A Smart Wearable Device for Preventing Indoor Electric Shock Hazards

Zaipeng Xie[1](✉), Hanxiang Liu[1], Junpeng Zhang[1], Xiaorui Zhu[1], and Hongyu Lin[2]

[1] Hohai University, Nanjing, China
zaipengxie@hhu.edu.cn
[2] Southeast University, Nanjing, China

Abstract. The emerging wearable IoT technology is evolving dramatically in recent years and resulted in a wide adoption in various applications. Electric shock hazard is one of the major indoor hazards for consumers who may fail to recognize potential electrical risks. This paper proposes a smart wearable IoT device with risk assessment algorithms for preventing indoor electrical shock hazards. This device consists of two hardware components: a receiver and a detector embedded in a power switch. The detector consists of a Wi-Fi module, a current sensor, a NFC module, and an Arduino mini module that communicates with a software routine monitoring the status of the power switch and its connected appliances. The receiver is a passive NFC tag that can be designed as an accessory or clothing that customers may wear. A risk assessment algorithm is proposed using a set of predefined inference rules. The software routine is developed to provide early warnings to customers where potential electrical shock risk level is high. This paper describes the implementation details as well as the algorithms. Experimental results are summarized and they demonstrate that the proposed smart wearable device can be effective in predicting electric shock hazards in an indoor environment.

Keywords: Wearable device · Smart device · IoT · Electric shock hazard · Risk analysis

1 Introduction

With the prevalence of appliances in modern families, indoor electric shock hazard has been reported [1] as one of the major causes of accidents in household. Electricity consumers could incur electric shock due to lack of experience and

Supported by the Innovative and Entrepreneurial Talent Program of Jiangsu Province (Grant No. 2016B17078) and partially supported by the National Key R&D Program of China (Grant No. 2016YFC0402710).

X. B. Zhai et al. (Eds.): MLICOM 2019, LNICST 294, pp. 293–304, 2019.
https://doi.org/10.1007/978-3-030-32388-2_25

failure of recognizing potential electric hazards. Recent research [2] revealed that power switch and appliance malfunction may cause electrical hazards, accounting for 40% of all electrical fatalities of year 2017 in China. The majority of these incidents were caused by direct contact with power lines, power outlets, appliances, and hand-carried conductive objects. Children and pets are especially vulnerable to electric shock hazards, because they are naturally inquisitive and can be tempted to approach and explore those areas. Hence, preventing indoor electric shock has become one of the primary issues for the household electrical safety.

Recent advances in the Internet of Things (IoT) technology has made smart IoT devices accessible to customers in vast industrial and household applications. For example, Kamilaris et al. [3] implemented a solution for a web-based energy-aware smart home framework that connects smart IoT devices to the Internet, where a star topology and a multi-hop topology was evaluated for apartments. Cloud-based IoT paradigm was proposed in [4] where all data from different IoT sensors can be gathered in the cloud platform that may provide a high reliability and scalability. IoT systems can bring a natural advantage for embedded applications to detect hazards. Lezama et. al. [5] developed an IoT system for AC series arc detection by inter-period correlations of current via embedded sensors. Mader et. al. [6] implemented hazard analysis framework for automotive IoT systems. IoT hardware for instrumentation and measurement [7] was widely adopted in several industrial applications [8] at CERN. Wearable devices [9] as one type of IoT devices are usually designed as accessories or clothing that people may wear. They are often expected to continuously collect and upload various data to improve the quality of life. Although small in size, wearable IoT devices often require reliable communication and reduced power consumption of the system. Many smart wearable IoT devices have emerged for the past several years in a variety of applications.

Smart wearable IoT technology can be effective in preventing indoor electric shock accidents and providing early warnings to customers. This paper explores a smart wearable IoT solution for preventing indoor electrical shock hazards that can provide modularity and economic viability. The proposed device consists of two hardware parts: the detector part is integrated in the power switch and it employs a Wi-Fi module, a current sensor, a Near Field Communication(NFC) module, and an Arduino mini [10] module that communicates with a software to monitor the status power switches and appliances; the receiver part is a passive device that can be worn by human or pets. Based on a set of predefined inference rules, a risk assessment algorithm is implemented and it is capable of evaluating the electric shock risk of power switches and appliances. The algorithm can be deployed on a local or cloud-based server and it will provide early warnings to the related personnel via portable devices. Potential electrical shock hazards are suggested based on the acquired data from the wearable devices. This paper presents the basic building hardware and software elements for delivering the infrastructure of the smart wearable device. Section 2 discusses system description that includes the hardware implementation and the risk assessment algorithm with he inference rules for risk analysis. Experimental results are demonstrated in Sect. 2.4 and final remarks are concluded in Sect. 3.

2 System Description

The proposed smart wearable IoT device consists of two hardware components: a detector and a receiver. A software is deployed on a local or cloud server to interact with the hardware. Figure 1 shows a diagram of the proposed system. The detector is integrated with a power switch where it contains a Wi-Fi module, a current sensor, a NFC module, and an Arduino mini module that communicates with a software routine to monitor the status of power consumption; the receiver is a passive device that can be designed as an accessory or clothing that people may wear. Based on a set of predefined inference rules, a risk assessment algorithm is implemented to evaluate the electric shock risk level of the power switches and appliances.

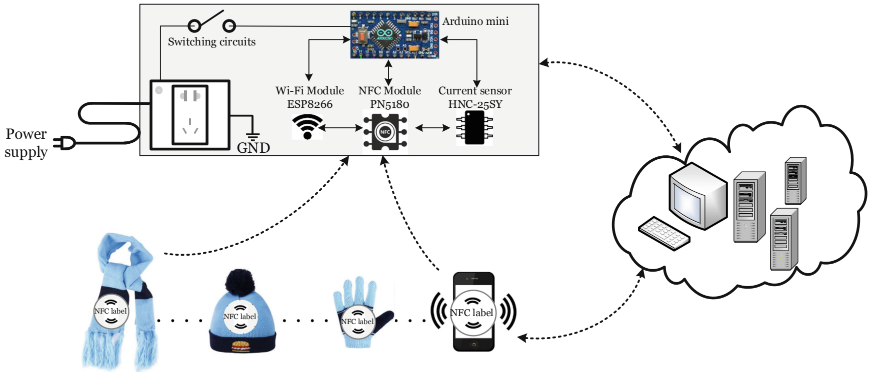

Fig. 1. Diagram of the proposed overall system.

2.1 Hardware Implementation

The designed hardware device has the following four major features: (1) to raise an alert when the wearable IoT device is detected within an effective range of the power switch that equipped with our detector; (2) to turn on and off the power switch automatically; (3) to monitor the average current of the power switch; (4) to connect with a wireless router and send/receive real-time data periodically. The system is required to be compact such that it can be fit into a typical electrical junction box. Hence, design consideration is required to implement the hardware in a compact size while achieving the aforementioned features.

Figure 2 shows the schematic of the proposed hardware. The proposed wearable hardware has a receiver component using a NFC tag and it does not require

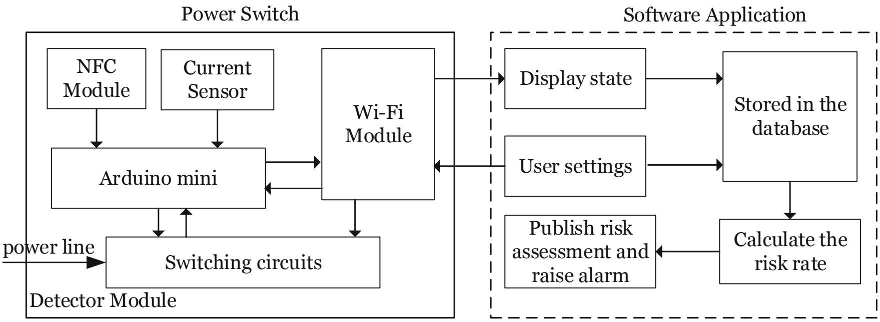

Fig. 2. Schematic of the proposed hardware implementation.

battery. The receiver can be designed as a clothing for human or a collar that a pet may wear. The proposed wearable hardware has a detector system that consists of a Wi-Fi module, a current sensor, a NFC reader module, and an Arduino mini module. The NFC reader module can be triggered when the receiver is within the effective range (about 50–75 cm of distance). When the NFC reader module is triggered, an alert signal is raised and the power switch is turned off simultaneously. The current sensor collects the output current of the power switch. The Wi-Fi module connects the Arduino mini module to the Internet and publish the real-time sensor data to a time series database.

The NFC module is implemented using a full NFC front-end IC (Model PN5180)[11] and it is responsible for sensing the distance of the NFC tag. The communication distance of PN5180 complies with the ISO/IEC 15693 and ISO/IEC 18000-3 communication protocols [12], and it can sense specific NFC tags within a range of about 50–75 cm, which makes it suitable as an distance sensor for our proposed system.

The current sensor is implemented using a multi-range Hall Current Sensor (model HNC-25SY) that has a high immunity to external interference. The main purpose of this sensor is to monitor the average AC current of the power switch and provides sensed data for the risk assessment algorithm.

The Wi-Fi module is implemented using the low-power Wi-Fi card (model ESP8266). The ESP8266 is an integrated microchip with a compact design that supports a variety of modes including softAP, station, softAP+station. The Wi-Fi module is connected to an ATmega168-based Arduino mini development board via a serial port and it provides a fast wireless data transfer rate.

The Arduino mini module [10] is a small micro-controller board based on the ATmega168 microprocessor. This module has 14 digital input and output pins, 6 analog inputs, an on-board resonator, and holes for mounting pin headers. This module has a compact size and easy to program. Its main role is to control the power switch and handle the transferring of sensor data and user instructions via the Wi-Fi module.

Figure 3 shows the control flow of the hardware system. When the system is turned on, the NFC module and the current sensor are initialized. If the Wi-Fi module has not been configured or the configuration information is incorrect, the system will transit to the configuration mode. After the Wi-Fi module is successfully configured and connected to the wireless network, the detector resumes the working mode. At the working mode, the Arduino mini module acquires the measured current data periodically. On receiving a user instruction, the Arduino mini module is interrupted and executes the user instruction. The NFC reader constantly monitors the existence of approaching NFC tag. It will produce a warning signal and shut down the power switch on detecting an wearable device that contains the NFC tag within its working range.

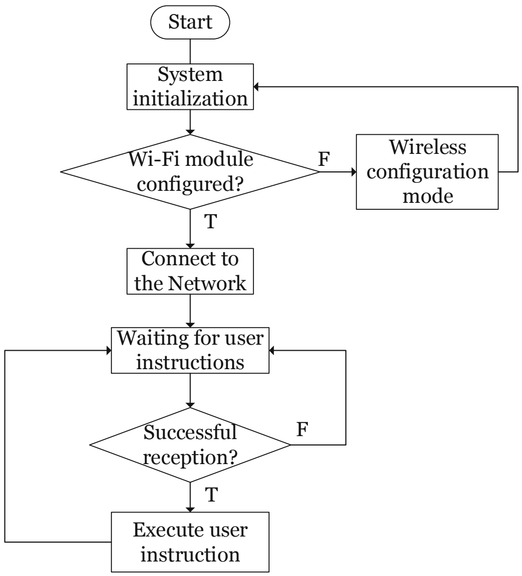

Fig. 3. The control flow of the hardware system.

2.2 Software Implementation

A software routine has been developed to allow users to view and configure the hardware at any time. The software routine can be run on a local or cloud-based server. The routine works as a finite state machine that transits between two states: the initialization state and the executing state. At the initialization state, it is required to configure the Wi-Fi module and pair the software routine with the hardware. On completion of the pairing, the software transits to the executing state, where the software is collecting data continuously on the server. The data includes the average current and the NFC alarm signal.

Figure 4 shows the flow chart of the software routine. The data captured on the software routine is interpreted for two purposes: (1) displaying the hardware

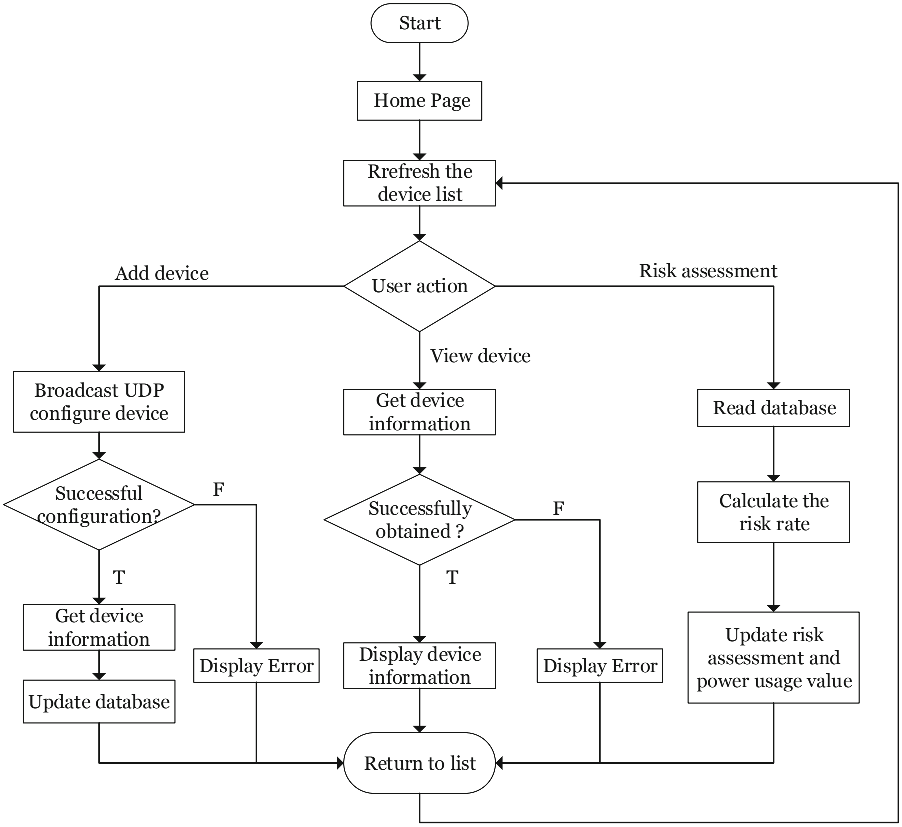

Fig. 4. The flow chart of the software implementation.

status; (2) calculating the risk factor of individual power switch. A risk assessment algorithm is implemented to assess an electric hazard risk using the historical data. At the same time, the user can perform operations such as switching on and off the switch, viewing historical data, and viewing the risk-level heatmap of all connected power switches.

2.3 The Risk Assessment Algorithm

The risk assessment algorithm is used for evaluating the level of the electric shock hazard at each device. A device is considered as a power switch containing the detector hardware. A heatmap is generated to describe each device's risk level based on collected data. The potential electric shock hazard is evaluated using the historical data and warning can be raised to assist preventing potential electric shock. This section describes the analysis model of the risk assessment algorithm. As shown in Fig. 5, the risk assessment algorithm has three input variables: the measured average current in Ampere, the number of NFC alarm events per time unit, and the age of the power switch. The output of the algorithm is the calculated risk level assessment.

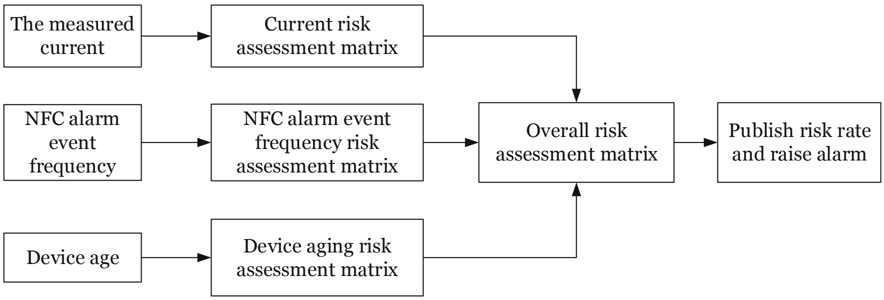

Fig. 5. Data flow of the risk assessment algorithm.

The Risk Assessment Matrix [14] is an effective method to evaluate potential risk in decision making systems by considering the category of risk rate against the category of severity. It employs a matrix to visualize potential risks in a qualitative way. The evaluated risks are generated using the input data and described in several risk levels. Four levels are adopted in our algorithm as Low I, Moderate II, High III, and Extreme IV. The Low I corresponds to a low risk and the power switch has no risk of electric shock. The potential electric shock hazard is small or negligible, the frequency of contact is close to zero. For this level of risk, no additional measures are required to reduce the risk. Moderate II corresponds to a moderately dangerous, slightly risky device that may cause a slight electric shock. The resulting hazard is moderate and may not occur as usual. For this level of risk, it is acceptable when the activity of children or pets is within the guardian's line of sight. High III corresponds to a high risk. Power switch at this level may cause an electric shock and great damage to the body. For this level of risk, strict prevention of customers from exploring such area is suggested. Extreme IV corresponds to a extremely high risk that may incur electric accidents and even life threats. For this level of risk, such device should be replaced and isolated from general contact, the area around the device should be isolated to children and pets.

The risk assessment for the average current is defined in Table 1 that determines the electrical shock risk level. When the current reaches [10, 30] mA through the human body, it will cause tender stimulus; a [30, 100] mA current will cause some pain on human body. While a [100, 250] mA current will cause a strong pain and possible cramp. When the current through the body exceeds 250 mA, the subject may incur severe damage to its tissue and even death. The risk level of the current is quantified to interpret electric shock hazards. Different current values correspond to different consequences, including A0, A1, A2, and

A3. The four levels can be summarized as given in Table 1. Here, level A0 has a quantization value of 1, level A1's quantization value is 10, and the quantization value of Level A2 and A3 are 100 and 1000 respectively.

Table 1. The Risk Matrix for the average current.

	Risk level	Average current (mA)	Risk quantization
A0	Low I	[10, 30]	1
A1	Moderate II	[30, 100]	10
A2	High III	[100, 250]	100
A3	Extreme IV	$[250, +\infty]$	1000

The risk assessment for the number of NFC alarm events is also part of the overall risk analysis. Since the total number of NFC alarm event varies randomly in different scenarios. We propose using the NFC alarm event frequency, $\tilde{T}$, to assess its risk factor and it can be defined by the following equation

$$\tilde{T} = \frac{1}{N}\sum_{i=1}^{N} T_i \tag{1}$$

Here, the risk factor of the number of NFC alarm events can hereby be defined as the event frequency correspond to different NFC alarm risk levels, including E0, E1, E2, and E3. The four levels can be summarized as given in Table 2:

Table 2. The Risk Matrix for the NFC alarm events.

	Risk level	Event frequency	Risk quantization
E0	Low I	$[0, 0.5\tilde{T}]$	1
E1	Moderate II	$[0.5\tilde{T}, \tilde{T}]$	10
E2	High III	$[\tilde{T}, 1.5\tilde{T}]$	100
E3	Extreme IV	$[1.5\tilde{T}, +\infty]$	1000

The risk assessment for the aging of electronic components is also one of the factors in the overall risk analysis. The aging of power switches can have a direct relationship with the electric shock hazard. The failure rate of electronics usually has a bathtub shape [13]: i.e., the risk level noticeably decreases due to early failures that could be caused by design faults or initial implementation defects. The risk level increases after a useful life span due to material fatigue and component aging. The bathtub shaped risk function is adopted in our algorithm as a piece-wise function with four segments. The risk assessment of the device aging is categorized into four risk levels, G0, G1, G2, and G3 as in Table 3.

Table 3. The Risk Matrix for the aging of electronics.

	Risk level	Age (years)	Risk quantization
G0	Low I	$[0, 0.5]$	10
G1	Moderate II	$[0.5, 1]$	1
G2	High III	$[1, 3]$	10
G3	Extreme IV	$[3, +\infty]$	100

The overall risk assessment for the proposed smart IoT wearable system is hence defined as a combination of the average current (A), the number of NFC alarm events (E), and the aging of electronic device (G) as given by Equation

$$V(I, \tilde{T}, age) = A(I) \cdot E(\tilde{T}) \cdot G(age) \quad (2)$$

where $V(I, \tilde{T}, age)$ is the overall risk assessment, I is the measured current of the particular power switch, and $\tilde{T}$ is the NFC alarm event frequency.

2.4 Experimental Results

The experiments were carried out in a 80 m^2 apartment building where a total of twenty power switches have been replaced by the proposed hardware. The NFC tag is worn by an adult who lives inside this apartment. Test procedures were constructed and executed to measure the reliability and effectiveness of the smart wearable IoT system. All experiments were conducted in an indoor environment to emulate the condition of a typical household scenario. The experiments lasted for about 18 months and for each set of experimental trials, the data are collected and stored in a local server.

Figure 6 shows the measured average current of three typical devices in 18 months. The figure shows that the measured average current varies each month. But the variation is relatively small, about 5% to 15%, in a year long aspect. However, the data reveal that the average current differs among devices and it may cause a varying level of electric shock hazard for different areas.

Figure 7 shows the number of NFC alarm events of three typical devices in 18 months. The number of NFC alarm events varies randomly from month to month. The data reveals that some devices can have frequent visits for several months. This may indicate that users visit those areas regularly and it may cause a high level of electric shock hazard near those devices. Customers can be suggested to pay extra attention to those areas and caution can be taken for individual devices.

Figure 8 shows the generated heatmap of all twenty devices in 18 months. The heatmap is an excellent visualization tool for the customers to understand potential hazards. In Fig. 8, the colorbar indicates potential hazard risk levels inside the house, where light blue means a relatively low risk level (Low I), yellow means a moderate risk level (Moderate II), green means a high risk level (High III), and red means an extreme situation where the probability of electric

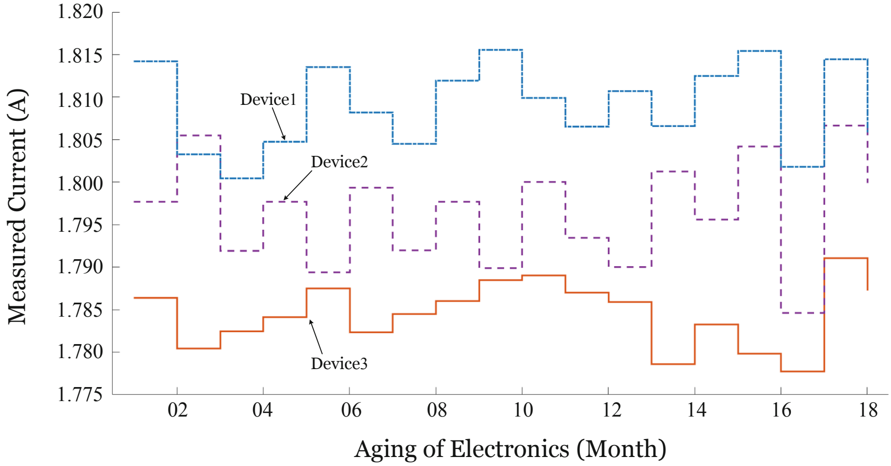

Fig. 6. The measured average current of three typical devices for 18 months.

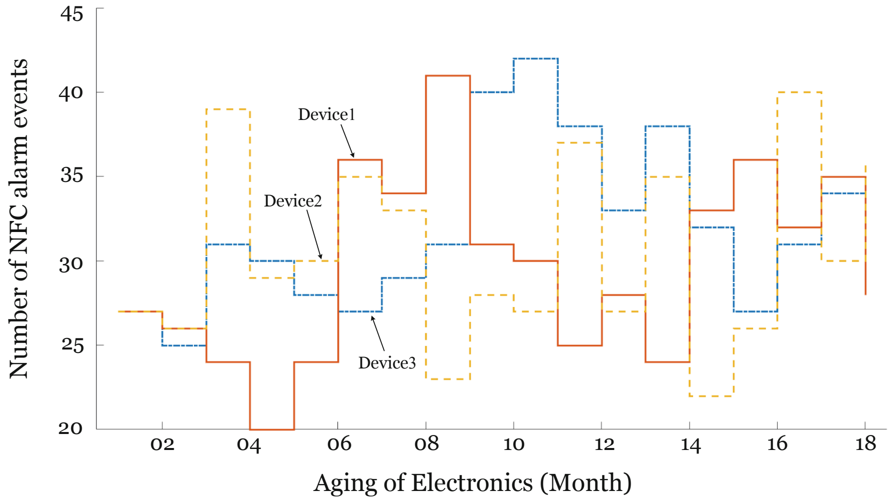

Fig. 7. The measured NFC alarm event of three typical devices for 18 months.

shock hazard can be very high (Extreme IV). The results reveal quite a lot of information about the potential electric shock hazards, for example, Device-2 shows a high risk level in the first two months and the hazard was prevented due to the isolation of those areas such that electric shock hazard can be prevented. Device-12 exhibits a repeating pattern of high risk levels and it could indicate that the user is visiting this area on a regular basis. Customers can, hence, take actions to prevent hazards just by viewing the heatmap. A fine-grained definition can be employed to manifests in a higher number of overall risk levels, which can potentially benefit in flexibility when highlighting the electric hazard. In summary, the experimental results demonstrated an example scenario where the proposed device can be effective in visualizing and estimating the risk factors of the corresponding area.

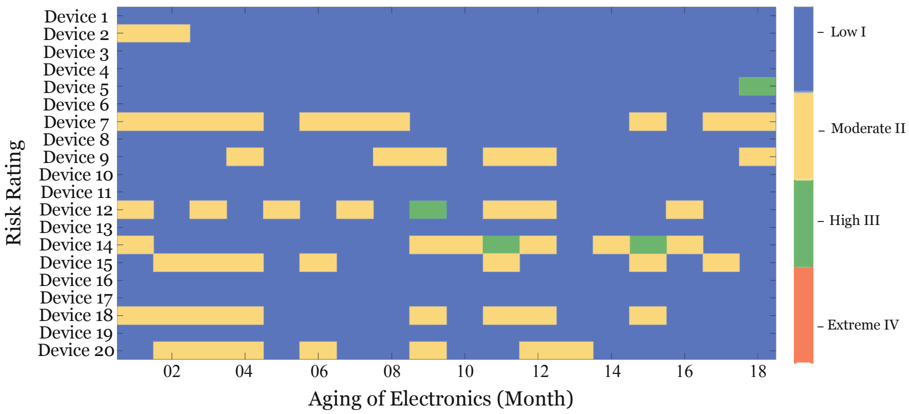

Fig. 8. The generated heat-map of all twenty devices for 18 months. (Color figure online)

3 Conclusions

This paper proposes a smart wearable IoT device that is capable of preventing indoor electric shock hazards. The overall hardware and software design details are described, and a recommended algorithm for assessing hazard risks is presented. The entire device utilizes an NFC module, a current sensor, a Wi-Fi module paired with an Arduino mini micro-controller to achieve the functionality. Customers can operate on the device through a software application where the sensor data, NFC signals, and the age of the equipment are used to evaluate the potential electric shock risk of each device. The risk assessment algorithm has been evaluated in an experimental test scenario for eighteen months; and the experimental results show that the proposed system can provide convenient and easy understandable visualization heatmaps to users. In summary, the proposed system is effective in preventing electric shock hazard and assisting parents and pet owners to protect their loved ones.

References

1. Gordon, L.B., et al.: A complete electrical shock hazard classification system and its application. IEEE Trans. Ind. Appl. **54**(6), 6554–6565 (2018). https://doi.org/10.1109/TIA.2018.2803768
2. Statistical analysis of the causes of electric shock accidents (2019). http://www.dgxue.com/anquan/jichu/1913.html
3. Kamilaris, A. et al.: HomeWeb: an application framework for Web-based smart homes. In: 18th International Conference on Telecommunications, Ayia Napa, Cyprus, pp. 134–139 (2011). https://doi.org/10.1109/CTS.2011.5898905
4. Biswas, A.R. et al.: IoT and cloud convergence: opportunities and challenges. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, pp. 375–376 (2014). https://doi.org/10.1109/WF-IoT.2014.6803194
5. Lezama, J., et al.: An embedded system for AC series arc detection by inter-period correlations of current. Electr. Power Syst. Res. **129**(1), 227–234 (2015). https://doi.org/10.1016/j.epsr.2015.08.005
6. Mader, R., et al.: A computer-aided approach to preliminary hazard analysis for automotive embedded systems. In: 18th IEEE International Conference and Workshops on Engineering of Computer-Based Systems, Las Vegas, USA, pp. 169–178 (2011). https://doi.org/10.1109/ECBS.2011.43
7. Harnett, C.: Open source hardware for instrumentation and measurement. IEEE Instrum. Meas. Mag. **14**(3), 34–38 (2011). https://doi.org/10.1109/MIM.2011.5773535
8. CERN Open Hardware Repository (2019). https://www.ohwr.org/projects/cernohl
9. Seneviratne, S., et al.: A survey of wearable devices and challenges. IEEE Commun. Surv. Tutor. **19**(4), 2573–2620 (2017). https://doi.org/10.1109/COMST.2017.2731979
10. Banzi, M., Shiloh, M.: Getting Started with Arduino: The Open Source Electronics Prototyping Platform. Maker Media Inc., Sebastopol (2014)
11. NXP Semiconductors.: PN5180 High-performance multiprotocol full NFC Forum-compliant frontend: Product data sheet, Rev. 3.2 (2017)
12. ISO/IEC 18000–3 (2019). https://www.iso.org/standard/53424.html
13. Bebbington, M., et al.: Useful periods for lifetime distributions with bathtub shaped hazard rate functions. IEEE Trans. Reliab. **55**(2), 245–251 (2006). https://doi.org/10.1109/TR.2001.874943
14. Yang, Q., et al.: A rough set approach for determining weights of decision makers in group decision making. PloS One **12**(2), e0172679 (2017). https://doi.org/10.1371/journal.pone.0172679