iJournals: International Journal of Software & Hardware Research in Engineering
ISSN:2347-4890, ijournals.in/ijshre
Volume 13 Issue 4, April 2025

Optimizing IoT Security for Hospital Applications

Authors: Mohd Ikram Husain[1], Ms Madhu[2], Dr Bassam Ali[3]

[1]M. Tech Student, Azad Institute of Engineering & Technology, Lucknow
[2]Profeesor, Azad Institute of Engineering & Technology, Lucknow
[3]Profeesor, RR Institute of engineering & Technology, Lucknow

ABSTRACT

This Paper contributes to the development of a structured and objective methodology for assessing and comparing IoT device security in healthcare environments. It also recommends security practices including network segmentation, biometric authentication, and the implementation of IT asset management (ITAM) solutions

The exponential adoption of Internet of Things (IoT) devices in the healthcare sector has revolutionized medical diagnostics, treatment, and patient monitoring. However, this connectivity introduces significant cyber security challenges due to the sensitive nature of the data involved and the heterogeneity of device architectures. This study investigates the critical security concerns in IoT-based healthcare systems, focusing on threats such as data breaches, unauthorized access, malware attacks, and vulnerabilities arising from inadequate device security. The research underscores the importance of protecting Confidentiality, Integrity, and Availability (CIA) of data, as healthcare data is highly valuable and regulated under strict compliance frameworks like HIPAA.

To systematically evaluate the security of IoT medical devices, the study proposes a Fuzzy Analytic Hierarchy Process (FAHP)-based multi-criteria decision-making model. This model integrates expert judgments to assess five key security attributes: confidentiality, integrity, availability, authentication, and authorization. Six device alternatives were analyzed using fuzzy logic to quantify subjective assessments and reduce bias. The results identified the most secure device alternative (D6) based on its highest closeness coefficient to the ideal security profile.

Keywords: IoT, Healthcare, Remote monitoring, protected health information (PHI)

1. INTRODUCTION

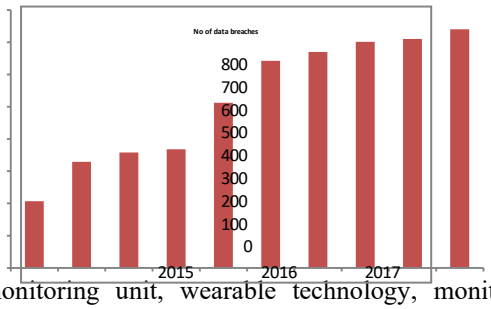
IoT systems are increasingly being linked to the Internet, doctor's office networks, as well as other IoT devices in order produce tools for improving health care as well as enhance healthcare professionals' power to cure patients. These same characteristics raise the possibility of cybers security risks. Healthcare systems, like some other software systems, could be vulnerable to unauthorized access, which can jeopardize the device's efficacy and safety. Potential threats cannot be completely eradicated, and lowering cybersecurity risks is particularly difficult. To effectively manage cybersecurity risks in the health care landscape, producers, hospitals, as well as infrastructure must collaborate. [1-5] Interconnected IoT devices as well as different mobile health (mHealth) technological advances have the capacity to change health care, and even though they could also be a platform that reveals patients as well as health care practitioners to safety and information security consequences such as being breached, infected with a virus, and susceptibletounauthorisedaccess.Patientsafetyconcerns,suchasharmordamage,area major concern due to networked healthcare industry security flaws; vulnerable IoT devices can also be utilized to target other parts of a network at the same time. The techniques and practices that preclude unauthorized users from gaining unauthorized access to or manipulate over IoT equipment as well as the information they produce are referred to as IoT device cyber security. IoT device cyber security can be thought of as a subset of IoT cyber security [6-8]. Moreover, there are some substantial variations among IoT security in broad sense as well as IoT

device cybersecurity in general and especially. The most significant distinction is that the data derived byor saved on IoT devices is frequently so private that it presents an especially significant danger [9].

It's one thing for an attacking player to gain access to ones IoT thermostat as well as gain knowledge that what temperature configurations users use; it's really quite another for a malicious actor to gain access to information about a patient's pulse rate as well as blood pressure, or to gain control of a IoT device implanted in a patient. Specific information could be applicable to HIPAA regulatory standards. Any health data that enables the patient to be identified is considered personally identifiable information (PII). Personally identifiable wellness information electronically stored is referred to as protected health information (PHI). Companies that are unable to secure such information may face penalties. IoT device security differs from IoT security in broad sense due to distinctions in how IoT device network's function, the consistency of IoT devices, as well as the complexity of implementing security fixes or software updates. Figure 1.1 illustrates the healthcare data breach report spanning from 2015 to 2024.

Figure1: Healthcare data breach report 2015 to 2024 (Source: HIPAA Journal)

Hundreds of network devices, which would include



monitoring unit, wearable technology, monitors, process flow, image processing, as well as patient data systems, are used in an usual hospital today. Such touchpoints provide several benefits for improved patient care; moreover, numerous IoT connected devices total absence robust security and could be used to gain access to the hospital's channel. In-home telehealth IoT equipment, like that usage to observe a patient's sugar levels or heart rate, are another prospective weak link. When information is wirelessly transmitted to health personnel via the open internet or perhaps a vulnerable Wi-Fi connectedness, the hospital's system becomes transiently susceptible to a cyberattack [14, 15].

1.1Reasons for Healthcare Security Issues:

Healthcare organizations are a popular target for cyber criminals for a variety of causes. Here are the five most important.

Healthcare data is valuable.

Patient data holds immense value in the healthcare industry. Healthcare organizations handle vast amounts of sensitive patient information, making their networks and smart devices prime targets for hacking attempts. According to IBM Security's annual survey, while the average cost of a data breach across all industries in 2020 was $3.86 million, the healthcare sector incurred the highest industry-average expense of $7.13 million. By investing in security interoperability, digitization, and response measures, healthcare professionals can significantly mitigate the risks of breaches, computer viruses, and costly non-compliance penalties from regulations such as HIPAA and the European Union's General Data Protection Regulation.

1.2 IoT devices are susceptible to hacking vulnerabilities.

The large network of interconnected IoT equipment of differing standards and producers creates security upkeep particularly difficult for IoT IT specialists. Whilst also IoT equipment do not always store massive volumes of patient information, they could be used by intruders to gain access to data-rich data centers. To lower transaction expenses and destruction caused by unauthorised access, the IoT industry should keep these points of entry up to date as well as protected.

1.3 Lack of sufficient education among healthcare staff regarding data security risks.

Cybersecurity threats on IoT equipment could be hazardous, even fatal. In September 2020, a ransomware threat disrupted the intake of new patients as well as forced sick patients to be rerouted. Whereas the hospital worked to restore solutions, few death occurred. Everybody in the healthcare organisation is a participant of the security team because they have access to linked equipment as well as networks that store susceptible patient data. That is why, in order to prevent unauthorised access to private information, user and the staff must adopt a zero-trust authentication scheme.

1.4 Patient data is shared with multiple healthcare providers through remote means..

Telemedicine as well as collaborative effort among healthcare doctors have greatly increased the patient's chances of receiving the highest quality of care. Moreover, safeguarding patient information in a virtual space is becoming increasingly difficult. To recognise and confer access to authorised individual people across devices as well as locations, numerous companies are leveraging multifactor as well as risk-based verification mechanisms. Predicated on suspicious behaviour, IT supervisors can increase the rigour of the verification process.

1.5 Smaller healthcare organizations are easier targets.

Because major hospital organisations hold the much more patient data, they are the most precious targets for potential attacks. Smaller companies, on the other hand, have very few assets to devote to cybersecurity, trying to make them much easy pickings for cybercriminals. If ones practise is a small one with few resources, they should concentrate the cyber resilience on governance, risk assessment, and statutory requirements. Individuals can safeguard the patients' information in the cloud settings, tremendously reducing the sophistication of IT and security that your company is accountable for, because cloud technology companies frequently manage software updates and security preservation. Endpoint controls, as well as identity as well as access management, are used to defend and maintain IoT equipment, as well as to guarantee wireless connectivity.

2. PROPOSE METHODOLOGY

2.1 Hierarchy for the Evaluation

IoT device therapeutic approaches are now becoming crucially influential, entering new markets throughout the world as well as offering technological breakthroughs in preventative medicine for a variety of diseases. Furthermore, of that kind approaches may pose both consistent as well as unprecedented risks, with immediate life-threatening consequences in some instances.

Table 1 offers a concise summary of the numerous factors employed throughout the assessment procedure for IoT device protection.

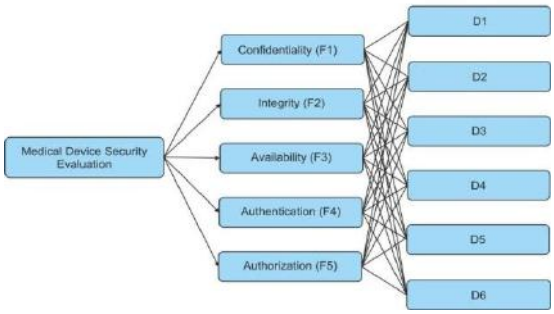


Figure2: Structural Diagram for Assessing Security of IoT devices

2.2 Fuzzy AHP Method

Multiple-criteria decision-making (MCDM) as well as multiple-criteria decision analysis (MCDA)is indeed an efficiency measurement sub-discipline which expressly analyses multiple contrasting criteria in planning process. In thoroughly reviewing, contradictory criteria are common: cost or product cost is generally one of the key requirements, as well as some quality measure is generally another criterion, quickly at odds with the cost. Cost, convenience, safety, as well as fuel efficiency could represent some of the key requirements we think about when buying a car - it is strange for the cheapest model tobe the most pleasant as well as safest. Managers in asset management want to maximise returns while minimising risks; even so, stocks with the potential for high returns generally pose a significant risk of incurring losses. Customers' satisfaction as well as the expense of providing facility are fundamentally opposing characteristics in the hospitality industry. Generally people weigh set of criteria tacitly in their everyday routines as well as may be content with the implications of such decisions taken solely on empiricism.

Whenever the implications are high, however, it is critical to properly construct the challenge and expressly examine different criteria. In addition to the extremely complicated issues involving numerous criteria in deciding whether or not construct a nuclear electricity plant, however there are also various parties who really are seriously influenced by the implications.

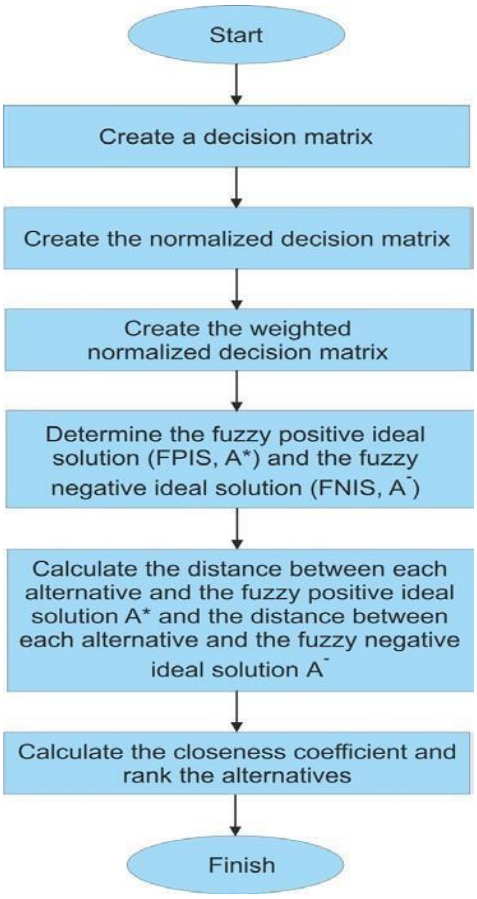


Figure3: Flowchart of Fuzzy AHP

3. RESULT ANALYSIS

The alternative options are assessed based on multiple attributes, and the results of the decision matrix are presented below. It should be noted that if multiple qualified professionals are involved in the evaluation, Table 4.1 displays the arithmetic mean of their assessments.

Table1: Decision Matrix

	F1	F2	F3	F4	F5
D1	(4.378,6.378, 8.378)	(4.156,6.156, 7.578)	(4.733,6.733, 7.978)	(3.844,5.844, 7.311)	(3.533,5.489, 7.178)
D2	(3.756,5.711, 7.400)	(4.022,6.022, 7.578)	(3.800,5.800, 7.267)	(3.933,5.933, 7.444)	(3.667,5.667, 7.356)
D3	(3.756,5.711, 7.622)	(4.333,6.333, 7.800)	(4.200,6.111, 7.578)	(4.333,6.333, 7.622)	(4.156,6.111, 7.622)
D4	(3.711,5.622, 7.356)	(4.022,6.022, 7.711)	(3.933,5.933, 7.622)	(4.067,6.067, 7.667)	(4.067,6.067, 7.844)
D5	(4.111,6.111, 7.711)	(3.889,5.889, 7.400)	(4.111,6.111, 7.756)	(3.711,5.711, 7.311)	(4.244,6.244, 8.022)
D6	(4.911,6.867, 8.289)	(4.822,6.822, 8.111)	(5.178,7.178, 8.200)	(5.133,7.133, 8.200)	(5.000,7.000, 8.156)

$$r_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right) \quad ; \quad c_j^* = \max_i c_{ij} \; ; \text{Positive ideal solution}$$

$$\blacklozenge_{ij} = \left(\frac{a_{ij}^-}{c_{ij}}, \frac{a_{ij}^-}{b_{ij}}, \frac{a_{ij}^-}{a_{ij}}\right) \quad ; \quad a_j^- = \min_i a_{ij} \; ; \text{Negative ideal solution}$$

The following Table4.2 depicts the normalized decision matrix.

Table 2: A normalized decision matrix

	F1	F2	F3	F4	F5
D1	(0.523,0.761, 1.000)	(0.512,0.759, 0.934)	(0.577,0.821, 0.973)	(0.469,0.713, 0.892)	(0.433,0.673, 0.880)
D2	(0.448,0.682, 0.883)	(0.496,0.742, 0.934)	(0.463,0.707, 0.886)	(0.480,0.724, 0.908)	(0.450,0.695, 0.902)
D3	(0.448,0.682, 0.910)	(0.534,0.781, 0.962)	(0.512,0.745, 0.924)	(0.528,0.772, 0.930)	(0.510,0.749, 0.935)
D4	(0.443,0.671, 0.878)	(0.496,0.742, 0.951)	(0.480,0.724, 0.930)	(0.496,0.740, 0.935)	(0.499,0.744, 0.962)
D5	(0.491,0.729, 0.920)	(0.479,0.726, 0.912)	(0.501,0.745, 0.946)	(0.453,0.696, 0.892)	(0.520,0.766, 0.984)
D6	(0.586,0.820, 0.989)	(0.595,0.841, 1.000)	(0.631,0.875, 1.000)	(0.626,0.870, 1.000)	(0.613,0.858, 1.000)

$$A^* = \{v_1^*, v_2^*, \ldots, v_n^*\} = \max_j v_{ij} \mid i \in B, \min_j v_{ij} \mid i \in C$$

$$A^- = \{v_1^-, v_2^-, \ldots, v_n^-\} = \min_j v_{ij} \mid i \in B, \max_j v_{ij} \mid i \in C$$

Where v_i^* is the top-most value of i for all the alternatives and also v_1^- is the lowest value of i for all the alternatives. B and C portray the positive as well as negative ideal solutions, respectively.

Table 3: The weighted normalized decision matrix

	F1	F2	F3	F4	F5
D1	(0.105,0.152,0. 200)	(0.102,0.152,0. 187)	(0.115,0.164,0. 195)	(0.094,0.143,0. 178)	(0.087,0.135,0. 176)
D2	(0.090,0.136,0. 177)	(0.099,0.148,0. 187)	(0.093,0.141,0. 177)	(0.096,0.145,0. 182)	(0.090,0.139,0. 180)
D3	(0.090,0.136,0. 182)	(0.107,0.156,0. 192)	(0.102,0.149,0. 185)	(0.106,0.154,0. 186)	(0.102,0.150,0. 187)
D4	(0.089,0.134,0. 176)	(0.099,0.148,0. 190)	(0.096,0.145,0. 186)	(0.099,0.148,0. 187)	(0.100,0.149,0. 192)
D5	(0.098,0.146,0. 184)	(0.096,0.145,0. 182)	(0.100,0.149,0. 189)	(0.091,0.139,0. 178)	(0.104,0.153,0. 197)
D6	(0.117,0.164,0. 198)	(0.119,0.168,0. 200)	(0.126,0.175,0. 200)	(0.125,0.174,0. 200)	(0.123,0.172,0. 200)

4. CONCLUSION

The present healthcare system has become increasingly digitized, providing more accessibility than ever before. This transformation has led to substantial advantages for both patients and healthcare providers. When patient information is maintained electronically, health professionals can quickly access and update accurate records. The improved efficiency of treatment that this enables can save lives, as well as organizations around the world are doing every thing they can to ensure that their advanced technologies establish at the very same speed as the business as a whole. Furthermore, there are significant challenges as well as intimidations, as with any incredibly quickly digital transformation process. Technological advancements, in specific, bring with them fresh

safety issues. Health care system and other infrastructure must make substantial investment opportunities in secure information managerial initiatives, with trained and experienced group members in charge of putting such procedures into practice.

Development without protection is a risky proposition, and the fact that healthcare institutions collect so much confidential information tries to amplify this in the health sector. People should be anticipated to comprehend as well as impose industry-specific data security suggestions influencing health practitioners, as well as go beyond and above some these minimum requirements to demonstrate cutting-edge data security techniques, in order to participate in secure healthcare information preparation. While acquiring on IoT data security appears to be a difficult task, it's also correct that generally contains would then be on the rise for several generations to come. Individual people may become an essential component of a firm's related to the management procedures group by having taken on such roles and responsibilities.

References

[1]T. Yaqoob, H. Abbasand and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3723-3768, 2019.

[2]K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," Symmetry, vol. 12, no. 6, pp. 1770-1792, 2020. 36

[3]A. Algarni, M. Ahmad, A. Attaallah, A. Agrawal, R. Kumar et al., "A hybrid fuzzy rulebased multi-criteria framework for security assessment of medical device software," International Journal of Intelligent Engineering and Systems, vol. 13, no. 5, pp. 51-62, 2020.

[4]A. Algarni, A. Attaallah, M. Ahmad, A. Agrawal, R. Kumar et al., "A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system," International Journal of Advanced Computer Science and Applications, vol. 11, no. 1, pp. 481-489, 2020.

[5]C. Bresch, S. Chollet and D. Hely, "Towards an inherently secure run-time environment for medical devices," in Proc. IEEE International Congress on Internet of Things, San Francisco, USA, pp. 140-147, 2018. [Online]. Available: https://hal.archivesouvertes.fr/hal-01898660.

[6]N. Christoulakis, G. Christou, E. Athanasopoulos and S. Ioannidis, "HCFI: hardwareenforced control-flow integrity," in Proc. Sixth ACM Conference on Data and Application Security and Privacy, New York, NY, USA, 38–49, 2016. DOI: https://doi.org/10.1145/2857705.2857722.

[7]A. I. Newaz, A. K. Sikder, L. Babunand and A. S. Uluagac, "HEKA: a novel intrusion detection system for attacks to personal medical devices," in Proc. 2020 IEEE Conference on Communications and Network Security, Avignon, France, pp. 1-9, 2020. DOI: 10.1109/CNS48642.2020.9162311.

[8]L. Zhou and Y. Makris, "HAFIX: hardware-assisted flow integrity extension," in Proc. 52nd Annual Design Automation Conference, San Francisco, CA, USA. pp. 1550-1555, 2015. [Online]. Available: https://dl.acm.org/doi/10.5555/3130379.3130740.

[9]S. Gao and G. Thamilarasu, "Machine-learning classifiers for security in connected medical devices," in Proc. 2017 26th International Conference on Computer Communication and Networks, Vancouver, BC, Canada, pp. 1-5, 2017. DOI: 10.1109/ICCCN.2017.8038507.

[10] D. Halperin, T. S. H. Benjamin, B. Ransford, S. S. Clark, B. Defend et al., "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 129-142, 2008. DOI: 10.1109/SP.2008.31.

[12] C. Li, A. Raghunathan and N. Jha, "Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system," in Proc. 2011IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, pp. 150–156, 2011. DOI: 10.1109/HEALTH.2011.6026732.

[13] H. Almohri, L. Cheng, D. Yao and M. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in Proc. IEEE/ACM International Conference on Connected Health: Applications, System, Philadelphia, PA, USA, pp. 114-119, 2017. DOI: 10.1109/CHASE.2017.69.

[14] Confickered! Medical Devices and Digital Medical Records are Getting Hacked. MassDevice, 2009. [Online]. Available: https://www.massdevice.com/confickered-medicaldevices-and-digital-medical-records-are-getting-hacked/.

[15] NoMoreClipboard Notice to Individuals of a Data Security Compromise. Business Wire, 2015. [Online]. Available: https://www.businesswire.com/news/home/20150610005964/en/NoMoreClipboard-Noticeto-Individuals-of-a-Data-Security-Compromise.

[16] Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. GAO: U. S. Government Accountability Office, 2012. [Online]. Available: https://www.gao.gov/products/GAO-12-816.

[17] FDA's Role in Regulating Medical Devices. U. S. Food & Drug Administration, 2018. [Online]. Available: https://www.fda.gov/medical-devices/home-use-devices/fdas-roleregulating-medical-devices.

[18] Y. Xu, D. Tran, Y. Tian and H. Alemzadeh, "Poster abstract: analysis of cyber-security vulnerabilities of interconnected medical devices," in Proc. 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, Arlington, VA, USA, pp. 23-24, 2019. DOI: 10.1109/CHASE48038.2019.00017.

[19] W. Alhakami, A. Baz, H. Alhakami, M. Ahmad, R. A. Khan, "Healthcare Device Security: Insights and Implications," Intelligent Automation and Soft Computing, vol. 27, no. 2, pp. 409-424. 2020.

[20]T. Bonaci, J. Yan, J. Herron, T. Kohnoand and H. J. Chizeck, "Experimental analysis of denial-of-service attacks on tele operated robotic systems," in Proc. ACM/IEEE Sixth International Conference on Cyber-Physical Systems, New York, NY, USA, pp. 11–20, 2015. DOI: https://doi.org/10.1145/2735960.2735980.

[21]A. Rayand and C. Rance, "An analysis method for medical device security," in Proc. Symposium and Bootcamp on the Science of Security, New York, NY, USA, Article 16, pp. 1–2, 2014. DOI: