frac{TP}{TP + FN}, \tag{14}$$

$$FPR = \frac{TN}{TN + FP}, \tag{15}$$

where TP, TN, FP, and FN are the number of predictions that are true positive, true negative, false positive and false negative, respectively.

The Accuracy represents the capability of the algorithm to predict negative and positive instances correctly. However, the TPR and FPR are for the prediction of positive and negative instances, respectively. In our testing strategy, we have tested the algorithm with different percentages of missing data to observe the performance of the algorithm. The performance of the algorithm is presented in Table V. The results show the different evaluation metrics of the missing data algorithm for a different number of missing values. As can be seen, the sensitivity of the algorithm is 93.61% when the percentage of the missing data is 3%. The sensitivity has not changed significantly when the percentage of missing data increases, which shows the capability of the algorithm to maintain a reasonable performance with different missing data percentages. Also, it continues to maintain a reasonable level of accuracy and ability to label the true class even when we remove a large fraction of the data.

TABLE V
PERFORMANCE OF MISSING DATA PREDICTION ALGORITHM

Missed data (%)	Accuracy (%)	Sensitivity (%)	Specificity (%)
3%	89.52%	93.61%	70.76%
7%	86.43%	93.03%	60.38%
10%	84.24%	92.61%	54.93%
14%	81.50%	92.05%	48.04 %
17%	79.55%	91.63%	44.17%
20%	77.70%	92.22%	40.88%
30%	72.10%	89.87%	32.74%
40%	67.25%	88.56%	27.31%

The performance of the anomaly detection process is evaluated based on the confusion matrix results by calculating the TPR and FPR. These two parameters were defined earlier in Equations (14) and (15), respectively. We generate eight different classes of missing data, these classes represent different percentages of missed data in the used dataset. In our experimentation, we calculate the effect of the missing data percentage on the performance of the algorithm. Fig. 5 presents the TPR and FPR of the anomaly detection process to show the capability of the algorithm to detect the outliers.

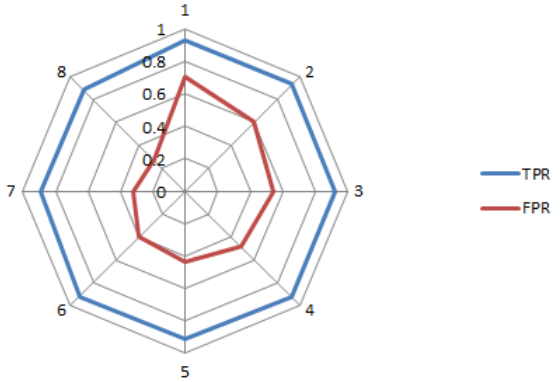

Fig. 5. TPR and FPR rates for the anomaly detection process for eight different classes of missing data.

V. DISCUSSION

In this subsection, we first demonstrate that our proposed scheme can ensure all the desirable security properties and subsequently we show the effectiveness of the proposed fault tolerant system.

A. Security Consideration

- **Mutual Authentication:** In our proposed authentication scheme, the LPU authenticates the user based on

the validity of the key-hash response Res_{Serv}, where only the legitimate server having the valid *challenge-response pair* (CRP) (C_i, R_i), can compute $Res_{Serv} = h(R_i||PID^*||N_u)$. On the other hand, the server can authenticate the LPU based on the validity of the key-hash response $Res_{Lpu} = h(EL||R^*_{i+1}||SK)$, where only the valid device can extract the required PUF output R_i, and $SK = h(N_u||R_i||N_s)$, which are imperative in computing Res_{Lpu}.

- **User Privacy:** During the authentication process, the LPU uses the pseudo identity PID^i_u, which is valid only upto a particular session. After that, the LPU gets a new pseudo identity PID^{i+1}_u from the server for use in the next session. Now, if an adversary captures the message $\{PID^i_u, N_u\}$, then he/she will not be able to identify the user. On the other hand, in case of loss of synchronization between the LPU and the server, the LPU uses the unused fake identity. In this way, our proposed scheme can ensure user privacy. Besides, during the authentication process, the LPU hides it's location identifier LAI_u with EL. Since a random number N_s is used in computing EL and the value of R_i changes in every session, it is difficult for an adversary to identify a user. Only the server can locate the user. In this way, the proposed scheme ensures location privacy.
- **Physical Security of the Devices:** In order to detect any faulty and physically tampered device, the concept of PUF has been utilized. Now, if an adversary tries to tamper with the device or if the device is faulty, then the behavior of the PUF will be changed. In that case, for a given challenge (C_x), the PUF will not be able to generate the desired response (R_x), which can be easily comprehended by the receiving end. As discussed, the proposed authentication scheme can also be applied between the LPU and the sensor nodes. Therefore, it will be straightforward for the LPU to detect any fault in the sensor nodes. Moreover, the proposed protocol uses PUFs to generate the secret keys for secure communication in the network. This eliminates the need to store secret keys in a device's memory. Therefore, an attacker who has physical access to a device cannot obtain any secret keys from the device. Besides, any such tampering attempt would change the behaviour of the PUF and the server can detect such changes. In this way, the proposed protocol can ensure security against physical attacks.
- **Data Security:** In this paper, our main objective is to design an effective IoT-based modern e-health-care system that can ensure authentication with physical security. For data security, we adopt OCB or any other single-pass authenticated encryption algorithm.

Now, to analyze the performance of the proposed scheme more comprehensively, we compare the computational cost of the proposed authentication scheme with respect to [6] and [8], which also ensures authentication between the server and LPU devices. For this, we emulate the cryptograpic operations used in the proposed scheme, [6] and [8] on a HTC One X mobile device (Operating as LPU) with 890 MHz clock and an Intel Core i5-2500 processor (Operating at Server). For PUF operation, we consider 128-bit arbiter PUF circuit on a MSP430 with 890 MHz clock. The simulation uses the JCE library for evaluating the cryptoghapic operations used in the proposed scheme, [6] and [8]. Simulation outcomes show that each hash operation at the LPU and the server takes 0.065 ms and 0.038 ms, respectively. Each ECC operation at the LPU and the server takes 13.62 ms and 8.79 ms, respectively. On the other hand, each PUF operation takes 0.043 ms. Table VI shows that the performance of the proposed authentication scheme is better than others. Besides, in Table I, we have already shown that the proposed scheme ensures all the describable security features as well.

TABLE VI
COMPARISON BASED ON THE COMPUTATIONAL OVERHEAD

Schemes	**Computation Cost at the LPU**	**Computation Cost at the Server**
Gope et al. [6]	$7h \simeq 0.45$ ms	$7h \simeq 0.0266$ ms
Yeh [8]	$6ECC + 4h$ $\simeq 81.73$ ms	$6ECC + 4h$ $\simeq 52.75$ ms
Proposed Scheme	$5h + 2P \simeq 0.411$ ms	$5h \simeq 0.19$ ms
***h*:** Hash Operation; **ECC:** Elliptic Curve Operation; ***P*:** PUF operation;		

B. Effectiveness

As discussed in Section I-B, even though BSN-care system [6] has some shortcomings, it is more effective than other existing IoT-based healthcare systems (see Table I). Moreover, addressing of the unresolved security issues in Section II makes the BSN-Care system the most comprehensive approach among the existing IoT-based healthcare systems with respect to their ability to satisfy the desirable security properties. The main intention in designing a fault-tolerant decision making scheme proposed in this paper is to add to the strengths of BSN-Care by alleviating its limitations in the decision making process under the conditions of uncertainty. The new scheme enables the existing system to detect false negative and false positive scenarios, thus allowing it to make more robust decisions with additional knowledge. Moreover, the new decision making scheme can make decisions even when there are missing values in the dataset received from the sensors. We now compare our proposed decision making approach with the BSN-Care system. Table VII shows a comparison between the exiting BSN-care system [6] and the proposed decision making approach with respect to their features. It can be seen that the proposed approach alleviates the limitations of the BSN-Care system pointed out in Section I-B and introduces multiple features for improved decision making while enhancing the security features of the system.

As additional operations are performed in the proposed approach, it is expected that it will have a higher execution time with compared to the BSN-care system. In the existing BSN-care system, when a new dataset is made available to the

TABLE VII
COMPARISON OF FEATURES OF EXISTING BSN-CARE [6] AND PROPOSED APPROACH

Features	BSN-Care [6]	Proposed approach
F1	✔	✔
F2	✗	✔
F3	✗	✔
F4	✗	✔
F5	✗	✔
F6	✗	✔
F1: Decision making under normal condition; **F2:** False positive detection; **F3:** False negative detection; **F4:** Decision making with missing value **F5:** Faulty sensor detection **F6:** Resilience against physical attacks on sensors		

decision making block, it directly makes a decision based on medical rules. Let the time taken for this decision making be t_{BSN}. In the proposed scheme, we treat the complete and incomplete (i.e., with missing values from sensors) dataset differently. For a complete dataset, the scheme always checks to see if any anomaly exists in the record, and let the time taken for this check be t_a. If no anomaly is detected, then the decision is made in t_{BSN} time as in the original BSN-Care system. Thus, the total time taken in this case is t_a+t_{BSN}. On the other hand, when an anomaly is detected, an extra time of t_k is needed on top of $t_a + t_{BSN}$ to generate additional knowledge. Hence, in this case, the total time needed would be $t_a + t_{BSN} + t_k$. Now, for the dataset with missing value, the proposed framework estimates and imputes the value to the record to make it complete. In this regard, we assume that the time required for missing value prediction and imputation is t_m. After this operation, the decision is made in the same way as it is done for a complete record. Therefore, depending on the scenario as described above, the total time for decision making with missing value could be either $t_m + t_a + t_{BSN}$ or $t_m + t_a + t_{BSN} + t_k$. Next, in order to comprehensively analyse the performance of the proposed system, here we emulate the whole process of the scheme on a machine with an Intel core i7 processor and 16 GB of memory. Based on our experiments, using averages taken over 20 runs, the anomaly detection process takes approximately 1986 ms. On the other hand, in order to make a decision when no anomaly is detected, the simulation takes 3210 ms. Now, we consider a scenario when an anomaly is detected in the dataset. In this regard, the emulation takes 6132 ms. On the other hand, if there there are missing values in the dataset, an additional 1012 ms is required to estimate and impute the value to the record.

C. Formal Security Verification Using AVISPA Tool

In order to verify the security and robustness of the proposed security protocol in terms of the specific goals such as mutual authentication, replay attack protection etc., we performed a formal proof using AVISPA [38], which provides automated validation of security sensitive protocols and applications. It contains four backends and abstraction-based methods that are integrated through the high level protocol specific language (HLPSL). The outcome of the formal security verification of our proposed scheme using On-the-fly Model-Checker (OFMC) and Constraint Logic based Attack Searcher (CL-AtSe) backend is shown in Fig. 6 which shows that our proposed scheme is safe. That means our proposed scheme can accomplish all the goals. Due to space limitations, the details of the implementation process of the proposed scheme are provided in the supplementary material.

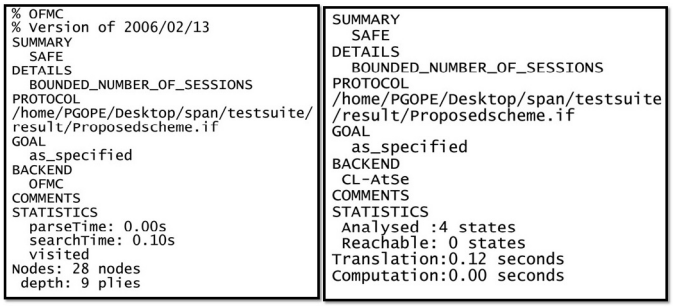

Fig. 6. The results obtained with the AVISPA tool.

VI. CONCLUSIONS

This paper presents a fault-tolerant decision making scheme for IoT-based healthcare systems to achieve robust decision making under the conditions of uncertainty while providing strong security features. Analyses show that our proposed scheme is efficient and can ensure the imperative features that are greatly important in designing any advanced IoT-based modern healthcare system.

ACKNOWLEDGEMENTS

This research was supported in part by Singapore Ministry of Education Academic Research Fund Tier 1 (R-263-000-D63-114).

REFERENCES

[1] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in *International workshop on wearable and implantable body sensor networks*, vol. 5. Boston, MA;, 2004.

[2] J. W. Ng, B. P. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G.-Z. Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (ubimon)," in *International conference on ubiquitous computing (Ubicomp)*, 2004.

[3] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "Alarm-net: Wireless sensor networks for assisted-living and residential monitoring," *University of Virginia Computer Science Department Technical Report*, vol. 2, p. 17, 2006.

[4] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "Medisn: Medical emergency detection in sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 10, no. 1, p. 11, 2010.

[5] S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321–1330, March 2015.

[6] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

[7] H. Wang, J. Gong, Y. Zhuang, H. Shen, and J. Lach, "Healthedge: Task scheduling for edge computing with health emergency and human behavior consideration in smart homes," in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017, pp. 1213–1222.

[8] K.-H. Yeh, "A secure iot-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10 288–10 299, 2016.

[9] X. T. Kong, H. Luo, G. Q. Huang, and X. Yang, "Industrial wearable system: the human-centric empowering technology in industry 4.0," *Journal of Intelligent Manufacturing*, pp. 1–17, 2018.

[10] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[11] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, 2020.

[12] T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, "AGE: authentication in gadget-free healthcare environments," *Information Technology and Management*, pp. 1–20, 2019.

[13] S. Binu, M. Misbahuddin, and J. Paulose, "A Signature-Based Mutual Authentication Protocol for Remote Health Monitoring," *SN Computer Science*, vol. 1, no. 1, p. 8, 2020.

[14] M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks," *Security and Communication Networks*, vol. 2019, 2019.

[15] S. Sengupta, "A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System," in *Emerging Technology in Modelling and Graphics*. Springer, 2020, pp. 501–518.

[16] N. Jalloul, F. Porée, G. Viardot, P. L'Hostis, and G. Carrault, "Activity Recognition Using Complex Network Analysis," *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 989–1000, 2018.

[17] K. Altun, B. Barshan, and O. TunÃ§el, "Comparative study on classifying human activities with miniature inertial and magnetic sensors," *Pattern Recognition*, vol. 43, no. 10, pp. 3605 – 3620, 2010.

[18] F. Attal, S. Mohammed, M. Dedabrishvili, F. Chamroukhi, L. Oukhellou, and Y. Amirat, "Physical human activity recognition using wearable sensors," *Sensors*, vol. 15, no. 12, pp. 31 314–31 338, 2015.

[19] A. Subasi, M. Radhwan, R. Kurdi, and K. Khateeb, "IoT based mobile healthcare system for human activity recognition," in *2018 15th Learning and Technology Conference (L&T)*. IEEE, 2018, pp. 29–34.

[20] A. Mannini, S. Intille, M. Rosenberger, A. Sabatini, and W. Haskell, "Activity recognition using a single accelerometer placed at the wrist or ankle," *Medicine and science in sports and exercise*, vol. 45, no. 11, pp. 2193–2203, 2013.

[21] J. Yin, Q. Yang, and J. J. Pan, "Sensor-Based Abnormal Human-Activity Detection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, pp. 1082–1090, Aug 2008.

[22] L. Bao and S. S. Intille, "Activity recognition from user-annotated acceleration data," in *International conference on pervasive computing*. Springer, 2004, pp. 1–17.

[23] U. Maurer, A. Smailagic, D. P. Siewiorek, and M. Deisher, "Activity recognition and monitoring using multiple sensors on different body positions," in *International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06)*, April 2006, pp. 1–4.

[24] L. Wang, T. Gu, X. Tao, and J. Lu, "A hierarchical approach to real-time activity recognition in body sensor networks," *Pervasive and Mobile Computing*, vol. 8, no. 1, pp. 115–130, 2012.

[25] J. Pärkkä, M. Ermes, P. Korpipaa, J. Mantyjarvi, J. Peltola, and I. Korhonen, "Activity classification using realistic data from wearable sensors," *IEEE Transactions on information technology in biomedicine*, vol. 10, no. 1, pp. 119–128, 2006.

[26] M. Ermes, J. Pärkkä, J. Mäntyjärvi, and I. Korhonen, "Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions," *IEEE transactions on information technology in biomedicine*, vol. 12, no. 1, pp. 20–26, 2008.

[27] M. Zhang and A. A. Sawchuk, "Human daily activity recognition with sparse representation using wearable sensors," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 3, pp. 553–560, May 2013.

[28] D. Tao, Y. Wen, and R. Hong, "Multicolumn Bidirectional Long Short-Term Memory for Mobile Devices-Based Human Activity Recognition," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1124–1134, Dec 2016.

[29] Y. Guo, D. Tao, W. Liu, and J. Cheng, "Multiview Cauchy Estimator Feature Embedding for Depth and Inertial Sensor-Based Human Action Recognition," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 4, pp. 617–627, April 2017.

[30] M. L. Shuwandy, B. Zaidan, A. Zaidan, and A. Albahri, "Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review," *Journal of medical systems*, vol. 43, no. 2, p. 33, 2019.

[31] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[32] P. Gope, J. Lee, and T. Q. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[33] S. Guilley and R. Pacalet, "SoCs security: a war against side-channels," in *Annals of Telecommunications*, vol. 59, no. 7-8. Springer, 2004, pp. 998–1009.

[34] M. S. Kirkpatrick, S. Kerr, and E. Bertino, "System on chip and method for cryptography using a physically unclonable function," Jun. 10 2014, uS Patent 8,750,502.

[35] P. Rogaway, M. Bellare, and J. Black, "OCB: A block-cipher mode of operation for efficient authenticated encryption," *ACM Transactions on Information and System Security (TISSEC)*, vol. 6, no. 3, pp. 365–403, 2003.

[36] S. Lyu and H. Farid, "Steganalysis using color wavelet statistics and one-class support vector machines," in *Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306. International Society for Optics and Photonics, 2004, pp. 35–46.

[37] H. A. Simon, "Spurious correlation: A causal interpretation," *Journal of the American statistical Association*, vol. 49, no. 267, pp. 467–479, 1954.

[38] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "Avispa: automated validation of internet security protocols and applications," *ERCIM News*, vol. 64, no. January, 2006.

Prosanta Gope (M'18) is currently working as an Assistant Professor (Lecturer) in the Department of Computer Science (Cyber Security) at the University of Sheffield, UK. Dr. Gope served as a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight authentication, authenticated encryption, access control, security of mobile communications, healthcare, Internet of Things, Cloud, RFIDs, WSNs, Smart-Grid and IoT Hardware. He has authored more than 70 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the Distinguished Ph.D. Scholar Award 2014 by National Cheng Kung University (Taiwan). He currently serves as an Associate Editor of the IEEE Internet of Things Journal, IEEE Sensors Journal, the Security and Communication Networks, and the Mobile Information Systems Journal.

Youcef Gheraibia received the Ph.D. degree in computer engineering from the University of Annaba, Algeria, in 2016. He is currently a Research Associate in the Assuring Autonomy International Programme, University of York. His research interests include optimisation, machine learning, probabilistic risk and safety analysis, and autonomous system safety. He has published over 20 papers on these and related topics. In 2016, he received the National Innovation Award from the Algerian Government.

Sohag Kabir received the Ph.D. degree in computer science and the M.Sc. degree in embedded systems from the University of Hull, UK, in 2016 and 2012, respectively. He is currently working as an Assistant Professor in the Department of Computer Science at University of Bradford, UK. Prior to that, he was a research associate in the Dependable Intelligent Systems (DEIS) Research Group at the University of Hull. He has worked in EU projects on safety, including MAENAD and DEIS. His research interests include model-based safety assessment, probabilistic risk and safety analysis, fault tolerant computing, and stochastic modelling and analysis.

Biplab Sikdar (S'98-M'02-SM'09) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include computer networks, and security for IoT and cyber physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing