A Comprehensive Risk Assessment Framework for IoT-Enabled Healthcare Environment

Mofareh Waqdan[a], Habib Louafi[b] and Malek Mouhoub[c]

Department of Computer Science, University of Regina, Regina, SK, Canada

fi

Keywords: Internet of Things (IoT), Risk Assessment, Risk Parameters, IoT Attacks.

Abstract: The significance of risk assessment in medical sectors, particularly in emergency rooms, is crucial due to the criticality of the service. We present a comprehensive risk assessment framework for analyzing the risks associated with deploying and using Internet of Things (IoT) technologies in a healthcare environment. In this context, we improve upon the existing methodologies by dynamically calculating the risk score for different devices profiles, considering their number along with other parameters, such as network protocols, device heterogeneity, device security updates, device physical security status, device history status, layer history status, and device criticality. The framework helps healthcare organizations identify, assess, and manage the risks of IoT, which can range from data privacy and confidentiality to system integrity, availability, and performance.

1 INTRODUCTION

The overwhelming spread and use of the Internet have enabled hyper-connectivity, where data and information can instantly be shared anywhere across the globe. This phenomenon of hyper-connectivity has further been fueled by the concept of the IoT, which has transformed our daily lives in a wide variety of ways (Koohang et al., 2022). IoT applications are now extended to roughly all facets of human life, e.g., transportation, e-governance, sustainable cities, smart agriculture, power grids, smart homes, e-healthcare, etc. This hyper-connectivity through IoT networks is not always safe or secure because attackers are always on a hunt to find weaknesses, misconfigurations, protocol flaws, or hardware failures in order to subvert the Confidentiality, Integrity, and Availability (CIA) of these IoT networks. Moreover, the heterogeneous nature of IoT devices along with their limited computing and processing power make the problem quite intense. This becomes way more serious in IoT-enabled healthcare facilities, especially emergency rooms, critical care units, and operation theaters (Razdan and Sharma, 2022). IoT has revolutionized healthcare service delivery by connecting medical devices and systems that help monitor and manage patient health more accurately, and efficiently, which has never been possible before.

However, this advancement also carries risks that must be addressed prior to IoT applications implementation as cyber-attacks might directly affect human lives in critical care and otherwise. The compromise of CIA objectives taking place as a result of a highly expected cyber-attack definitely results in impacting normal and routine business operations of any organization. In these circumstances, the organization is considered to be prone to risks. A security risk is usually evaluated as a function of the likelihood of a certain threat agent exploiting any potential vulnerability and the consequent negative business impact on the system or network (Roy, 2020). Organizations adopt multiple ways to thwart such risks and ensure protection against them with the implementation of certain security controls. The entire process of managing and mitigating risks is called Information Assurance (IA) (McIlwraith, 2021). Risk Management is the fundamental component of any organization's IA program, as it helps in identifying the current threats, vulnerabilities, and their associated risks, with an aim to provide a cost-effective defensive and information protective regime. The risk management programs as shown in Figure 1 are meant to address all the four types of security events (Interruption, Interception, Modification, and Fabrication).

[a] https://orcid.org/0000-0003-4916-3911

[b] https://orcid.org/0000-0002-3247-3115

[c] https://orcid.org/0000-0001-7381-1064

Waqdan, M., Louafi, H. and Mouhoub, M.
A Comprehensive Risk Assessment Framework for IoT-Enabled Healthcare Environment.
DOI: 10.5220/0012060900003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 667-672
ISBN: 978-989-758-666-8; ISSN: 2184-7711

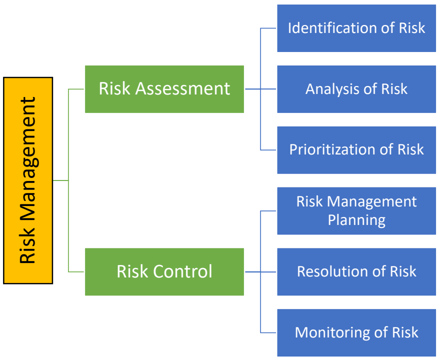

Figure 1: Risk management components.

In Table 1, we summarize the reviewed solutions and framework related to IoT risk assessment. Overall, the existing research work focuses on Risk Assessment in an IoT-enabled healthcare environment using contemporary approaches, where only the Risk and Likelihood impacts are taken into account. They do not take into account cases, where the number of devices is variable and differs significantly. This was the key factor that led us to develop the proposed Risk Assessment framework for IoT-enabled healthcare environments, taking into consideration the important parameter of the number of devices thereby giving more insightful risk scoring.

IoT devices in a healthcare environment are highly prone to a number of cyber risks. The most significant of these risks involve the security and privacy of patient data. Due to the high degree of interconnectivity, there is an increased risk of someone gaining unauthorized access to patient data and affecting its CIA. Moreover, due to the centralization of data, it has become increasingly difficult for healthcare providers to ensure the privacy of patient data. Another major risk in IoT-based healthcare environments is their potential for malfunction or service disruption. As components are interconnected, a disruption in one component may affect the entire system, resulting in unintended consequences. This is especially concerning in critical care settings, where any error could have dire consequences. Moreover, a potential risk is the production of large amounts of data that are difficult to interpret and use. The complexity of the data collected may overwhelm healthcare providers if they are not trained to properly interpret and use the data. This becomes more serious when the number of devices is increasing (Raghuvanshi et al., 2022).

In this paper, we propose a comprehensive risk assessment framework for IoT-enabled healthcare environments. Our framework takes into account all the aforementioned concerns, and is meant to be used by researchers and practitioners in cyber security related to healthcare systems.

2 PROPOSED RISK ASSESSMENT FRAMEWORK

The proposed risk assessment framework, for IoT devices in an emergency healthcare environment, is based on Risk Likelihood, Impact Likelihood, and the Device Profile and Threshold level. Figure Figure 2 explains the overall flow of the proposed risk assessment methodology.

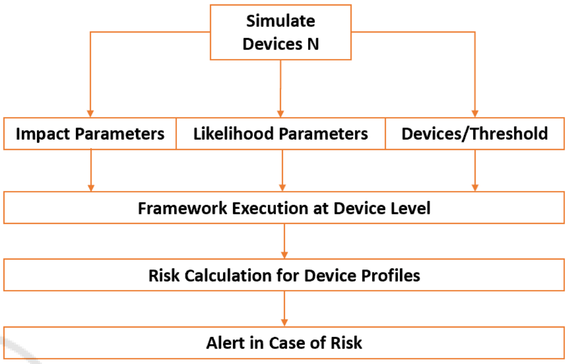

Figure 2: Proposed Framework.

2.1 Risk Evaluation

Risk is not just a technical problem, it is also a managerial one. Any asset in the organization, be it hardware, software, services, human resource, etc., face risks that challenge its confidentiality, integrity, and availability. Risk is always an amalgamation of threat to the asset, the likelihood of occurrence of that threat, and the corresponding impact on business. From these perspectives, the threat's impact and its likelihood are of immense importance as the business aspect in our case is linked to the healthcare sector's emergency facility. The broader risk evaluation formula is given by Equation 1.

$$\mathbb{R}_a = \mathbb{W}_a \times \mathbb{S}_a \tag{1}$$

where, a represents any asset, $\mathbb{W}$ represents the risk impact due to vulnerabilities and cybersecurity issues, and $\mathbb{S}$ is the likelihood of that risk-taking place.

2.2 Risk Impact Evaluation ($\mathbb{W}$)

Since the risk impact class $\mathbb{W}$ is a key factor in determining the risk potential, and its overall impact on the organization and asset, it is therefore fundamentally important to study the very causes of this factor. The proposed risk evaluation framework takes into account the following key factors that play a part in the risk impact: - Network factor (N) - Protocol factor (P) - Network design (D) - Device Level (L)

Table 1: Existing work on IoT security risk assessment.

Research Work	**Risk Detection Technique(s)**	**IoT Environment**	**Strengths**	**Weaknesses**
(Jasour et al., 2022)	Profile justification, risk assessment model selection, security monitoring, model evaluation, validation, and update	Connected and autonomous vehicles	Dynamic risk evaluation, Making use of ML techniques	Not accounting for the number of IoT-enabled devices. Validated only on the network of vehicles
(Zhao et al., 2021)	IoT-based threat situation awareness architecture using edge computing	Normal IoT equipment	Use of ML for dynamic evaluation. Use of dedicated device for threat analysis	The framework has only been tested for threats generated as a result of network traffic
(Matsuda et al., 2021)	Penetration Testing	Industry 4.0 components	Use of AI and OPC Unified Architecture along with penetration test for real world monitoring of threats	The size of the IoT network has not been accounted for in Risk evaluation
(Bahizad, 2020)	Risk Assessment considerations for developing IoT devices	IoT communication devices	The proposed framework did discuss risks due to increasing IoT devices in the network	No new or novel risk assessment and evaluation framework solution provided
(Wang et al., 2020)	IoT device recommendation mechanism for selecting trusted participants	Smart city environments	An intelligent device selective recommendation mechanism along with game theory based validation method.has been proposed	Not very scalable for more IoT devices dynamically being added and removed from network
(Matheu et al., 2020)	Real-world Risk assessment strategy	Industry 4.0	IoT cyber-security certification framework, integrating research and technical tools have been discussed	Survey of existing frameworks; no novel solution has been provided
(Oser et al., 2020)	Helps selecting optimal/secure IoT devices through user awareness	IoT device(s) selection	Focused on improved users' ability to assess the security of connected devices	Findings are based on survey/ interview of one organization with only limited number and types of IoT devices
(Datta, 2020)	SIEM based risk assessment framework	Focuses on five major IoT attacks	An end-to-end IoT Platform with integrated SIEM has been tested against five types of cyber attacks	Focuses on DDoS attacks in a simulated docker container environment instead of a real IoT network
(Radanliev et al., 2020)	Real-time intelligence, AI/ML	Industrial IoT	Dynamic supply chain system integrated with ML based real-time analytics has been proposed	Proposed system is suitable for only SME with limited IoT devices
(Chen et al., 2020)	Probability response and utility attenuation behavioral model	Power grids	Behavioral model is proposed and tested on IEEE RTS-79 system, making use of probability responses	The proposed framework has only been tested only for cyber-attacks on Power grids
(Radanliev et al., 2018)	Functional Dependency, Network-based Linear Dependency Modelling	Generic IoT	Use of mathematical formalism for IoT Risk assessment along with the economic impact of IoT attacks on the networks has been presented	No use of modern analytics, such as the use of AI/ML
(Samad et al., 2018)	Flexible four-step Risk evaluation model (justification, model selection, training, security monitoring)	Autonomous Vehicles (Child Seats)	The proposed framework presents an autonomous system, working at multi-level of mobile cloud infrastructure	Tested on a Baby car seat, connecting with cloud; thus limited numbers and types of devices
(Nurse et al., 2017)	Analysing dynamic and unique IoT characteristics	CPS	A comprehensive survey of IoT characteristics used in Risk Assessment	No new/novel framework presented

- Attack attributes (A), which are detailed in the following:

Network Attacks/Issues (N): All the IoT networks placed in a healthcare facility are potentially connected to the Internet and are part of some network to offer speedy, robust e-healthcare services. Being part of the network(s) automatically makes them susceptible to a wide variety of issues, which if compromised directly impacts the device's functionality and indirectly affects the overall IoT network. There can be many network-related issues and attacks that can generate and amplify the risk impact. Table 2 discusses a few network attacks, which may affect IoT devices in a healthcare facility.

Protocol Issues (P): Another issue that directly affects the risk likelihood is the protocol type used by the IoT devices. Many IoT devices make use of various protocols to communicate and perform their network-related tasks. For instance, MQTT, ZigBee, Bluetooth, and RFID are common protocols that are used by IoT devices and, to some extent, have some issues and are prone to certain protocol attacks.

Network Design Issues (D): The way the network is designed and configured also directly impacts the overall security. For instance, more intermediate systems would result in more windows of opportunity for the attacker, which significantly increases the risk. In this case, not just the number of compromised devices will increase but also the exposure factor of the IoT network will augment. Therefore, this factor is also fundamentally important in computing the overall risk impact.

Device Level Security (L): The security at the device level is also important, as different types of devices have different security issues. A vulnerable device is more susceptible to attacks as compared to a patched and/or hardened one.

Attack Attribute (A): We are also quite interested in the actual security attribute that has been compromised because, under different circumstances, the importance of security attributes vary significantly. For instance, Dos or DDoS attacks affect availability, while replay attacks target confidentiality or integrity, and ransomware targets availability. The violation of CIA objectives has different repercussions under different scenarios.

Given all the aforelisted factors, we propose to evaluate the risk impact for a given asset a, as shown in Equation 2.

$$\mathbb{W}_{\mathrm{a}} = (N+P+D+L+A)/5 \tag{2}$$

Table 2: Examples of Known Attacks and Their Impact.

Attacks	Impact
Denial of Service (DoS)	A DoS attack can directly bombard any IoT device with a large number of packets if not countered at the network's gateway. Since DoS attacks deplete the ability of a device to respond to normal/routine network probes, such as those related to a life-critical healthcare facility.
Distributed Denial of Service (DDoS)	DDoS attacks are more serious as compared to DoS attacks because in this case, the victim is targeted by a large number of machines (bots) making it tougher for the network gateway or border gateway firewall to detect and stop. A successful DDoS attack can make the device in particular and the network in general totally unable to perform its normal routine tasks.
Web Attacks	Since all IoT devices are part of a larger network, they do have an individual web component from where they are configured, operated, and hardened. This makes them vulnerable to a wide variety of web-based attacks, such as Remote Code Execution (RCE), Code/Command Injection, and Malicious File Inclusion. Successful execution of these attacks severely impacts the ability of the device to perform normally. Another major issue with web attacks is that they are not detected at the network gateway by the border firewall because they operate at the application layer of the TCP/IP stack. Therefore, a Web Application Firewall (WAF) is required to provide the appropriate protection. Most WAFs have their own issues because of their rule-based nature. They usually incorporate advanced techniques like deep learning for detecting web attacks (Shahid et al., 2022).

where, N, P, D, L, A are the Network factor, Protocol factor, Network design, Device Level, and Attack attributes, respectively. Note that, different weights can be assigned to the different factors. However, for simplicity reasons, in this paper, we assume that these factors impact the asset equally.

2.3 Risk Likelihood Evaluation ($\mathbb{S}$)

Apart from the direct threat to assets as a result of any cybersecurity issue, the likelihood or the probability of the vulnerability getting exploited and the threat getting materialized matters a lot. Therefore, to evaluate the likelihood of security risk to happen, we identify three parameters, namely device attack history (H), Device layer security (L), and Device criticality (C), which are explained in the following.

Device Attack History (H): This parameter is also important as it reflects the history of attacks that have taken place on a particular device. For instance, an IoT device in a healthcare facility might have been attacked multiple times over a certain span of time. A device that has been a victim of frequent attacks in history is highly likely to get affected once again.

Device Layer Security (L): Since IoT is a multi-layered architecture, where devices (network assets) operate at multiple layers, therefore the likelihood of attack varies significantly. For instance, resources at the perception layer are far less prone to attacks and eventual risks as compared to network resources at the network or the application layer. Similarly, the business layer is relatively safer, compared to the network layer. Hence, there is a need to relate the likelihood of an attack and eventual risk with the IoT layer as well.

Device Criticality (C): Moreover, the more critical the device, the more targeted it can be, and so its compromise can be more fatal as compared to other devices.

IoT devices in a healthcare environment, such as a pacemaker and an insulin pump, are way more critical, compared to blood pressure monitors and blood sugar checkers, because they directly affect human lives. Thus, their compromise would be detrimental to the entire organization's reputation.

Based on the aforelisted likelihood parameters, we propose to evaluate the risk likelihood for a given asset a, as shown in Equation 3.

$$\mathbb{S}_{\mathrm{a}} = (H+L+C)/3 \tag{3}$$

where, H, L, and C represent the device attack history, device layer security, and device criticality, respectively. Similarly, different weights can be assigned to different parameters. For simplicity reasons, in this paper, we assume that these factors impact the asset equally.

2.4 Attack Coverage (Number of IoT Devices)

In most real-world situations, risk impact and risk likelihood are not sufficient to evaluate the overall risk to an asset and an organization. This becomes more obvious when talking about IoT networks, where the number of connected devices is much higher than those in orthodox networks. Moreover, keeping in view the network attacks we discussed earlier (e.g., DDoS attack), the number of devices plays a crucial role in the magnitude of the attack.

2.4.1 Threshold (T)

We use the threshold to distinguish what the proper parameters are when evaluating the security risk. The threshold can be determined by system managers, security experts, or business owners. This can provide more flexibility when having many critical device profiles with very few device proportions in each profile, which is the case in almost all IoT systems (e.g., healthcare). In such a scenario, when the number of devices falls below the threshold, and the proportion of devices in each profile is used as a parameter to evaluate risk, the risk will not be accurate even if these devices are critical (heart monitor or insulin pump) and under a potential attack. Thus, we further elaborate on the importance of the number of devices as a parameter and threshold with the help of the following scenarios.

1. **Scenario 1:** Let us suppose a particular attack has taken place on any IoT device(s) that might not be critical enough. Moreover, the likelihood of the attack was also not very high. Under normal circumstances, such attacks will be ignored and their corresponding risks will not be catered for. But, what if the number of devices compromised as a result of such an attack is very high? In this scenario, such an attack cannot be ignored. Indeed, because the number of infected/compromised devices is so high, the corresponding risk needs to be taken seriously.
2. **Scenario 2:** Suppose that a single but crucial IoT asset in the organizational IoT network has been threatened/attacked through a mechanism whose likelihood is also very high. In this case, if the asset is isolated and not further spreading the attack by acting as a pivot point, then the overall magnitude of risk should not be as inflated as it appears to be when it is calculated through Equation 1.

Therefore, it is clear that the number of devices could accentuate the need to come up with yet another parameter, which is also important in contributing to the overall risk. We call this parameter *Attack Coverage*, as it conveys the number of affected/infected devices. Besides, it is important to normalize the ratio of devices by assigning them some weights so that the overall risk is uniformly evaluated across all IoT devices in the organizational network. The new risk formula after introducing the attack coverage (number of devices) is presented in Equation 4 and Equation 5, whereas Table 3 shows how device weights are assigned, with respect to their ratios.

$$\mathbb{R}_a = \mathbb{W}_a \times \mathbb{S}_a \times w_a \tag{4}$$

where, w_a represents the weight of the asset a.

Thus, the Risk to the asset a becomes now as shown Equation 5:

$$\begin{aligned}\mathbb{R}_a = \Big((N+P+D+L+A)/5\Big) \\ \times \Big((H+L+C)/3\Big) \times w_a\end{aligned} \tag{5}$$

Table 3: Device Weight Allocation through Ratio.

Device Ratio	Assigned Weights
60%	1
49% to 50%	0.7
20% to 39%	0.5
below 20%	0.2

Therefore, for each asset, the risk is evaluated and a score, between 0 and 1, is returned. The latter is then used to classify the risk into one of these categories: very low, low, medium, high, or very high, based on their criticality criteria presented in Table 4.

Table 4: Risk Ranges and Criticality.

Risk Values	Criticality
0.8 - 1.0	Very high
0.6 - 0.8	High
0.3 - 0.6	Medium
0.2 - 0.3	Low
0 – 0.2	Very low

3 CONCLUSION AND FUTURE WORK

The rapid growth of IoT creates new security risks for organizations. In order to evaluate these risks, organizations need to develop a Risk Assessment Framework for IoT as organizations have a dire need to focus their efforts on creating a comprehensive risk assessment framework for IoT. Such a framework should identify, assess, and respond to the potential risks of IoT, including the risk impact and its likelihood. This could include selecting an appropriate security architecture, conducting an assessment of the system, deploying protective controls, and regularly testing the security of the system.

In addition, organizations should also consider the physical security of IoT systems, as well as their ability to respond to any incidents. Organizations should also consider the specific needs of each IoT system, such as application-level security, authentication, authorization, and encryption.

Our risk assessment framework takes into account the key aspects of risk impact, likelihood impact, and the number of devices as well, which are the key contribution of the framework. The number of devices has a direct impact on the overall risk evaluation, as they are directly linked with the device threshold. Moreover, the proposed framework shows that the risk faced by an IoT device changes if the device threshold is modified.

In the near future, we are planning to validate the effectiveness and usability of the proposed framework on a simulated IoT-enabled healthcare system. We will then expand our testing to other scenarios, and ultimately test it with IoT datasets captured from real-world test beds.

REFERENCES

Bahizad, S. (2020). Risks of increase in the iot devices. In *2020 7th IEEE international conference on cyber security and cloud computing (CSCloud)/2020 6th IEEE international conference on edge computing and scalable cloud (EdgeCom)*, pages 178–181. IEEE.

Chen, B., Yang, Z., Zhang, Y., Chen, Y., and Zhao, J. (2020). Risk assessment of cyber attacks on power grids considering the characteristics of attack behaviors. *IEEE Access*, 8:148331–148344.

Datta, S. K. (2020). Draft-a cybersecurity framework for iot platforms. In *2020 Zooming Innovation in Consumer Technologies Conference (ZINC)*, pages 77–81. IEEE.

Jasour, A., Huang, X., Wang, A., and Williams, B. C. (2022). Fast nonlinear risk assessment for autonomous vehicles using learned conditional probabilistic models of agent futures. *Autonomous Robots*, 46(1):269–282.

Koohang, A., Sargent, C. S., Nord, J. H., and Paliszkiewicz, J. (2022). Internet of things (iot): From awareness to continued use. *International Journal of Information Management*, 62:102442.

Matheu, S. N., Hernandez-Ramos, J. L., Skarmeta, A. F., and Baldini, G. (2020). A survey of cybersecurity certification for the internet of things. *ACM Computing Surveys (CSUR)*, 53(6):1–36.

Matsuda, W., Fujimoto, M., Hashimoto, Y., and Mitsunaga, T. (2021). Cyber security risks of technical components in industry 4.0. In *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, pages 1–7. IEEE.

McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

Nurse, J. R., Creese, S., and De Roure, D. (2017). Security risk assessment in internet of things systems. *IT professional*, 19(5):20–26.

Oser, P., Feger, S., Woźniak, P. W., Karolus, J., Spagnuelo, D., Gupta, A., Lüders, S., Schmidt, A., and Kargl, F. (2020). Safer: Development and evaluation of an iot device risk assessment framework in a multinational organization. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(3):1–22.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., Maddox, L., and Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, 3(1):1–21.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., and Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in industry*, 102:14–22.

Raghuvanshi, A., Singh, U. K., and Joshi, C. (2022). A review of various security and privacy innovations for iot applications in healthcare. *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*, pages 43–58.

Razdan, S. and Sharma, S. (2022). Internet of medical things (iomt): overview, emerging technologies, and case studies. *IETE Technical Review*, 39(4):775–788.

Roy, P. P. (2020). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, pages 1–3. IEEE.

Samad, J., Reed, K., and Loke, S. W. (2018). A risk aware development and deployment methodology for cloud enabled internet-of-things. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 433–438. IEEE.

Shahid, W. B., Aslam, B., Abbas, H., Khalid, S. B., and Afzal, H. (2022). An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling. *Journal of Network and Computer Applications*, 198:103270.

Wang, B., Li, M., Jin, X., and Guo, C. (2020). A reliable iot edge computing trust management mechanism for smart cities. *IEEE Access*, 8:46373–46399.

Zhao, Y., Cheng, G., Duan, Y., Gu, Z., Zhou, Y., and Tang, L. (2021). Secure iot edge: Threat situation awareness based on network traffic. *Computer Networks*, 201:108525.