Hindawi
Security and Communication Networks
Volume 2023, Article ID 9781321, 1 page
https://doi.org/10.1155/2023/9781321

Retraction

Retracted: SWOT: A Hybrid Hardware-Based Approach for Robust Fault-Tolerant Framework in a Smart Day Care

Security and Communication Networks

Received 11 July 2023; Accepted 11 July 2023; Published 12 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Sharma, K. Gupta, D. Gupta, S. Juneja, H. Turabieh, and S. Sharma, "SWOT: A Hybrid Hardware-Based Approach for Robust Fault-Tolerant Framework in a Smart Day Care," *Security and Communication Networks*, vol. 2022, Article ID 2939469, 16 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2939469, 16 pages
https://doi.org/10.1155/2022/2939469

Research Article

SWOT: A Hybrid Hardware-Based Approach for Robust Fault-Tolerant Framework in a Smart Day Care

Sheetal Sharma,[1] **Kamali Gupta**,[2] **Deepali Gupta**,[2] **Sapna Juneja**,[3] **Hamza Turabieh**,[4] **and Subhash Sharma**[5]

[1]*Goswami Ganesh Dutta Sanatan Dharma College, Sector 32, Chandigarh, India*
[2]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India*
[3]*KIET Group of Institutions, Delhi NCR, Ghaziabad, India*
[4]*Department of Information Technology, College of Computing and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[5]*NSN Branch Operations OY (FIKE), Nairobi, Kenya*

Correspondence should be addressed to Subhash Sharma; subhash.1.sharma@nokia.com

Received 21 February 2022; Revised 19 April 2022; Accepted 25 April 2022; Published 27 May 2022

Academic Editor: Bharat Bhushan

Internet of Things (IoT) has made its imprint on every part of the globe today. Offices, households, factories, industries, agriculture, and day cares, among other places, have all upgraded to their innovative version. It has propounded great potential in various real-world applications. The topical trends in the adoption of IoT have also highlighted the challenges associated with the performance of IoT devices. IoT devices require continuous monitoring for any performance degradation. A bibliometric analysis of 587 papers is undertaken on the Scopus database to spot the increasing interest of researchers in fault detection in IoT. A smart system's or an IoT-based space's usability, efficiency, and performance are all built on a fault-tolerant approach and interruption-free smooth operations. The investigation was carried out based on the literature to determine the need for a pro-fault detection system in an IoT-enabled day care. Kids' security and safety are highly dependent on the hassle-free working of smart devices. It's overhead to carry out device tracking manually along with demanding kids. This issue needs to be addressed to uphold the smart day care's trustworthiness. A pro-fault detection approach can be applied to resolve the aforementioned issue to enhance the smart day care's performance and efficiency. This paper proposes SWOT, a novel hybrid hardware-based approach in an IoT-based day care to safeguard the proper working of all IoT devices deployed. It screens every single appliance associated with a smart day care to detect the faulty appliance beforehand. The solution will assist the day care staff in providing the best care and security to their kids without any overhead. SWOT evaluation proved that it is an economical and efficient approach in detecting faults, accurately, swiftly, and with a low false alarm ratio.

1. Introduction

Internet of Things (IoT), specifically IoT, has grown in popularity as a new sensing paradigm for interacting with the physical environment. It is clear that in the not-too-distant future, hundreds of millions of people and businesses with billions of dollars will have smart sensors and advanced communication technology, which will push current systems to their limits. This has already led to a shift in the way we live [1–3]. Smart spaces rely on sensors for their smartness. Thus, sensors are an inseparable component of a smart setup [4]. They sense the data from environments and feed them for analytical processing [5]. Sensors can be heterogeneous and are deployed in relentless conditions making them prone to failures and inducing faults in devices. If any device goes faulty for a longer time, it can lead to great perdition which can challenge the smart space's credibility [6]. Smart day care is an example of such a space that employs smart devices like room temperature and humidity sensors, air-quality sensors, body temperature

sensors, fire and door sensors, etc. Its smartness and pro features are completely credited to the proper working of such sensors deployed in day care. Parents opting for smart day cares actually vouch for the unswerving and dependable services offered by smart day cares. These services are grounded on sensors' smartness. Faulty or erroneous readings can push the system's performance and reliability into a compromising state. For instance, if the fire sensor goes out of order, it will not detect fire in the day care and will not activate the fire alarm or automated firefighting system. Or say, if the door sensor is not responding, it will not report the forced entry into the day care, posing a direct threat to kids' security inside the day care. So, real-time monitoring of sensors' health is a must. Manual checkups of sensor faults can induce unwanted delays and thus can be hazardous. A pro-fault detection system, which can automatically detect the faulty sensor well in time and ensure halt-free functioning of smart day care, is the need of the hour. Automated fault detection is gaining key attention in the research domain also. In the field of smart day care, a large portion of the research done drives just to foster smart gadgets or frameworks for well-being observing, security, and movement following of kids. Running against the norm, no consideration regarding the smooth working of IoT gadgets and sensors is given, which are similarly significant for the problem-free working of brilliant day care. The key objective of this paper is to propose a pro-fault detection approach based on a hybrid hardware-based model to routinely monitor the smart device's health in real time and report faults detected to the technician concerned automatically. In this approach, readings are captured from sensors and based on various factors that can affect sensors' readings, unhealthy devices are identified. The paper is organized as mentioned below.

The paper initially signifies the role and need of fault detection in smart spaces. This is followed by an analysis of the Scopus database with the help of the biblioshiny tool of Rstudio to sum up the academic work done on fault detection in IoT over the last decade in Section 2. Proceeding further, Section 3 states the research gaps in smart day cares and the significance of a pro-fault detection system in place. In Section 4, categories of existing fault detection models are surveyed. Moreover, observed gaps in other hardware-based work from the proposed approach are tabulated. Section 5 proposes a novel approach and algorithm SWOT for pro-fault detection in smart day care. Results and discussion on SWOT evaluation are done in Section 6. Conclusion and future research directions are discussed in Section 7.

2. Fault Detection in IoT

Fault detection is one of the important facets to be considered as it helps in determining the system's proneness to failure and ensures the smooth working of smart devices in IoT-enabled environments. The rectification of faults well in time enhances the quality, reduces the cost, and improves the effectiveness of the whole system.

The adoption of IoT technology has provided comfort, flexibility, and security and has improved the quality of life. It can be inferred that a complete IoT-based solution can be implemented in different areas viz a viz homes, offices, day cares, industries and manufacturing, etc. An expressive and productive smart workplace enhances the comfort of its employees. They are also inspired to share their excellent achievements at work. In IoT environments, there is a need to develop a model that can assist in the resolution of real-world problems that users confront regularly. The problem was the need to keep track of faulty appliances in a smart space. Many organizations still keep this track manually and it becomes difficult to search every corner to see if there is any faulty appliance along with demanding work. There can be plenty of different appliances present in space. Humans tend to make mistakes and may forget to report and repair faulty appliances well in time. Consider an example of a health monitoring system for elderly care, where the elder's complete health is taken care of by smart devices. If a sensor measuring the oxygen level goes faulty, it will either stop reporting or will report the wrong oxygen level and could be fatal, before it could be detected by any human. So, a reduction can be made in human-based errors by reducing human intervention. It is the need of the hour to build a user-friendly, scalable, reliable, and flexible environment. The increasing demand and speed of IoT-enabled technologies have also made it more difficult to detect and recover faults quickly [7]. Fault-tolerant and reliable IoT solutions improve the customer experience. Fault identification and rectification promptly are critical for quality control, as well as lowering maintenance costs and time.

Smart space to be fault-tolerant is the need of the hour that has attracted many authors to put efforts in this direction. This is quite evident from a quantitative analysis called bibliometrics analysis that was conducted utilizing parameters from academic literature such as authors, keywords, sources, and affiliations. Moreover, a total of 587 publications were shortlisted with the keywords "Fault Detection" with an "AND" operator with "Internet of Things" with and "OR" operator with "IoT" for the period from 2011 to 2021.

As indicated in Figure 1, 318 conference papers, 198 articles, 14 book chapters, 49 conference reviews, and 5 review articles from various sources with 3 others were referenced.

As learned from Figures 2(a) and 2(b), fault detection or fault diagnosis and Internet of things or IoT is the most relevant and trending keyword referenced by authors.

28.9% of total work published on fault detection and Internet of Things is in the year 2020; whereas, 22.31% was published in the year 2019 as represented by Figure 3.

From the above analysis, it can be determined how fault detection in IoT has gained pace over the last decade with extensive work done in the years 2019 and 2020.

Some of the recent work done in this direction is stated below:

Wanget al. [8] provided a solution for IoT-based process fault diagnostic and prediction concerns and prediction concerns. The solution analyzes data received by sensors and discovers a coincidental association between physical devices. After that, a real-time health index of the devices is

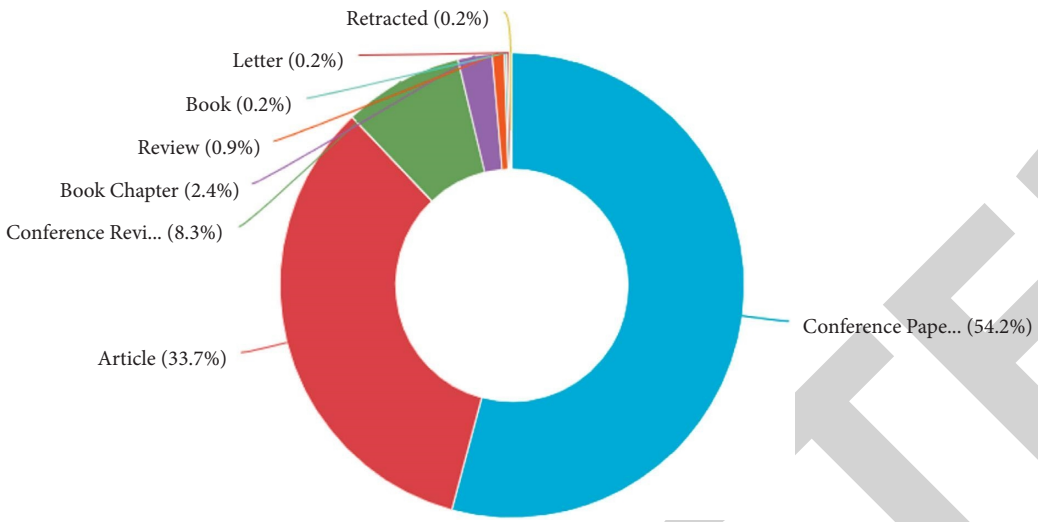


Figure 1: Documents classified by types.

tracked to detect defects. Furthermore, for strongly connected devices, defect prediction can be done based on the casual relationship. Then, to prevent future mistakes, actions can be suggested. Testing on a real-world application confirmed the practicality of the proposed method.

In addition to the previous, Mundada et al. [9] used a back-propagation learning algorithm and a software defect prediction technique based on an artificial neural network. Artificial neural networks are used to locate and anticipate the erroneous module. In comparison to the algorithm of traditional back-propagation, the results showed that artificial neural networks trained using robust back-propagation produce noticeable results.

DICE is a system developed by Choi et al. [10]. The system comprises two phases: the pre-phase extracts context information based on sensor correlation and the post-phase extracts context information based on sensor correlation. The real-time data are compared to the extracted data in the next real-time phase. The departure of faulty sensors from precomputed context is used to identify them. DICE successfully identifies problematic devices with 94.9 percent precision and 92.5 percent recall, according to the findings. The technology also claims to detect defects in an average of 3 minutes and to identify problematic devices in an average of 28 minutes.

Chakraborty et al. [11] suggested a fall-curve primitive-based system for sensor identification and defect detection in IoT devices. The candidate system proved that fall-curve properties such as manufacture, uniqueness, and platform independence can accurately identify and detect sensors.

A sensor failure prediction model was developed by Vibhute et al. [12]. The model gathers sensor data, and by inferring methods, predicts failure. The program finds the elements that may contribute to sensor failure and so creates a predictive model to depict system behavior. For all nonlinear systems, the proposed approach can anticipate sensor failure with 99 percent accuracy.

Gaddam et al. [13] talked about numerous outliers and anomaly detection approaches in sensors in their study. The importance of having proper protocols and approaches for tackling several specific limits and challenges of IoT is emphasized in the essay. The paper provides a clear and accessible summary of outlier detection approaches, as well as their benefits and drawbacks. They also demonstrated a multiagent deep reinforcement outlier identification strategy based on learning.

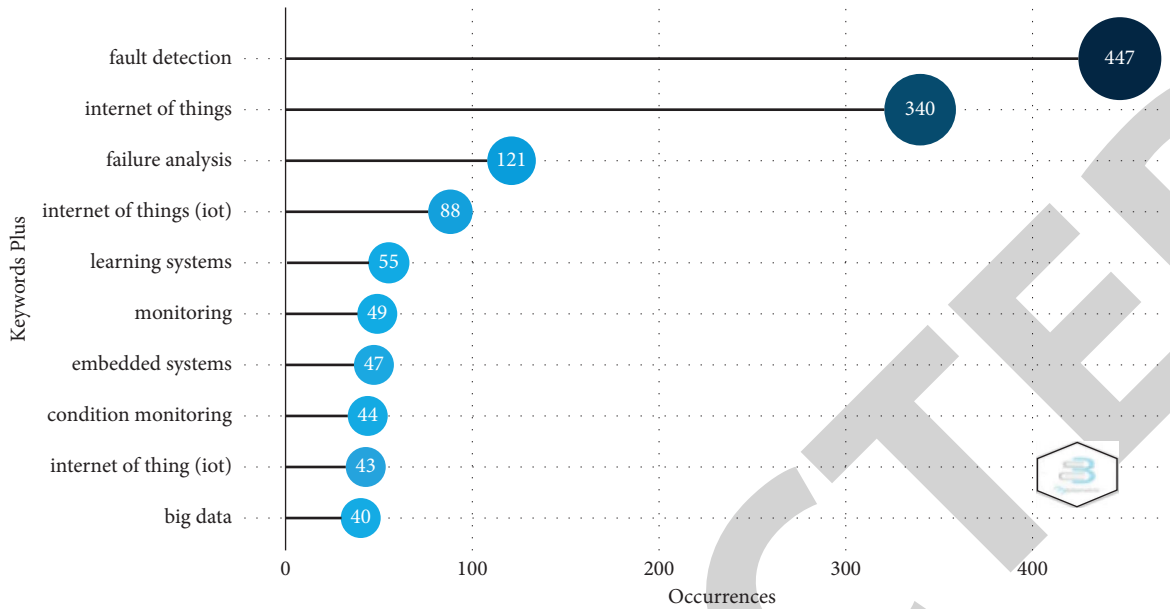
Arun et al. [14] presented an IoT-based smart office setup. The system employs various sensors like temperature, door locks, humidity sensors, automatic light control systems, and smoke detection sensors. These sensors collect real-time data from the atmosphere. Sensors are connected to the ESP32 microcontroller. The system ensures the smooth functioning of offices. The system operates in both automatic and manual modes.

The section below discusses how vital it is for a smart day care to have a pro-fault detection system in place.

3. Importance of Fault Detection in Smart Day Care

The adoption of IoT technology has provided comfort, flexibility, and security and has improved the quality of life. IoT-based applications operate on real-time information with no occurrence of failures in their operation [15]. The presence of IoT technology assists the implementation and smooth functioning of smart day cares [16, 17]. It can be concluded from the analysis done above, fault detection is the key to having an efficient, robust, fault-tolerant, and smooth operating smart space that has earned keen interest from researchers as well.

A child's health and security in day care can be monitored using IoT technology. Various sensors are employed to keep a check on the temperature, motion, and humidity settings required for infants. Working parents can be remotely updated with the status of their child every hour. An expressive and productive smart day care strengthens parents' trust and comfortability [18, 19].



(a)

(b)

Figure 2: (a) Most relevant words. (b) Most trending words.

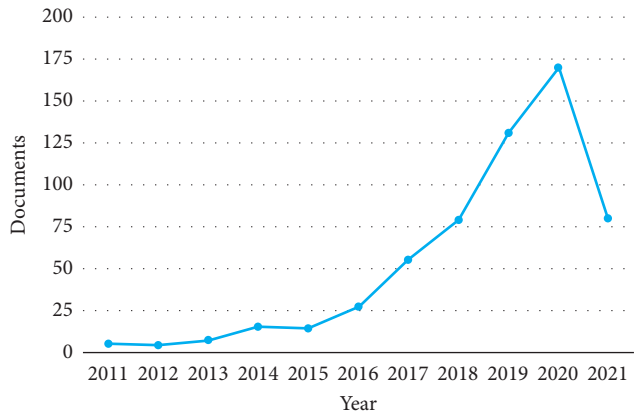


Figure 3: No. of documents year-wise.

The significance of fault detection in a smart day care can be understood by underlying points.

(i) With kids around, it requires day care employees to work in synergy to take complete care of their safety, health, and tracking. Moreover, to provide dedicated attention to the children in a day care, the caretakers must be carefree from other hassles that can divert their focus from kids.

(ii) The problem was the need to keep a track of faulty appliances in a smart day care. Many day cares still keep this track manually and it becomes difficult to search every corner of the day care to see if there is any faulty appliance along with demanding kids. Also, there can be plenty of different appliances present in the day care [20].

(iii) Undersized research is done in the area of smart day care. Moreover, most of the research done leads only to develop smart devices or systems for health monitoring, safety, and motion tracking of infants in day care. On the contrary, no attention to the smooth functioning of IoT devices and other appliances is given, which are equally important for the hassle-free functioning of a smart day care [16–18, 20–23].

(iv) In a day care system, safety and security are critical concerns. Smooth functioning and fault tolerating robust system is the base of a smart day care. Different sensors are responsible for monitoring a child's health and safety parameters. Improper working of these sensors can end up as a loophole in a child's safety. For example, if the motion sensor goes faulty, it will not capture, if any child is entering a danger zone or defective temperature sensors will not notify caretakers well in time when the infant's body temperature rises.

(v) The variety of gadgets and advancements utilized builds the IoT framework's weakness to security dangers. Efforts should be taken to ensure hassle-free operations of all devices.

(vi) Humans tend to make mistakes and may forget to report and repair faulty appliances well in time. Moreover, manual detection of faults can lead to delays in rectification and lead to fault severity. It implies that a severe fault can turn out to be fatal and cause momentous loss. It should be considered beforehand and averted from being great perdition [5].

(vii) Indeed, even numerous clients expect to change to IoT applications however attributable to inadequate information or absence of time to deal with different IoT applications or gadgets accessible, they face impediments to simple reception of IoT [24, 25].

To address the abovementioned issues, a fault detection approach is needed. For which, existing fault diagnosis models were studied and a summary is presented in the next section.

4. Classification Fault Diagnosis Methods

Many faults diagnosis models are available as shown in Table 1 [13, 25–29]. Model-based, hardware-based, or history -based techniques can be employed for fault detection that can generate efficiency as well as save time. Though different techniques can be differentiated based on different parameters such as assumptions, statistical model strengths, weaknesses, and accuracy.

In prevailing times, systems that are robust and fault-tolerant are gaining importance due to the halt-free services they offer. Faults if delayed or not resolved for long can lead to fatal and costly outcomes. IoT's enticing promises are accompanied by obstacles and constraints that must be considered and addressed. IoT solutions that are secure, strong, efficient, and inexpensive are essential for a smart world that is ready for the future.

After analyzing existing models, this research proposes a fault detection methodology based on a hybrid hardware-based model. Table 2 presents existing work done based on the same methodology and observed gaps from the proposed methodology. Following are common observations:

(i) Hardware-based techniques are not much explored and worked on.

(ii) Hardware redundancy is a traditional approach for detecting faults; it involves extra cost, space, weight, and maintenance for redundant devices.

(iii) Detection of valid and invalid measurements relies on approximation or redundant data which may be temporarily affected and not reliable.

(iv) Fault detection is based only on limits calculated by different methods. Drift and device condition is not taken care of while calculating the threshold limits.

(v) Timely current fluctuations/spikes were not considered.

(vi) The indicator considered only the current levels of the device.

(vii) Other factors affecting the current consumption of the device were not considered like device aging, frequency of repairs.

(viii) Unplugged sensors were not anticipated or handled.

In the following section, the proposed approach is explained with help of the experimental setup and workflow it adheres to, supported by a flowchart and its algorithm to provide real-time monitoring of devices in a smart day care.

5. Proposed Approach

This section characterizes a new approach for managing a smart environment like a day care with a hybrid hardware-based model. The day care environment precisely affects the working efficiency of the staff taking care of kids. So, a stress-free and relaxing environment is essential in the day care [37, 38]. A smart day care guarantees the finest and

Table 1: Classification of fault diagnosis methods [13, 25–29].

Fault Diagnosis	Model-based	Qualitative	Abstraction hierarchy
			Fault trees
			Digraphs
			Fuzzy
		Quantitative	Analytical redundancy
			Parity space
			Kalman filter
			Parameter estimation
			Diagnostic observers
	Hardware-based	Hardware redundancy	
		Voting techniques	
		Special	
		Limit checking	
		Frequency analysis	
	History-based	Artificial intelligence	Fuzzy logic neural network
		Clustering	K-means
		Classification	Support machine vectors Bayesian network KNN
		Statistical methods	Parametric
			Nonparametric
		Expert systems	Knowledge-Based
			Rule-based
		Pattern recognition	

Table 2: Comparison with existing work on hardware-based approaches of fault detection [30–36].

Title	Summary	Observed gaps
Fault detection with limit checking [30]	The paper discusses fault detection methods using limit checking as follows 1. Limit checking of absolute values 2. Using trend checking using the first derivative of readings 3. A combination of absolute values and trends can be applied as limits 4. Detection with binary thresholds with an estimation of mean and variance	1. Fault detection is based only on limits calculated by different methods were discussed 2. Device aging/drift is not taken care of while calculating the threshold limits 3. Timely current fluctuations/spikes are not considered 4. Missing data are not considered
An automatic sensor fault detection and correction algorithm [31]	This article attempts to detect a faulty reading among a set of measurements and proposes a correction scheme. It involves two levels: the detection of a problem and its localization afterward	1. The outmoded approach of hardware redundancy for measurement is used. It involves extra cost, space, weight, and maintenance for redundant devices 2. Detection of reliable and poor measurements relies on approximation or redundant data which may be temporarily affected
(12) United States patent (54) METHOD OF DETECTING FAULTS USING 373 A Sty [32]	An indicator for a faulted circuit was designed that reports a fault current reading for the monitored circuit crosses one of the levels of threshold limits even after some propagation delay	1. The indicator considered only the current levels of the device 2. Other factors affecting the current consumption of the device were not considered like device aging, frequency of repairs, unplugging of the device 3. IoT or smart devices/sensors are not considered
The study of hardware redundancy techniques to provide a fault-tolerant system. [33]	The paper studies different hardware redundancy techniques	The traditional approach for detecting faults. It involves extra cost, space, weight, and maintenance for redundant devices
An adaptive threshold algorithm for sensor fault based on the grey theory [34]	An adaptive dynamic threshold adjustment algorithm based on the grey theory. In this method, the threshold value can be dynamically adjusted according to the real-time mean and variance of the residual	Factors affecting the current consumption of the device were not considered like drift, spikes, frequency of repairs, unplugging of the device not considered

Table 2: Continued.

Title	Summary	Observed gaps
Hitchhiker's guide to successful remote sensing deployments in Mongolia [35]	The author builds an economic air quality sensor that gathers real-time data from varied locations. The paper presents the implementation and challenges faced in the deployment of the same	Unplugged sensors were not anticipated and considered in their design
Fault detection using limit checking: a brief introductory review [36]	This includes fault detection using limit checking of absolute values, trend checking, fixed and adaptive thresholds, and change detection	Other factors affecting the current consumption of the device were not considered like device aging, frequency of repairs, and unplugging of the device

most active exploitation of physical infrastructure and IT resources [39, 40]. Kids demand complete attention and care. There must be a hassle-free involvement of the day care staff while taking care of kids. In such a scenario, to keep track of faults and maintenance of all appliances or IoT devices in day care is added overhead. So, the health of smart devices in smart day care is as important as other vitals, which can be ensured by pro-fault detection [41, 42].

The proposed approach is aimed to enhance the efficiency and fault tolerance in the smart day care [43]. It binds all the IoT devices/sensors configured in the day care to a common programmed smart system [44].

This paper proposes a hybrid hardware-based approach that combines

(i) Special hardware: Special hardware like the current sensor is attached to all current-based devices to capture the current consumed by those devices. Based on which health of the current device can be investigated.

(ii) Limit Checking: The reading **Y** of the device/sensor is validated for fault detection while considering the following checks:

(i) Stuck at zero vlue
$Y = 0$

(ii) Absolute limit checking with 2 level thresholds
$Y < T\_\text{min}$ OR $Y > T\_\text{max}$
Where T_min and T_max are the healthy range for the device/sensor readings.
$Y < T\_\text{extd\_min}$ OR $Y > T\_\text{extd\_max}$
Where $T\_\text{extnd\_min}$ and $T\_\text{extnd\_max}$ are the higher levels of the threshold for devices that becomes valid as the device/sensor ages or the number of repairs increases.

(iii) Trend checking
$Y_d = \mathbf{Y} - \mathbf{Y_p}$
Where Y_P is the reading of the device/sensor in the previous iteration. So, the rate of change in measure value can also be analyzed.

(iii) Frequency analysis: Some frequency patterns of devices, even if they operate under normal conditions can be diagnosed as abnormal. Patterns considered are as follows:

(i) Device aging

(ii) Frequency of repairs

(iii) Abnormal power consumption pattern

5.1. Experimental Setup. The proposed approach involves live monitoring of various electrical appliances and IoT devices via sensors deployed in a smart day care. All these devices are centrally connected to an Arduino Mega 2560 Rev.3 microcontroller board as depicted in the smart day care prototype in Figure 4. This prototype is used to generate simulated datasets for smart day care. Listed below are different sensors and hardware components deployed for the proposed approach in a smart day care prototype.

(a) Temperature and humidity sensor: To monitor the appropriate temperature and humidity levels in smart day care, a DHT11 sensor is used. It combines a capacitive sensor element for humidity and a thermistor for sensing temperature. It works out stickiness from 20 to 90% and temperature from 0°C to 50°C with a precision of ±1% and ±1°C, individually. It is a cheap digital sensor that can be easily interfaced with Arduino Mega 2560 Rev microcontroller.

(b) Motion sensors: It is used to detect the motion of the child in the day care. So that, if the child approaches some unsafe object like electric switches, the day care staff get notification may be via a buzzer. An ultrasonic sensor SR04 is used to serve the purpose. They are designed for anticollision detection.

(c) Air quality sensor: Kids are quite sensitive, which makes it more important to keep a check on the air quality inside the day care. The MQ-135 sensor can sense and measure many types of toxic gases like NH3, CO2, alcohol, etc.

(d) Fire sensor: A photodiode is a sensor intended to identify and react to the presence of smoke or flame. This sensor helps to place a firefighting system in day care.

(e) Door-lock sensor: Reed sensors are used to manage automatic door-locks inside a day care for detecting whether there is forced entry or not. They are additionally used to make frameworks carefully designed by putting either magnets or switches in covers so when they are eliminated, it impels the switch setting off the alert.

(f) Current sensor: Measurement of current is essential for the appropriate working of electronic gadgets like

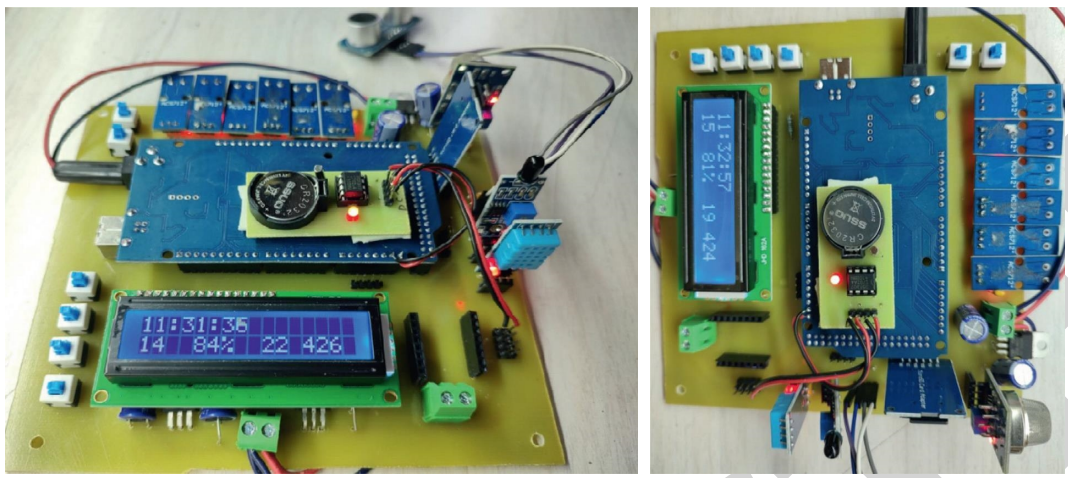


Figure 4: Hardware-based model for the smart day care prototype.

fridge, microwave, lights, fan, CCTV, AC, etc. The ACS712 current sensor is the sensor that can be utilized to quantify and work out the measure of current applied. It works with both analog and digital current. It helps in foreseeing issues in a gadget and forestall harming of hardware.

(g) Body temperature sensor: It is vital to keep checking the body temperature of kids. In case of fever, proper aids can be taken. A wearable device integrated with a thermistor can be utilized to constantly check the fever.

(h) Microcontroller: Arduino Mega 2560 Rev.3 is applied in the setup, which is a low-cost microcontroller based on ATmega2560. It consists of a sufficient number of pins to support many features and most importantly its interface is compatible with all IoT devices/sensors. It has 1 KB of inbuilt SRAM and EEPROM of 512 bytes.

(i) MP3 player: It is used to play some prerecorded sounds like warning messages in case of any danger detected around the kids or buzzers.

(j) LCD Screen: An LCD screen of 16×2 (32 characters) to display the current temperature and humidity or load controlled by programming the microcontroller.

(k) Real-time Clock: It is attached to keep all devices in sync with the current date and time.

In the smart setup presented in this paper, all the devices and sensors deployed inside a smart day care are connected to the microcontroller, which facilitates centralized control over them. The SDRAM inside the microcontroller acts as a data storage for readings of all the devices. Readings samples are collected on a regular slice of time basis with a fixed time window of 30 secs. Figure 5 shows the graph of readings of all the devices in setup concerning time. It shows both faulty and non-faulty readings. Data are assumed not to be cumulated to previous day data, rather each day new data log is maintained till the main power supply is on. Interpretation of readings for all anticipated devices is mentioned in Figure 6.

All the data captured by the microcontroller is processed using an algorithm explained in the next section, for detecting a fault in any device/sensor.

5.2. Proposed Workflow and Algorithm: SWOT. The workflow in Figure 7 demonstrates the complete flow analysis of the proposed approach. Initially, all the electrical appliances and IoT devices/sensors deployed inside the smart day care are turned on by supplying power to them. Next, the data/readings are captured and via the microcontroller's interface are stored in an SD card. A python-based algorithm is then applied to detect faults in the data. Afterward, each device reading is checked for the presence of outliers indicating faults in the device. If an abnormality is detected, the fault is identified and reported to the concerned personnel. Else, if no abnormal readings are detected, the device is considered in a healthy state. The cycle again resumes by capturing new readings. This process continues till the devices are not switched off.

The flowchart in Figure 8 and the algorithm in Figure 9 show the steps performed to detect faults based on the data captured from devices.

The working methodology is explained below:

(i) For each device deployed in smart day care, the default device status is set to healthy.

(ii) Reading for each device is fetched.

(iii) If the reading is zero, then the algorithm will wait for the next two iterations to subside issues like unplugged devices or missing data. Even if after two iterations, the reading remains zero, the device status is set to unhealthy.

(iv) Next, the device reading is checked against the valid threshold $T\_\min$ and $T\_\max$, which is the reading range for a healthy device. The algorithm will again wait for two following iterations to subside the issues like spikes or fluctuations. If still reading is out

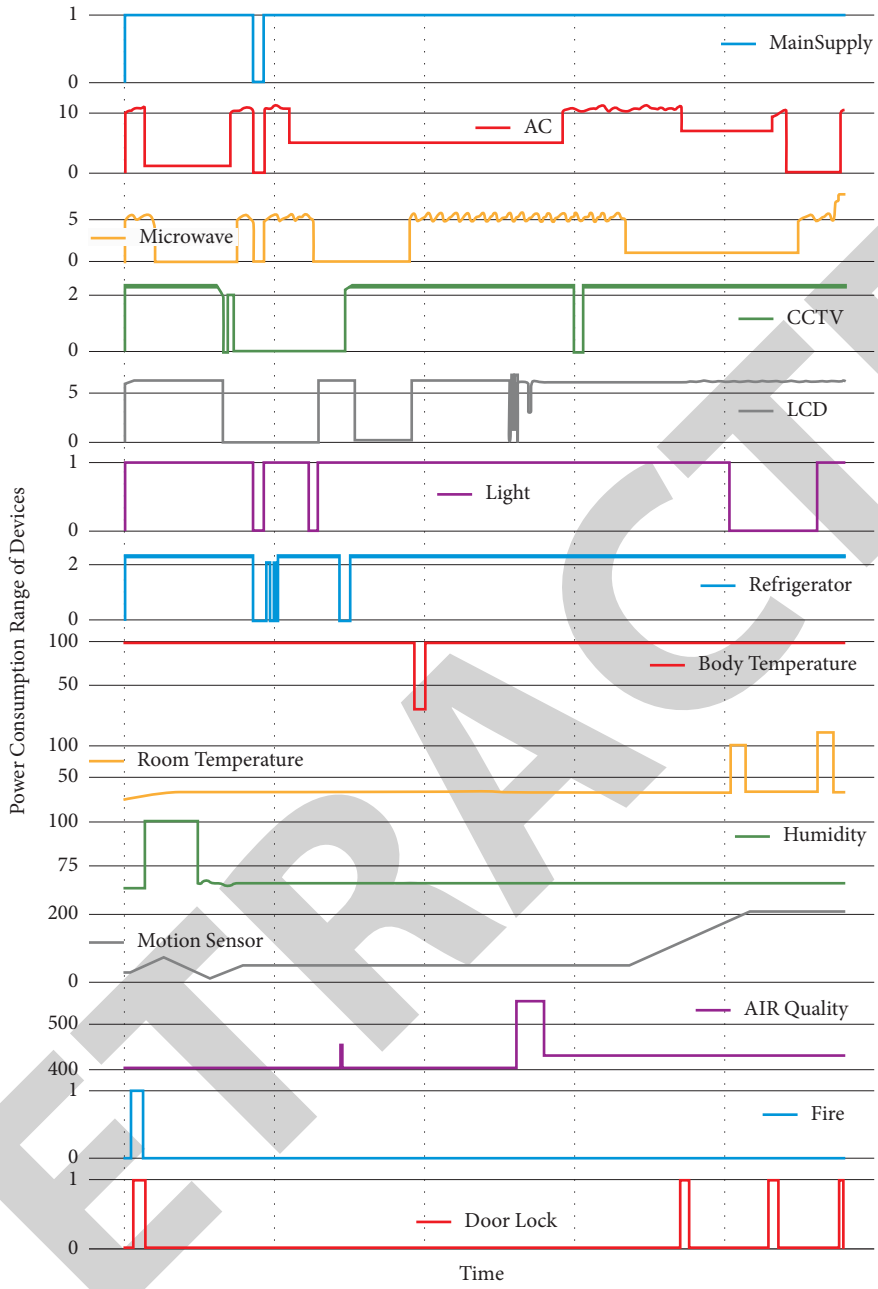


Figure 5: Power consumption of devices in a smart day care.

of the healthy range, then going a step further the reading is compared with the next level of threshold T_extnd_min and T_extnd_max, which is extended ranges calculated based on factors like device aging, drift, or the number of repairs the device has undergone. If device reading is going beyond the extended range also, the device status is set to unhealthy.

(v) Lastly, the reading is checked against any particular pattern, which may be under valid thresholds but the trend cannot be considered as healthy such as spikes and unusual current consumption patterns which may indicate that the device will soon be out of order. It is done by tracking the first derivative of the readings. The algorithm waits for the next four cycles to ensure the trend is not temporary. If the pattern persists the device is considered unhealthy.

The section below discusses the results and performance of the SWOT algorithm.

6. Results and Discussion

It is quite important to evaluate the performance against some metric, as it provides a quantitative indication of objectives achieved. The performance of a fault detection algorithm can be evaluated with the help of a confusion matrix and the possibility of outcomes of the algorithm

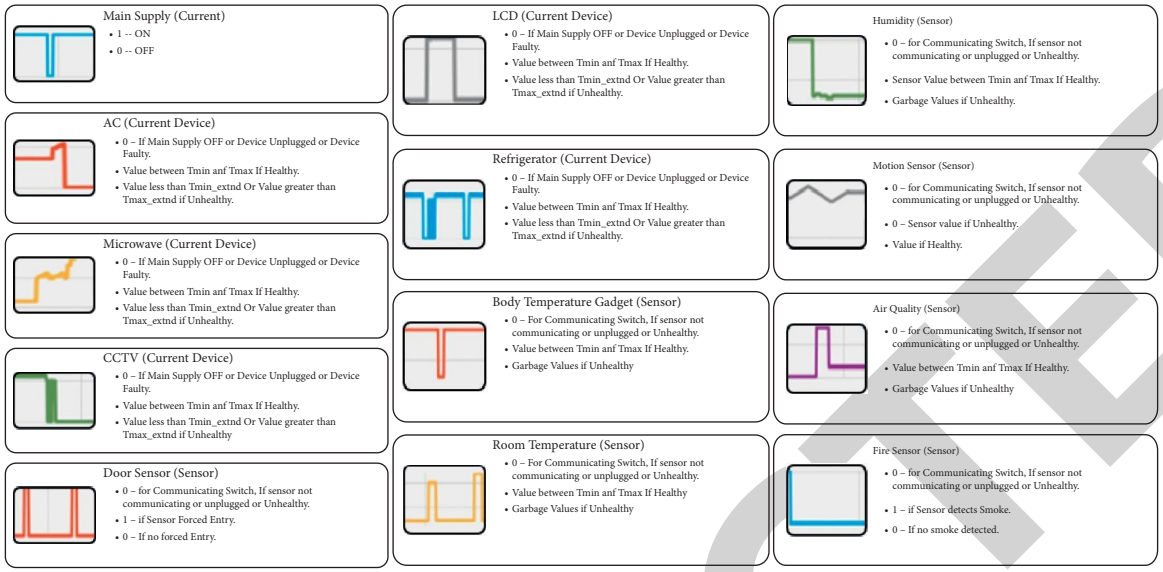


Figure 6: Interpretation of device's readings.

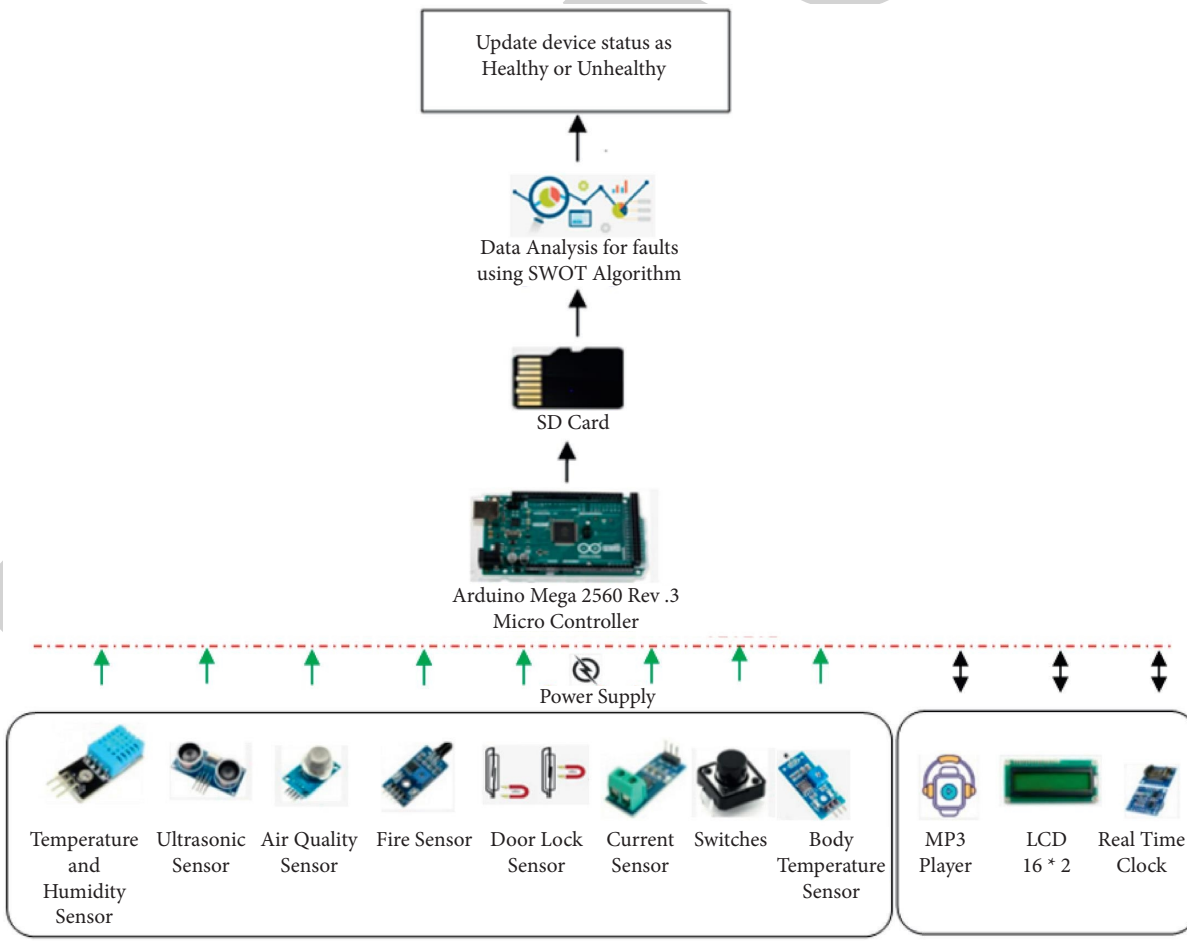


Figure 7: Proposed approach workflow.

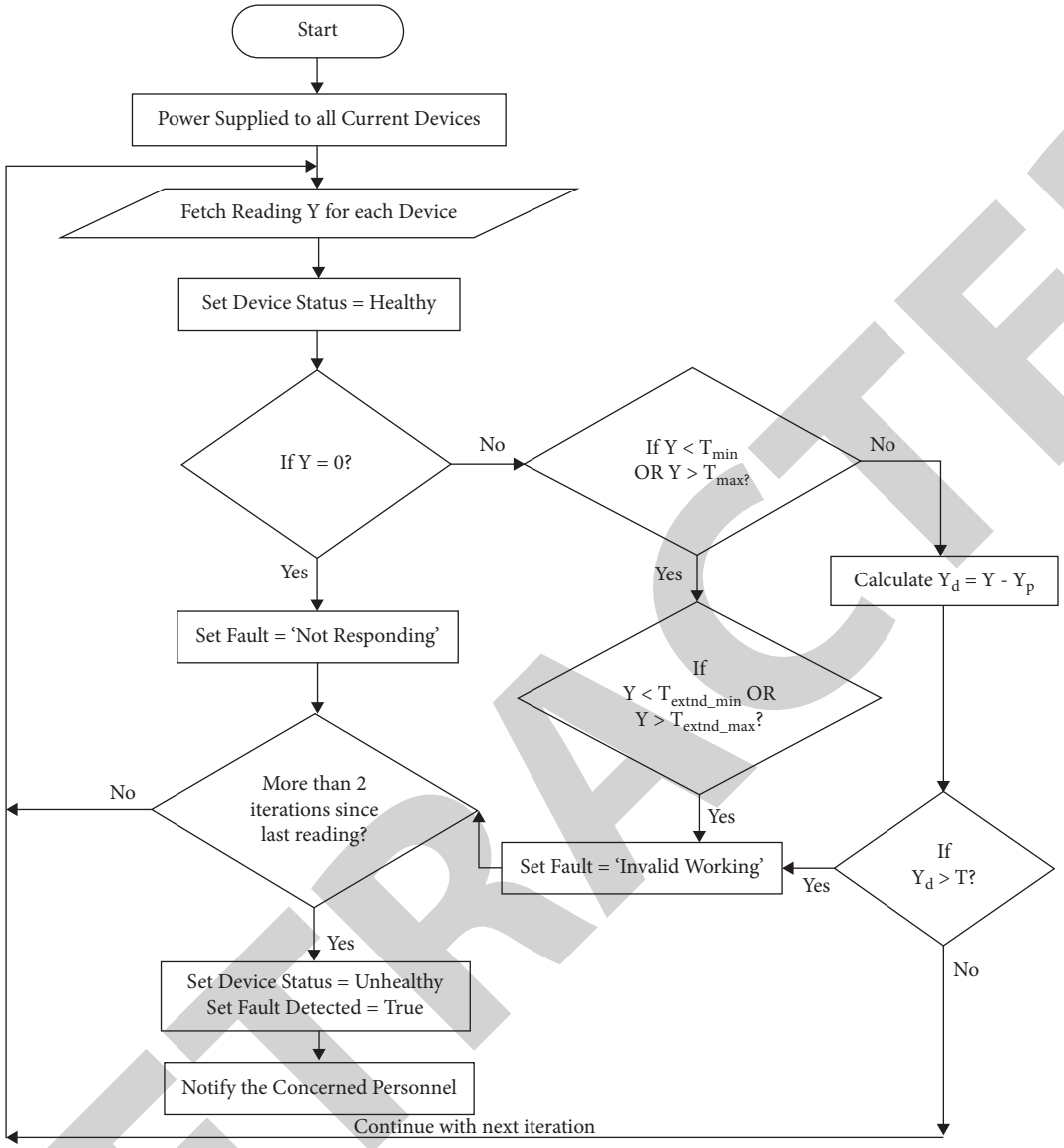


Figure 8: Flowchart for the proposed approach.

[30–32] as shown in Figure 10. Based on ground truth readings, a fault detection can have the following outcomes:

True Positive (TP): When fault exists and the algorithm truly reports a fault.

False Negative (FN): When fault exists but algorithm reports no fault.

False Positive (FP): Better known as a false alarm, when no-fault exists but algorithm reports faults.

True Negative (TN): When no-fault exists and the algorithm reports no faults.

No Detection (ND): Case where algorithm reports nothing.

Based on the abovementioned outcomes, following metrics can be used for evaluation [37, 45–47]:

Precision: It yields the proportion of positive results, formulated as in equation (1).

$$\text{Precision} = \frac{TP}{TP + FP}. \tag{1}$$

Accuracy: It yields the proportion of correct detection, formulated as in equation (2).

$$\text{Accuracy} = \frac{TP + TN}{TP + FN + FP + TN}. \tag{2}$$

True condition positive: It yields the total number of faulty samples, formulated as in equation (3).

$$TCP = TP + FN + ND. \tag{3}$$

True condition negative: It yields the total number of fault-free samples, formulated as in equation (4).

$$TCN = FP + TN + ND. \tag{4}$$

Algorithm: Automated Fault detection in Smart Daycare

Inputs: Live Data of all IoT devices/Sensors in Daycare in every 30 Sec
Output: Fault Detection and Device health status in Smart Daycare
for each Device in Smart daycare
  If main power supply is **ON then**
    Set **Device_Status** = **'Healthy'**
    If **Device_ON** = True then
      Fetch Y = reading of the Device
      If $Y = 0$ then
        Wait for 2 cycles
        Again, Fetch Y =reading for the Device
        If $Y = 0$ then --Stuck at Zero
          Set **Device_Status** = 'Unhealthy'
          Set **Fault_Detected** = 'True'
        End if
      Elseif $Y < T\_min$ OR $Y > T\_max$ then --limit Checking
        Wait for 2 cycles
        Again, Fetch Y = reading of the Device
        If $Y < T\_min$ OR $Y > T\_max$ then
          If $Y < T\_extd\_min$ OR T_extd_max then --Extended Threshold Checking
            Set **Device_Status** = 'Unhealthy'
            Set **Fault_Detected**= 'True'
            Notify the technician concerned
          End if
        End if
      Else
        $Y_d = Y - Y_{p|}$ --Trend Checking
        If $Y_d > T$ then
          Wait for 4 cycles
          If $Y_d > T$ then
            Set **Device_Status** = 'Unhealthy'
            Set **Fault_Detected**= 'True'
            Notify the technician concerned
          End if
        End if
      End if
    End if
End for

Figure 9: SWOT: algorithm for the proposed approach.

		Detected: Positivre	Detected: Negative
Actuals	Positive	True Positive (TP) Actual Faults	False Negative (FN) Missed Faults
	Negative	False Positive (FP) False Faults	True Negative (TN) No Faults

Figure 10: Confusion matrix [37, 45, 46].

False positive rate (false alarm rate): It yields a proportion of fault-free samples that are projected as faults, formulated as in equation (5)

$$PR = \frac{FP}{TCP}. \quad (5)$$

True positive rate: It yields the proportion of faults that are correctly reported, formulated as in equation (6).

$$TNR = \frac{TN}{TCN}. \quad (6)$$

The SWOT evaluation is done on data generated from a hardware simulated prototype of day care. Varied types of faults were inducted into the data. These faults include stuck at Zero, Outliers, Spikes, Drift, Constants, and Hung Device-type of smart device errors. In Figure 11(a), the precision of SWOT in detecting faults, concerning current devices, and sensors is shown. To ration the performance and test the efficiency of the SWOT, algorithms based on only absolute limit checking and limit checking combined with trend checking were also executed on the same test dataset. Figure 11(b) clearly proves the precision of SWOT is 98.72%, which is much higher than both 44% with limit checking and 70% with limit and trend combined.

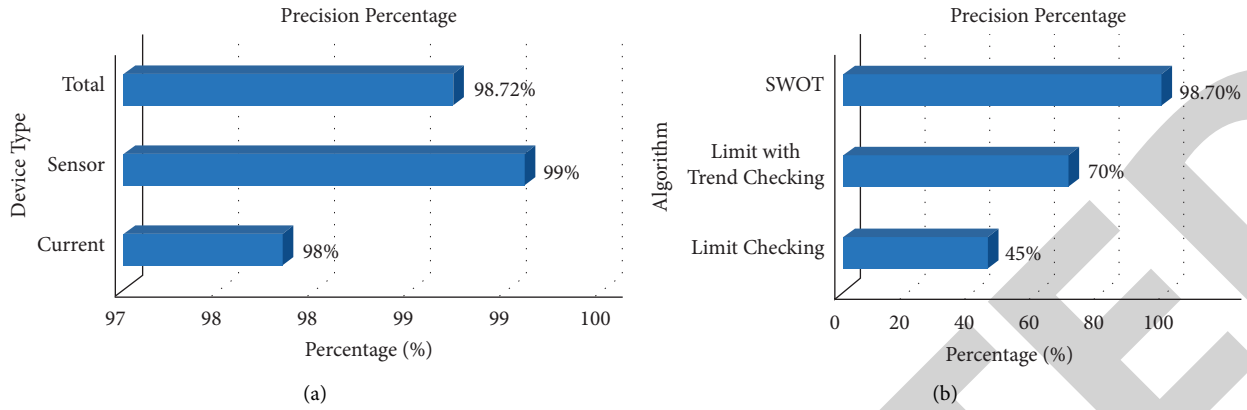


Figure 11: (a) SWOT: precision for current and sensor devices. (b) Comparison of precision percentage.

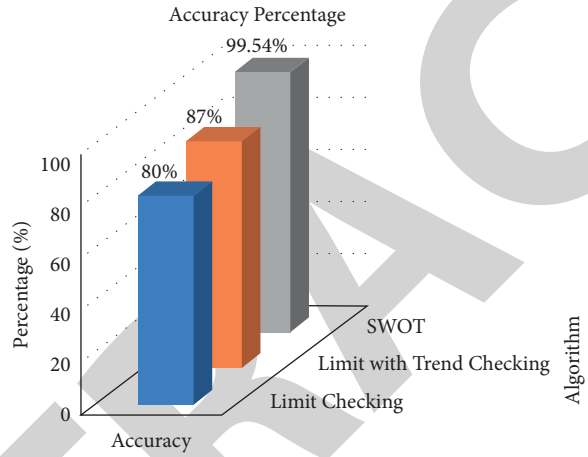


Figure 12: Comparison of accuracy percentage.

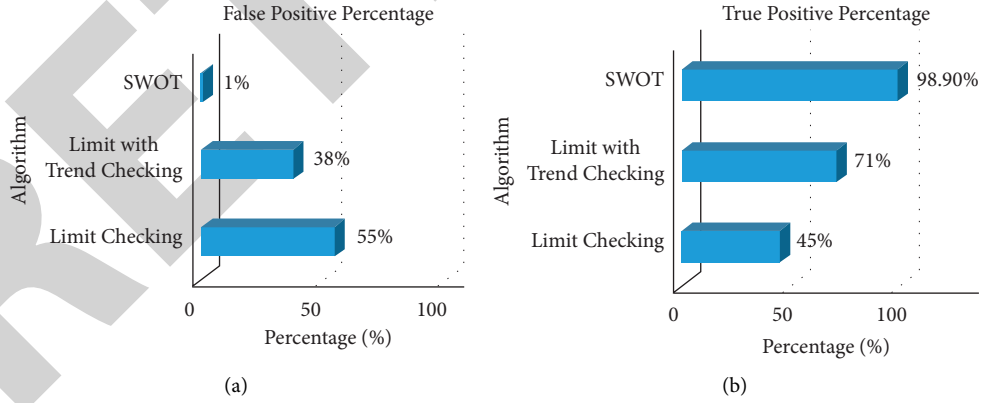


Figure 13: (a) False positive percentage graph. (b) True positive percentage graph.

The accuracy of the three respective algorithms is shown in Figure 12.

Figures 13(a) and 13(b) show that the false alarm rate and true positivity rate for SWOT are the best among the three algorithms. Also, the execution time for SWOT is very less, it processes data captured for 30 hours in just 37 secs. The results summarize that SWOT performs extremely well as compared to other hardware-based techniques for fault detection.

The algorithm has been named SWOT because it analyzes the strengths, weaknesses, opportunities, and threats of the underlying device to detect its health status.

In a busy place like day care, where the attention of the staff is primarily on the kids, a dedicated autonomous system to track the health of smart devices is the state-of-the-art framework. Table 3 discusses the SWOT analysis of the SWOT algorithm.

Table 3: SWOT analysis of algorithm SWOT.

Strength	Weaknesses	Opportunities	Threats
(i) All the devices in day care are monitored in real time and via one common module	(i) Device calibration is not anticipated	(i) SWOT can be easily integrated into other smart space environments as it has a generalized implementation approach	(i) The whole system is dependent on the ADC microcontroller, if that goes faulty, the system cannot perform at all
(ii) Easy to manage heterogeneous devices	(ii) it assumes that the ground device values are not biased	(ii) It can be tailored to accommodate any device or sensor	
(iii) Efficient and economical solution for controlling appliances automatically	(iii) Hung devices or constant are not handled. Readings with a consistent value across time, even if they are within a normal range, are known as constant values		
(iv) A new data log is maintained each day. So, not much storage is needed	(iv) Uncertainty faults that are induced by sudden events or situations or sporadic like fire, floods, chemicals, etc. cannot be tracked		
(v) Low false alarm rate			
(vi) High positivity rate			
(vii) High precision			
(viii) Very less execution run-time			
(ix) Can track outliers, stuck at zero, missing data, drift, noise/Spikes			

7. Conclusion and Future Work

Internet of things has renewed the working of almost every workplace around the world. Not only the way operations were being performed but also the way things were being viewed. The dependency of the performance of smart space on IoT devices has also raised the concern of the system's fault-tolerant approach and robustness. Smart devices or sensors are pillars of smart setup, their malfunction can have fatal outcomes and degrading effects on the overall performance. To ensure hassle-free and smooth functioning, detection of faults and failures in the smart system well in time is a key requisite. Also, according to the study performed on the Scopus database, a lot of work on fault detection was done in the years 2019 and 2020. This paper throws light on the significance of fault detection in smart day care while summarizing the work done in the directions. A day care is a place where parents entrust their child's safety and protection. This trust adds to the big responsibility that staff at day care has to adhere to. With kids around, it becomes difficult for them to go around every bend of the day care embedded with smart devices to check for faulty appliances. The paper proposed SWOT, a hybrid approach that brings information from day care apparatuses to take a look at the wellbeing status of each appliance. The information gathered from IoT gadgets/sensors is shipped off to a python-based algorithm for fault identification. At that point, health status is imparted to the end-user. The versatile application with the end-user involves programming that monitors all gadgets and cautions the client on deviation or faults. The literature study rolled out that little work has been done on a smart day care and the significance of a fault-tolerant or fault detection mechanism. Many pieces of research have been performed on developing and introducing smart devices to track kids' movement and monitor their health. On the contrary, the proposed approach focuses on the health and fault tolerance of smart devices, which are major components of a smart system. A pro-fault detection system will ensure the performance and robustness of smart devices. SWOT leverages the best of different hardware-based fault detection techniques by integrating them into a novel hybrid approach that has markable precision, accuracy with minimum false positivity rate and runtime.

Following enhancements can be implemented as future work.

(i) SWOT can be blended with cloud-based smart applications to report the health status of each device in the smart space in real-time.

(ii) Solution-based recommendations can be proposed to a technician concerned to handle the fault detected using above the algorithm.

Data Availability

The data will be available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to acknowledge Taif University Researchers Supporting Project Number (TURSP-2020/125), Taif University, Taif, Saudi Arabia.

References

[1] H. N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," *Enterprise Information Systems*, vol. 14, no. 9-10, pp. 1279–1303, 2020.

[2] A. Gaddam, K. O. Lundqvist, J. Citizen, and D. B. Calixto, "IoT and wireless sensor network for interactive waka structure," in *Proceedings of the 11th International Conference on Sensing Technology (ICST)*, pp. 1–4, IEEE, Sydney, NSW, Australia, December 2017.

[3] A. Gaddam, M. Al-Hrooby, and W. F. Esmael, "Designing a wireless sensors network for monitoring and predicting droughts," *International Journal on Smart Sensing and Intelligent Systems*, vol. 7, no. 5, 2020.

[4] I. Lee and K. Lee, "The internet of things (IoT): applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[5] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing*, vol. 6, no. 5, 2016.

[6] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[7] Y. Liu, Y. Yang, X. Lv, and L. Wang, "A self-learning sensor fault detection framework for industry monitoring IoT," *Mathematical Problems in Engineering*, vol. 2013, Article ID 712028, 8 pages, 2013.

[8] C. Wang, H. T. Vo, and P. Ni, "An IoT application for fault diagnosis and prediction," in *Proceedings of the IEEE International Conference on Data Science and Data Intensive Systems*, pp. 726–731, Sydney, NSW, Australia, December 2015.

[9] D. Mundada, A. Murade, O. Vaidya, and J. N. Swathi, "Software fault prediction using artificial neural network and Resilient Back Propagation," *International Journal of Computer Science and Engineering*, vol. 5, no. 3, 2016.

[10] J. Choi, H. Jeoung, J. Kim et al., "Detecting and identifying faulty IoT devices in smart home with context extraction," in *Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 610–621, IEEE, Luxembourg, Europe, 2018, June.

[11] T. Chakraborty, A. U. Nambi, R. Chandra, R. Sharma, M. Swaminathan, and Z. Kapetanovic, "Sensor identification and fault detection in IoT systems," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, pp. 375-376, Shenzhen China, 2018, November.

[12] D. S. Vibhute and A. S. Gundale, *Early Detection of Sensors Failure Using IoT*, 2019.

[13] A. Gaddam, T. Wilkin, M. Angelova, and J. Gaddam, "Detecting sensor faults, anomalies and outliers in the internet of things: a survey on the challenges and solutions," *Electronics*, vol. 9, no. 3, 2020.

[14] S. Arun, R. K. Anjaneya, and N. S. Dharshan, "Smart office monitoring system using IoT," *International Research Journal of Engineering and Technology*, vol. 6, no. 4, pp. 4560–4564, 2019.

[15] D. Macedo, L. A. Guedes, and I. Silva, "A dependability evaluation for Internet of Things incorporating redundancy aspects," in *Proceedings of the 11th IEEE international conference on networking, sensing and control*, pp. 417–422, IEEE, Miami, FL, USA, 2014, April.

[16] M. Uppal, D. Gupta, S. Juneja, G. Dhiman, and S. Kautish, "Cloud-based fault prediction using IoT in office automation for improvisation of health of employees," *Journal of Healthcare Engineering*, Hindawi Limited, vol. 2021, Article ID 8106467, 13 pages, 2021.

[17] S. Siraj, *ARCTIC: An IoT-Based System for Child Tracking in Day Care*, 2019.

[18] S. Srithar, "A continuous infant monitoring system using iot," *International Journal of Future Generation Communication and Networking*, vol. 13, no. 3, pp. 2407–2431, 2020.

[19] C. S. Jeong and M. R. Kwon, "A study on safety management of day care center using disaster management system," *The Journal of The Institute of Internet, Broadcasting and Communication*, vol. 18, no. 1, pp. 29–35, 2018.

[20] C. Shao, Y. Yang, S. Juneja, and T. GSeetharam, "IoT data visualization for business intelligence in corporate finance," *Information Processing & Management*, vol. 59, no. 1, 2022.

[21] S. Juneja, G. Dhiman, S. Kautish, W. Viriyasitavat, and K. Yadav, "A perspective roadmap for IoMT-based early detection and care of the neural disorder, dementia," *Journal of Healthcare Engineering*, Hindawi Limited, vol. 2021, Article ID 6712424, 11 pages, 2021.

[22] D. Badgujar, N. Sawant, and P. D. Kundande, *Smart and Secure I oT Based Child Monitoring System*, pp. 387–390, 2019.

[23] A. R. Nair, "IoT based infant supervising system," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 12S, pp. 67–72, 2019.

[24] P. Gouthaman and S. Sankaranarayanan, "Agile software risk management architecture for IoT-fog based systems," in *Proceedings of the International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 48–51, IEEE, Tirunelveli, India, 2018, December.

[25] A. B. Sharma, L. Golubchik, and R. Govindan, "Sensor faults: detection methods and prevalence in real-world datasets," *ACM Transactions on Sensor Networks*, vol. 6, no. 3, pp. 1–34, 2010.

[26] O. Ghorbel, M. W. Jmal, W. Ayedi, H. Snoussi, and M. Abid, "An overview of outlier detection technique developed for wireless sensor networks," in *Proceedings of the 10th Int. Multi-Conference Syst. Signals Devices, SSD 2013*, pp. 1–6, Hammamet, Tunisia, March 2013.

[27] D. Miljković, F. D. P. Shenoy, and P. M. Ameer, "Anamoly detection in wireless sensor networks," in *Proceedings of the IEEE Reg. 10 Annu. Int. Conf. TENCON*, pp. 1504–1508, Kochi, India, October 2019.

[28] H. Upadhyay, S. Juneja, A. Juneja, G. Dhiman, and S. Kautish, "Evaluation of ergonomics-related disorders in online education using fuzzy AHP," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 2214971, 11 pages, 2021.

[29] A. Mouzakitis, "Classification of fault diagnosis methods for control systems," *Measurement and Control (United Kingdom)*, vol. 46, no. 10, pp. 303–308, 2013.

[30] R. Isermann, "Fault detection with limit checking," *Fault-Diagnosis Systems*, Springer, Berlin, Germany, 2006.

[31] J. Lacaille, "An automatic sensor fault detection and correction algorithm," in *Proceedings of the 9th AIAA Aviation Technology, Integration and Operations (ATIO) Conference, Aircraft Noise and Emissions Reduction Symposium (ANERS)*, Hilton Head, South Carolina, September 2009.

[32] I. L. Us, "Method OF detecting faults using 373 A sty," vol. 2, no. 12, (12) United States Patent (54), 2012.

[33] M. Sadeghi, H. Soltani, and M. KHayyambashi, "The study of hardware redundancy techniques to provide a fault tolerant system," *Science Journal*, vol. 36, no. 4, 2015, http://dergi.cumhuriyet.edu.tr/ojs/index.php/fenbilimleri%20©2015%20Faculty%20of%20Science.

[34] L. Wu, B. Yao, Z. Peng, and Y. Guan, "An adaptive threshold algorithm for sensor fault based on the grey theory," *Advances in Mechanical Engineering*, vol. 9, no. 2, Article ID 168781401769319, 2017.

[35] L. Alcantara, J. Miera, B. Ariun-Erdene, and C. C. Teng, "The hitchhiker's guide to successful remote sensing deployments in Mongolia," in *Proceedings of the 2020 Intermountain Engineering, Technology and Computing (IETC)*, pp. 1–6, IEEE, Orem, UT, USA, October 2020.

[36] D. Miljkovic, "fault detection using limit checking: a brief introductory review," in *Proceedings of the 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 908–913, IEEE, Opatija, Croatia, September 2021.

[37] N. ElHady and J. Provost, "A systematic survey on sensor failure detection and fault-tolerance in ambient assisted living," *Sensors*, vol. 18, no. 7, 2018.

[38] M. Majid, S. Habib, A. R. Javed et al., "Applications of wireless sensor networks and internet of things frameworks in the industry Revolution4.0: a systematic literature review," *Sensors*, vol. 22, pp. 1–36, 2022.

[39] R. H. Jhaveri, S. V. Ramani, G. Srivastava, T. R. Gadekallu, and V. Aggarwal, "Fault-resilience for bandwidth management in industrial software-defined networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3129–3139, 2021.

[40] P. Kumar, R. Kumar, G. Srivastava et al., "PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326–2341, 2021.

[41] M. A. Khan, Z. Dur, B. Ashraf, H. Ali, J. Rashid, and J. Kim, "Dynamic modeling of a nonlinear two-wheeled robot using data-driven approach," *Processes*, vol. 10, no. 3, p. 524, 2022.

[42] Y. Hikmat, H. Tanveer, A. K. Zulfiqar, K. Deepika, Y. L. Mi, and W. Sung, "Vision sensor-based real-time fire detection in resource-constrained IoT environments," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 5195508, 15 pages, 2021.

[43] N. Ahmed, R. Amin, H. Aldabbas, K. Deepika, B. Alouffi, and T. Shah, "Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges," *Security and Communication Networks*, vol. 2022, Article ID 1862888, 19 pages, 2022.

[44] J. Rashid, M. A. S. Syed, and I. Aun, "A novel fuzzy k-means latent semantic analysis (FKLSA) approach for topic modeling over medical and health text corpora," *Journal of Intelligent and Fuzzy Systems*, vol. 37, no. 5, pp. 6573–6588, 2019.

[45] S. Frank, G. Lin, X. Jin, and R. Singla, "Metrics and methods to assess building fault detection and diagnosis tools," *Natl. Renew. Energy Lab*, https://www.nrel.gov/docs/fy19osti/72801.pdf, 2019.

[46] M. Syafrudin, G. Alfian, N. Fitriyani, and J. Rhee, "Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing," *Sensors*, vol. 18, no. 9, p. 2946, 2018.

[47] M. K. Hasan, M. Akhtaruzzaman, S. R. Kabir et al., "Evolution of industry and blockchain era: monitoring price hike and corruption using BIoT for smart government and industry 4.0," *IEEE Transactions on Industrial Informatics*, 2022.