INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 9.47]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 10, Issue - 1, January - 2024

DOIs:10.2015/IJIRMF/202401027 --:-- Research Paper / Article / Review

IoT Security Performance Evaluation in Healthcare System

Dr. Priyanka D. Halle
Assistant Professor,
Department of Information Technology, SKNSITS, Lonavala, Maharashtra, India
Email - hallepriyanka2011@gmail.com

Abstract: *Revolutionary improvements in patient care have been made possible by the integration of Internet of Things (IoT) technology into healthcare systems, enabling effective and individualised healthcare services. This survey study report explores the field of IoT applications in healthcare, with an emphasis on how they might improve patient care. The many uses of IoT in healthcare systems are consolidated in this research by examining previous research studies and real-world applications. The first section of the article explains how the IoT is revolutionising patient care through data-driven decision-making, personalised therapy, and remote monitoring. The many IoT devices, sensors, and systems used in the healthcare sector to track vital signs, manage chronic illnesses, and improve the delivery of healthcare are described in detail in a thorough literature analysis. From a methodological standpoint, this study employs an inclusive approach, covering a broad range of IoT applications in various healthcare fields, including telemedicine, wearable devices, smart healthcare infrastructure, and ambient assisted living. Through this comprehensive study, we evaluate the impact of IoT technology on patient care and highlight the effectiveness of IoT technology in improving diagnostic accuracy, treatment outcomes, and patient engagement. This paper also explores the challenges and ethical considerations associated with widespread adoption, security, interoperability, and regulatory compliance. Methodologically, this review adopts a structured approach to evaluate the performance of IoT-enabled healthcare systems in various areas, such as remote patient monitoring, predictive analytics, smart medical devices, and healthcare infrastructure. It inspects key performance indicators (KPIs) such as data accuracy, reliability, latency, scalability, interoperability, and cost efficiency. Finally, this paper summarises the current state of IoT applications in healthcare systems, highlights the transformative potential to improve patient care, and identifies future research avenues for continued innovation and integration of IoT technologies to further optimise healthcare services and ultimately promote patient-centred care in a connected healthcare ecosystem.*

Key Words: *IoT, Healthcare system, Performance analysis, Security.*

1. INTRODUCTION:

Assessing the security performance of IoT in healthcare systems involves evaluating the effectiveness of security measures implemented to safeguard patient data, ensure device integrity, and protect against cyber threats. Security concerns in IoT-constructed healthcare systems are paramount due to the confidentiality of patient data and the interconnected nature of medical devices. As highlighted by Khan et al. (2018), the integration of various IoT devices, such as wearables, sensors, and medical equipment, in healthcare environments introduces significant security challenges. Vulnerabilities in these devices can lead to data breaches, unauthorized access, and potentially life-threatening consequences for patients. The paper emphasizes the need for robust security measures to safeguard patient information, ensure device integrity, and protect against cyber threats in IoT-based healthcare systems [1]. In addition, the complexity of security and privacy issues related to IoT is highlighted by Mohamed et al. (2018). The paper emphasizes the need for comprehensive security measures to address vulnerabilities in healthcare IoT systems and protect patient privacy and medical data from attacks.[2].

Patient data and the interconnectivity of medical devices are among the most sensitive areas of security concern in IoT-based health systems. The integration of various IoT devices, such as wearables and medical sensors, as well as connected medical equipment creates a heterogeneous attack surface that is vulnerable to a variety of security threats. In the paper Yadav (2019) highlights the urgent need for strong security measures to safeguard patient information, protect device integrity, and reduce the risk of cyber-attacks in IoT enabled healthcare environments [3]. IoT security

performance entails displaying the different tiers, parts, protocols, and security controls put in place to protect an IoT ecosystem. An explanation of the parts: [4]

- Device Layer: This layer consists of Internet of Things (IoT) devices that gather and send data, including wearables, actuators, sensors, and other smart devices. Every gadget has embedded systems, communication modules, and sensors.
- The communication layer controls how data is sent between Internet of Things devices and gateways or the cloud. For data exchange, it uses protocols like MQTT, CoAP, or HTTP. To ensure communication security, it may also use authentication and encryption techniques. In between IoT devices and the cloud, gateway/edge computing serves as a middleman, aggregating data, preprocessing it, and putting security measures like encryption, intrusion detection, and firewalls in place.
- Cloud Services: This layer consists of cloud platforms that store, process, and analyse data produced by Internet of Things devices. Applications, databases, and servers are all part of it. This place uses security features including encryption, access limits, and recurring security audits.
- Security Protocols and Measures: A variety of security protocols and measures are implemented across the whole Internet of Things ecosystem.

1. Authentication and Authorization: Techniques to guarantee that the system is only accessible by approved people or devices.
2. Data Encryption: Methods to protect data from unwanted access by encrypting it both during transmission and storage.
3. Integrity checks: Procedures to confirm the accuracy of data and make sure it hasn't been altered.
4. Tools for monitoring and filtering network traffic in order to identify and stop such attacks include firewalls and intrusion detection/prevention systems (IDS/IPS).
5. Patch management and security updates: Frequent updates and patches are applied to software and hardware vulnerabilities.
6. Security Guidelines and Adherence: compliance with legal requirements (such as GDPR and HIPAA) and security policy implementation.

2. LITERATURE REVIEW:

Research on IoT cloud-based e-health systems has produced effective security protocols that offer complete frameworks with crucial software components to guarantee reliable and safe data transfer between devices. Apart from privacy and security, cloud based IoT E-health efficiency is another factor that must be considered when designing systems, allowing for the easy analysis and transmission of any amount of data without the need for additional delay caused by existing solutions. Data confidentiality, data integrity, service availability, accountability, authentication, access control, and non-repudiation make up the majority of crucial privacy and security elements for IoT-cloud-based e-health systems. While a number of studies have examined the security and privacy concerns of IoT-cloud-based e-health systems with different integrated implementations, a more thorough examination of these issues has necessary [5].

System-level vulnerabilities including memory modules, system apps, and architectural faults in a healthcare system are the direct targets of system-level assaults. Attackers may use these flaws to obtain sensitive data access and unapproved control. A healthcare system may be subjected to one of two main categories of system-level attacks. These are attacks on healthcare equipment that leverage weak authentication schemes and escalate privileges [6].

The security and privacy concerns of such sensing systems are frequently disregarded, despite the possibility that such widely available and inexpensive sensors may replace the reactive healthcare system currently in place with preventative treatment. Medical devices must be extremely secure, as they collect and handle extremely sensitive personal health data, compromising the privacy of the user. This security extends to the related communications on the devices. Nevertheless, the computational capability of the downsized IoMT devices is quite restricted, and only a small number of security techniques can be implemented in them [7].

The topic of research that deals with protecting linked IoT devices and systems is known as IoT security. The security hierarchy of the IoT's demonstrates how different security methods may be used at different levels. To achieve safe network interconnection, the network layer primarily focuses on network environment security technologies like firewalls, secure routing, wireless network security. The application layer, on the other hand, uses user authentication and access control to guarantee the security of the application system. Due to its high susceptibility to increasingly complex security threats, the sensory layer mostly employs attack detection and intrusion response strategies to thwart unauthorised intrusions. Among the most important IoT security issues are availability, confidentiality, integrity, and authentication [8].

Based on literature review, it is important to stress that traditional cyber security criteria only include preventative and defensive measures for healthcare IoT systems; they are not designed to address the majority of vulnerabilities and assaults. While medical sensors and IoT devices are embedded in uncontrolled and open settings with unknown and untrusted actors, they could only be successful in defending against known threats. As a result, associated to other businesses, security concerns and hazards in healthcare systems are far more complex [9].

IoT-based healthcare will use cloud technology to solve the storage issue. Because of its extreme capacity, the cloud environment can handle large amounts of data and do analyses on them with easy. As a result, machine learning is being utilised to secure cloud data and machine learning-based cloud-based IoT-Healthcare will be completely reliable [10].

Blockchain has recently been used to develop new technologies, such Internet of Things-based security and public services. Businesses also employ blockchain because of its high security and dependability to draw in clients. Furthermore, because blockchain operates in a distributed context, it is immune to the single point of failure problem. Blockchain is mostly utilised in smart cities, which are made up of several IoT devices dispersed around the city. Scalability, efficiency, robustness, time effectiveness, and computational cost-effectiveness are all improved by integrating blockchain with IoT's technologies. The data produced by IoT can be kept in a blockchain that is controlled by servers in the cloud [11].

WSN provides communication capabilities, sensor devices are utilised to gather data and the gathered data should be secure. The algorithms process the gathered data in order to carry out the required analysis. In addition, cloud services provide access to users, including medical professionals and patients, and storage for the gathered data. In order to enhance patient outcomes, IoT healthcare apps must be secure and secured, taking into account not just the dangers to patients' privacy and security, but also additional consequences including financial risks and privacy breaches [12].

Four general groups can be used to categorize attacks against IoT-based systems. The first category is called a physical attack since the attacker physically enters the network and tries to start malicious processes inside the system. Malicious code injection, side-channel attacks, radio frequency signal jamming, and Internet of Things device tampering are examples of common physical assault techniques. When it comes to IoT device authentication, researchers use the physical unclonable function (PUF). One of the PUF's greatest features is that its precise microstructure can never be duplicated. Attackers try to manipulate the Internet of Things through two different types of attacks: network attacks and spear attacks. Without being physically close to the network, an attacker can still initiate an attack [13].

3. SECURITY PERFORMANCE ASSESSMENT OF IOT IN HEALTH CARE SYSTEM :

A healthcare system has gained significant importance recently due to its potential to enable innovative and creative solutions, or as a novel and fascinating topic for information gathered across various domains, as demonstrated by the study of radio frequency identification (RFID) and wireless medical sensor networks (WMSN). The WMSN monitoring system may track the patient's health and wirelessly transmit this data to a nearby workstation by using an RFID body sensor. Sensitive data should undoubtedly be protected before outsourcing due to privacy regulations, which renders outdated data usage methods like keyword-based document retrieval.

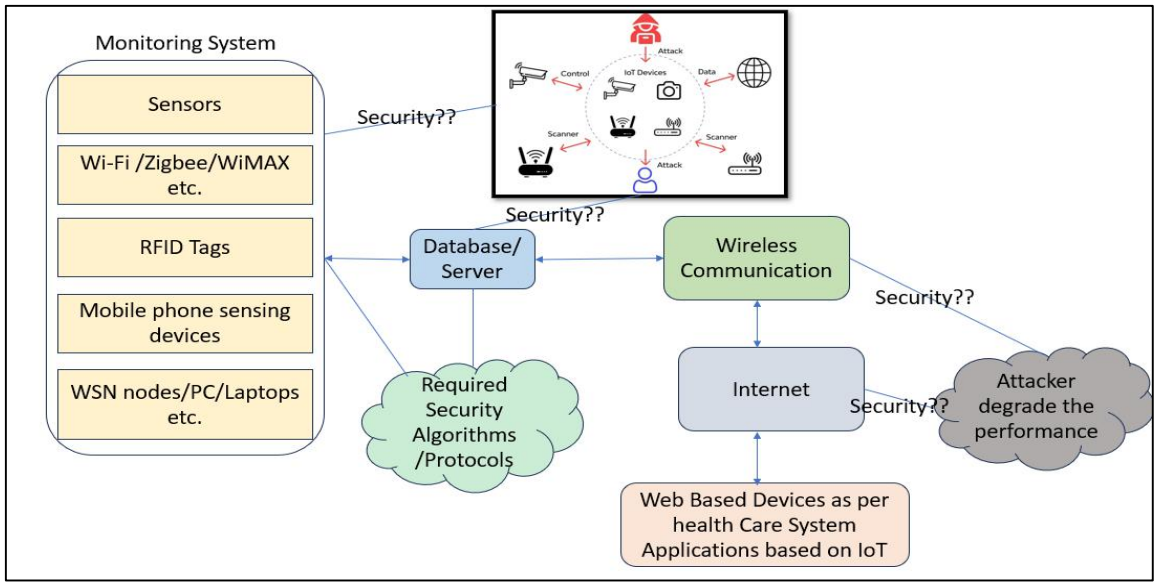

Figure 1 : Potentiel Points for Attack on IoT in Healthcare System

Figure 1 shows potential points of attack for IoT systems based in healthcare. The possibility of security and privacy problems has grown in tandem with the ease with which personal information is now accessible. Furthermore, one of the primary problems with remote patient monitoring systems is still getting the data to its destination safely and granting the authorised physician access to the patient's information [14,15]. The monitoring and care of patients have been transformed by the introduction of IoT devices into healthcare systems. But this technical progress also brings with it hitherto unheard-of security threats. The purpose of this research study is to locate and examine possible attack points in IoT frameworks used by healthcare organisations. IoT device vulnerabilities, including those in wearable health monitors, medical implants, and hospital equipment, are investigated through a thorough examination of the literature that has already been published.

Additionally, this study looks at the possible dangers and methods of attack that might be used against IoT devices in the healthcare industry, such as denial-of-service assaults, unauthorised access, data breaches, and device manipulation. This study is used in the paper's proposal of practical mitigation tactics and countermeasures, which required to highlights the significance of strong security protocols and encryption approaches. Innovative algorithmic techniques that are tailored to meet the particular security needs of IoT devices in healthcare include homomorphic encryption, lightweight encryption, blockchain-based authentication, and machine learning-assisted anomaly detection. Additionally, more study required to assesses the viability, computational cost, and performance of putting these algorithms into practice within IoT devices with limited resources while upholding strict security guidelines. In order to mitigate possible cyber risks and protect patient privacy in IoT-enabled healthcare systems, the suggested algorithms seek to strengthen the confidentiality, integrity, and availability of healthcare data [15,16,17].

4. CONCLUSION:

A comprehensive analysis of security performance in healthcare applications reveals both promising improvements and critical challenges. The evaluation highlights the key findings in IoT technology offers unprecedented opportunities for improving patient care and medical services delivery, but its integration also introduces vulnerabilities that require urgent attention. Risks to patient privacy and data integrity include security breaches, unauthorized access and data integrity threats. It is essential to implement robust security measures specifically designed for healthcare IoT ecosystems, such as encryption protocols, authentication mechanisms and anomaly detection systems. In addition, the evaluation highlights the need for balance between security and device performance and usability, as resource-limited IoT devices require light encryption and authentication protocols to ensure data protection without sacrificing operational efficiency. Regulatory compliance and compliance with healthcare standards are essential for building trust between patients, healthcare providers and stakeholders, while maintaining legal and ethical standards to protect patient information and maintain compliance with HIPAA and GDPR regulations.

REFERENCES:

Journal Papers:

1. Khan, Shafiullah, et al. (2018) "A Comprehensive Survey on Security and Privacy in Healthcare Internet of Things." IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1961-1990.
2. Mohamed, A. A., Guizani, M., Otrok, H., et al. (2018) "Security and Privacy in Internet of Medical Things (IoMT): Challenges and Solutions." IEEE Network, 32(6), 4-12.
3. Yadav, P., Gaur, M. S., & Buyya, R. (2019). "Security and Privacy Issues in IoT-Based Healthcare: A Comprehensive Survey." IEEE Access, 7, 18116-18137.
4. D. Singh, G. Tripathi and A. J. Jara, (2014)"A survey of Internet-of-Things: Future vision, architecture, challenges and services," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South), pp. 287-292, doi: 10.1109/WF-IoT.2014.6803174.
5. Amaraweera, S. P. and Halgamuge, M. N. (2019) “Internet of things in the healthcare sector: overview of security and privacy issues,” in Mahmood, Z. (ed), Security, privacy and trust in the iot environment, Cham, Springer International Publishing, pp. 153–179 [Online]. DOI: 10.1007/978-3-030-18075-1_8.
6. Butpheng, C., Yeh, K.-H. and Xiong, H. (2020) “Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review,” Symmetry: Culture and Science, vol. 12, no. 7, p. 1191 [Online]. DOI: 10.3390/sym12071191.
7. Chanal, P. M. and Kakkasageri, M. S. (2020) “Security and privacy in iot: A survey,” Wireless Personal Communications, vol. 115, no. 2, pp. 1667–1693 [Online]. DOI: 10.1007/s11277-020-07649-9.
8. Das, D. (n.d.) “Extensive Survey on Cloud-based IoT-Healthcare and Security using Machine Learning,.”

9. Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S. and Amin, R. (2021) "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey," Security and Communication Networks, vol. 2021, pp. 1–21 [Online]. DOI: 10.1155/2021/7142048.
10. El Zouka, H. A. and Hosni, M. M. (2021) "Secure IoT communications for smart healthcare monitoring system," Internet of Things, vol. 13, p. 100036 [Online]. DOI: 10.1016/j.iot.2019.01.003.
11. Halle, P. D. and Shiyamala, S. (2022) "Secure advance metering infrastructure protocol for smart grid power system enabled by the Internet of Things," Microprocessors and microsystems, vol. 95, p. 104708 [Online]. DOI: 10.1016/j.micpro.2022.104708.
12. Imran, M., Zaman, U., Imran, Imtiaz, J., Fayaz, M. and Gwak, J. (2021) "Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions," Electronics, vol. 10, no. 20, p. 2501 [Online]. DOI: 10.3390/electronics10202501.
13. López Martínez, A., Gil Pérez, M. and Ruiz-Martínez, A. (2023) "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," ACM Computing Surveys, vol. 55, no. 12, pp. 1–38 [Online]. DOI: 10.1145/3571156.
14. Nasiri, S., Sadoughi, F., Tadayon, M. H. and Dehnad, A. (2019) "Security Requirements of Internet of Things-Based Healthcare System: a Survey Study.," Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina : casopis Drustva za medicinsku informatiku BiH, vol. 27, no. 4, pp. 253–258 [Online]. DOI: 10.5455/aim.2019.27.253-258.
15. Newaz, A. I., Sikder, A. K., Rahman, M. A. and Uluagac, A. S. (2021) "A survey on security and privacy issues in modern healthcare systems," ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 1–44 [Online]. DOI: 10.1145/3453176.
16. Sun, Y., Lo, F. P.-W. and Lo, B. (2019) "Security and privacy for the internet of medical things enabled healthcare systems: A survey," IEEE access: practical innovations, open solutions, vol. 7, pp. 183339–183355 [Online]. DOI: 10.1109/ACCESS.2019.2960617.
17. Usak, M., Kubiatko, M., Shabbir, M. S., Viktorovna Dudnik, O., Jermsittiparsert, K. and Rajabion, L. (2020) "Health care service delivery based on the Internet of things: A systematic and comprehensive study," International Journal of Communication Systems, vol. 33, no. 2, p. e4179 [Online]. DOI: 10.1002/dac.4179.