International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

A Review of Cybersecurity Framework for IoT-Enabled Healthcare Applications

Niyati Agarwal[1], Deepshikha[2]

[1]Master of Technology, Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India
[2]Assistant Professor, Department of Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India

---

Abstract - *The integration of Internet of Things (IoT) technologies into the healthcare system has led the patient care system to rapidly integrate in real time, personalized care, reduced efficency. There is no doubt that the proliferation of IoT-enabled healthcare applications poses significant cybersecurity risks that have brought sensitive patient data, as well as, critical medical infrastructure under the attack of an increasing number of cyber threats, however. In this review paper, this current landscape of cybersecurity frameworks for IoT enabled healthcare applications are explored in terms of their strengths and limitations, and this applicability for addressing safety and security of healthcare applications. Using insights from the threat landscape, common vulnerabilities and attack vectors, we analyze existing frameworks such as NIST, HIPAA, HITRUST, and discuss why they present gaps in protecting healthcare IoT ecosystems. Additionally, we offer important building blocks to a robust cybersecurity framework targeting risk assessment, data protection, device security, network security, plus incident response. Additionally, we discuss some of the emerging technologies including blockchain, artificial intelligence and edge computing as possible enablers of enhanced security. We then outline future research directions and challenges, especially interoperability, the need for lightweight security solutions, and regulatory compliance. Among other objectives, the purpose of this paper is to provide an exhaustive work of a reservoir of resources from which researchers, healthcare providers and policymakers are able to develop and implement dynamic security strategies for the use of IoT in healthcare applications so as to guarantee the security, privacy and trustworthiness of these disruptive technologies.*

Key Words: Internet of Things (IoT), Healthcare IoT (IoHT), Threat Landscape, Risk Assessment, Smart Healthcare Systems, Cybersecurity Challenges, IoT-Enabled Healthcare Application.

1.INTRODUCTION

1.1.Background

The Internet of Healthcare Things (IoHT), a broadly used term for healthcare under Internet of Things (IoT), helped bringing in changes in the delivery and management of medical services. In the context of the IoT enabled healthcare applications, the data collected and communicated with the use of interconnected devices, sensors, and systems is usually transmitted in real time [1]. With this technological advancement, there has been creation of tailor made solutions like remote patient monitoring, wearable health wearable and devices smart hospitals which improve patient care, enhance operational efficiency and reduce healthcare cost. For example, health monitoring wearable devices (e.g., fitness tracker, glucose monitor) and smart medical devices (e.g., infusion pump, pacemaker) facilitate continuous health monitoring and serve as a critical resource for patients with chronic diseases. There is no doubt that IoT is very important for healthcare. Providing these healthcare provider with the capability to deliver proactive and personalized care, here they are able to detect problems early and intervene quickly. Additionally, IoT applications provide a way for easy communication between patients and healthcare professionals, overcoming geographical boundaries and increasing the accessibility of care, especially in remote and unreached areas [2]. The equipment in IoT enabled smart hospitals is optimized for efficient and streamlined workflows, automated processes and efficient allocation of resources to create a better and enhanced patient experience.

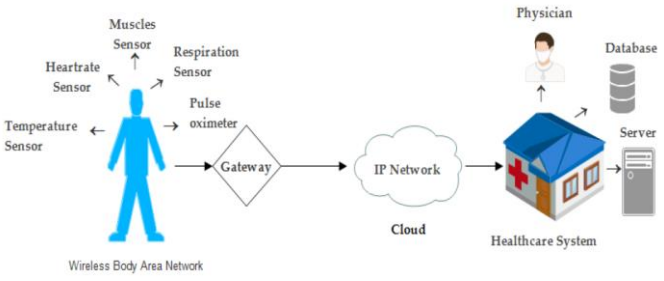

Figure-1: Traditional internet of things (IoT) architecture.

However, rapid adoption of the IoT in healthcare also brought with it substantial challenges to cybersecurity. The extensive interconnectedness of IoT devices makes healthcare systems vulnerable to cyber attacks of all sorts. These days, there is no greater source of sensitive patient data such as medical records, personal information that cybercriminals hunting for vulnerabilities on IoT devices and networks are looking to profit from. Compromise of medical devices that are in the wound like insulin pumps

or pacemakers can have life threatening consequences affecting the patient safety. With IoT increasingly relied upon across healthcare, the efforts to develop solid cybersecurity efforts have been leap-frogged, leading many systems to be open to attack via ransomware, data breaches and distributed denial-of-service (DDoS). Additionally, the resource constrains of many IoT devices (limited computational power, limited battery life) make the lack of standardized security protocols an even more serious problem. Thus, a need for an all-comprehensive cybersecurity framework for IoT enabled healthcare applications is urgently required [3].

1.2.Motivation

The heightened frequency and sophistication of cyberattacks in healthcare systems have illustrated the necessity of effective cybersecurity frameworks for the kind of IoT healthcare applications. As in the recent years, healthcare organizations have become prime targets for cybercriminals as they deal with the high value of sensitive patient data and the criticalness of medical services. Although it has not particularly disrupted the healthcare operations, ransomware attack, data breach and unauthorized access to medical devices have jeopardized the patient safety and privacy. Ransomware attacks are one of the most alarming trends that also involves those who encrypt crucial systems and then insist payment so that they can release it. For instance, in 2017 the WannaCry ransomware attack affected a plethora of healthcare organizations worldwide, including UK's National Health Service (NHS), which resulted in widespread disruption to patient care. Moreover, data breaches involving patient records being stolen are also becoming increasingly common as attacks are made on vulnerabilities in IoT devices and networks so that the attackers can gain unauthorized access. Although these breaches translate into monetary losses, lose trust by the patients as well as tarnish the image of the healthcare providers. The cost of cyberattacks on healthcare systems exceeds just financial damage and damage to reputation. Risks to patient safety exist associated with compromised medical devices, for example, insulin pumps, pacemakers, and imaging systems. They included things like hacked infusion pumps that could dispense an unauthorized dosage of medication, or a compromised pacemaker which could stop working at the wrong time – resulting in life-threatening situations. Such scenarios make it evident that medical applications with IoT ability should be secured to render medical systems benign and reliable.

Given the growing reliance of IoT in healthcare and ever increasing threatscape, there is a need for comprehensive cybersecurity frameworks. Healthcare IoT demands these frameworks to offset the distinct difficulties of the healthcare IoT arena: protecting delicate client information, safe operation of therapeutic gadgets, and solidarity of therapeutic organize. Healthcare organizations can address risks; protect patient information; and maintain the uninterrupted delivery of essential medical services by conducting robust cybersecurity measures and implementing it.

1.3.Objectives

The primary objectives of this review paper are twofold:

To Review Existing Cybersecurity Frameworks for IoT-Enabled Healthcare Applications:

The objective of this paper is to perform a thorough examination of the existing cybersecurity frameworks used in the Internet of Things (IoT) based Healthcare systems. Review will look into the applicability of highly recognized frameworks such as the National Institute of Standards and Technology (NIST) IoT Framework, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Trust Alliance (HITRUST) Common Security Framework in terms of addressing previously mentioned unique security challenges of healthcare IoT. Case studies for successful implementations and lessons learned from past cyber incidents will also be included in the analysis to give practical insights into how these frameworks work and how effective they truly are.

To Identify Gaps and Propose Improvements for Future Frameworks:

Although there are existing frameworks that offer a starting point to take a cybersecurity approach, IoT enabled healthcare specific requirements are not addressed well by such existing frameworks. This paper aims at filling the gaps with existing frameworks like absent common protocols for device authentication; under consideration of real-time threat detection; unsuitable computing power for resource constrained IoT devices. On this basis, the review will suggest actionable improvement and innovative strategies to improve the security of Health care IoT Ecosystems. This may include the integration of emerging technologies such as blockchain for secure data management, artificial intelligence for anomaly detection, and edge computing for processing data in the local network.

2.IOT IN HEALTHCARE: APPLICATIONS AND CHALLENGES

2.1 IoT-Enabled Healthcare Applications

IoT in healthcare has led to innovative applications that enhance medical services by using interconnected devices, sensors, and systems to collect, transmit, and analyze real-time health data. Key applications include remote patient monitoring systems, wearable health devices like fitness

trackers and glucose monitors, and smart medical devices such as infusion pumps and pacemakers, which improve treatment accuracy and efficiency. IoT is also used in hospital asset management, helping track medical equipment, supplies, and personnel, reducing losses, and lowering costs.

2.2 Benefits of IoT in Healthcare

The adoption of IoT in healthcare offers several benefits, including improved patient outcomes, enhanced operational efficiency, and real-time data collection and analysis. IoT-enabled applications help in early detection of health issues, allowing for timely intervention and personalized treatment plans. For example, remote monitoring systems can alert healthcare providers to abnormal health metrics, preventing complications and hospital readmissions. IoT also enhances operational efficiency by automating routine tasks, reducing administrative burdens, and better allocating resources, allowing healthcare providers to focus more on patient care. Smart hospital systems can automate processes like patient admissions, bed assignments, and discharges. Additionally, IoT generates vast amounts of real-time data, which can be analyzed to identify trends, predict health risks, and support evidence-based decisions, improving the effectiveness of medical interventions for healthcare professionals.

2.3 Challenges in IoT-Enabled Healthcare

Despite its numerous benefits, the widespread adoption of IoT in healthcare is accompanied by significant challenges:

- **Data Privacy and Security Concerns:** Being a prime target to cyber attacks, health data are therefore sensitive. Patient's privacy and safety can be compromised by unauthorized access to patient record or medical device.
- **Lack of Standardized Security Protocols:** The fact that health care IoT devices do not have universally accepted security standards only exacerbates vulnerabilities, which leaves systems vulnerable to cyber threats. This emphasizes the necessity for other comprehensive standardized cybersecurity framework.

3. CYBERSECURITY THREATS IN IOT-ENABLED HEALTHCARE

3.1 Threat Landscape

As IoT has rapidly adopted in healthcare, it has expanded the attack surface of healthcare systems and made them very vulnerable to a variety of cyber threats. The general cyber threats and healthcare threats are grouped broadly.

3.1.1.Overview of Common Cyber Threats

The traditional cyber threats like malware, phishing and distributed denial-of-service (DDoS) attacks are in fact applicable to healthcare IoT systems. Ransomware, and other kinds of malware, can slip into healthcare networks, encrypt all of the critical data, and ask you for money to release them. Some common and serious ways of hacking healthcare IT are phishing attacks which aim to steal the login credentials or install the malicious software onto healthcare staffs computers [5], and DDoS attacks which overwhelm the system and thereby cause service disruption.

3.2 Vulnerabilities in Healthcare IoT Systems

Identification of the vulnerabilities in healthcare IoT systems comes from both technical and operational weaknesses that the attackers are able to exploit.

Weak Authentication Mechanisms: In healthcare, many IoT devices rely on default or weak passwords in order to make those IoT devices become easy targets for brute force attacks. This vulnerability is exacerbated by the lack of multi factor authentication.

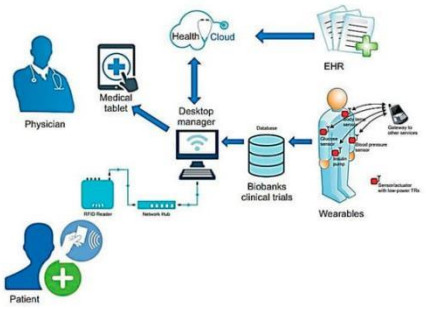

Figure-2: Revolutionary features of H-IoT in a hospital environment.

Lack of Encryption in Data Transmission: Most of the time, IoT devices transfer data to and from healthcare systems without encrypting the data, thus allowing sensitive patient information to be obtained and accessed without authorization. A viewing of the data without encryption amounts to a serious security hole in healthcare IoT.

Outdated Firmware and Software: The firmware or software that run these medical devices is frequently outdated, without any critical security patches. As a result, they are exposed to well known exploits and zero day exploits.

3.3 Impact of Cyberattacks

If this healthcare IoT system is attacked, patient safety, financial stability, and organizational reputation will all be impacted.

Patient Safety Risks: Medical devices that are compromised can cause life or death. For instance, it could impact such devices as a hacked infusion pump, for example, delivering the wrong quantity of medication or a tampered pacemaker that could go haywire and put the life of the patient in harm's way.

Financial Losses for Healthcare Providers: Ransom cybberattacks are a very good source of financial loss through the payment of ransom, regulatory fines, and the cost of recovery of breaches. The 2017 WannaCry ransomware attack damaged the National Health Service (NHS) in the UK to the tune of an estimated £92 million in damages and lost productivity.

4. EXISTING CYBERSECURITY FRAMEWORKS FOR IOT-ENABLED HEALTHCARE

4.1 Overview of Cybersecurity Frameworks

In order to keep pace with the rising cybersecurity threats in IoT enabled healthcare, a number of frameworks have been developed for general IoT systems as well as for healthcare applications. Only, these frameworks give guidelines, best practices and standards to ensure IoT ecosystems and protect sensitive data [22].

4.1.1.General IoT Cybersecurity Frameworks

NIST IoT Framework: For securing IoT devices, risk management, device identification and data protection are the main points that the National Institute of Standards and Technology (NIST) delivers an overall guideline for. It focuses on an IoT security life cycle approach starting from design till decommissioning.

ISO/IEC 27001: It is an international standard on information security management system (ISMS), and covers IoT devices. Therefore it provides a systematic approach of managing sensitive information for confidentiality, integrity, and availability [21].

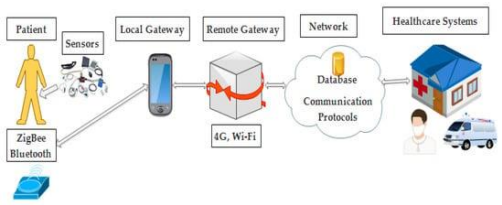

Figure-3: Flow of data from the patient to healthcare systems.

4.1.2.Healthcare-Specific Frameworks

HIPAA (Health Insurance Portability and Accountability Act): The HIPAA is there to set some standards for protecting sensitive patient data in the United States. Healthcare organizations are required to set in place safeguards for electronic protected health information (ePHI) that include data encryption and access controls [6].

HITRUST Common Security Framework (CSF): The HITRUST CSF combines these various regulatory standards such as HIPAA and GDPR into something that serves the unique needs of healthcare cybersecurity. It provides a risk-based management scheme for healthcare IoT systems security and compliance [19-20].

4.2. Analysis of Existing Frameworks

While healthcare IoT systems have advantages and disadvantages compared with existing frameworks, the latter provide a solid foundation for IoT cybersecurity.

Comprehensive Risk Management: However, risk assessment and mitigation, as per frameworks like NIST, ISO/IEC 27001, are vital processes for pinpointing and healing the flaws of wellness IoT systems.

Lack of IoT-Specific Guidance: In the case of general frameworks like NIST and ISO/IEC 27001, there are no detailed guidance for securing the IoT devices, specifically in healthcare field.

4.3 Case Studies

The insights drawn from examining real world implementations and incidents help us to such an extent that they aid in ascertaining the efficacy of experiments such as the case of cybersecurity frameworks in healthcare IoT.

Cleveland Clinic: The Cleveland Clinic has enhanced its cybersecurity posture by implementing the HITRUST CSF and complies with HIPAA and other regulations. With this framework, the organization could keep its IoT medical devices secured and ensure the security of patient data effectively.

Mayo Clinic: The NIST Cybersecurity Framework was adopted by Mayo Clinic to protect its IoT system with its risk management and continuous monitoring approaches. Using this approach, organization can prevent threats and maintain health care system integrity [18].

Medtronic Insulin Pump Vulnerabilities: In 2019, it was shown how vulnerable Medtronic's insulin pumps were to inadequate device authentication and encryption. This incident revealed the necessity of boosting security steps in medical devices and the requirement for cooperation between masters and healthcare supplier [17].

5. KEY COMPONENTS OF A ROBUST CYBERSECURITY FRAMEWORK FOR HEALTHCARE IOT

In order to meet the special constraints of securing networked clinical utensils, delicate patient information, and essential medical center facilities, a solid cybersecurity framework for IoT empowered medical attention must be cultivated. Some essential components required for developing the framework are:

5.1 Risk Assessment and Management

Any cybersecurity strategy is built on a thorough risk assessment. Healthcare organizations must determine the most likely and impactful threats — device hijacking, data breaches, ransomware attacks and others — and plan for them accordingly. In this process, threat modeling or risk matrices can be used tools [7]. Real-time monitoring systems implement in organizations help with detecting and reacting in a timely manner to the threats. [16] Advanced technologies such as artificial intelligence (AI) and machine learning (ML) can be used to identify anomalous traffic on a network or device behavior to improve the detection of threats.

5.2 Data Protection

Sensitive data is encrypted so that irrespective of whether attackers intercept it, they wouldn't be able to access it without information. For the protection of patient information it is important to have strong encryption protocols such as AES 256 for data at rest and TLS for data in transit [8]. The access control in data storage systems must be of course well protected; meaning that they can only be accessed by using role based access and multi factor authentication (MFA). Access logs can be routinely audited to ensure that no unauthorized access attempts take place and, thus, minimize the risks of data compromises.

5.3 Device Security

Secure Boot and Firmware Update: These are necessary to boot IoT devices securely and get regular firmware updates in place to avoid unauthorized modification. Secure boot mechanisms check for the integrity of the device's software, and timely updates 'patch' known vulnerabilities.

Strong authentication protocols: Strong authentication protocols which include biometric authentication or hardware based tokens can prevent unauthorized access to medical devices. Authorization mechanisms are to enforce the principle of least privilege, giving the users only the minimum set of access they need [15].

5.4 Network Security

Secure Communication Protocols (e.g., TLS, MQTT): This is done to ensure that data that is sent from devices and devices are securely encrypted and protected from interception by for example the Transport Layer Security (TLS) or the Message Queuing Telemetry Transport (MQTT).

Intrusion Detection and Prevention Systems (IDPS): Network traffic monitoring for suspicious activity, and automatic blocking or mitigation of attacks – this is the IDPS solution. But these systems are critical for defending against the types of advanced threats like DDoS attacks and malware [14].

5.5 Incident Response and Recovery

Developing a Response Plan for Cyber Incidents: A good incident response plan for healthcare organizations will define how to respond quickly and efficiently to cyber attacks. Also, the plan should include specific actions to guide the process of recognizing incidents, isolating and eliminating them, and communicating the incident to the stakeholders.

5.6 Compliance and Standards

Adherence to Regulatory Requirements (e.g., GDPR, HIPAA): To comply with regulations such as General Data Protection Regulation (GDPR) and HIPAA, it is compulsory to keep patient data safe and also prevent legal consequences such as high fines. This established these rules to go over data protection, breaches and the patients privacy.

Industry Best Practices and Certifications: An organization's cybersecurity posture can also be improved by adopting industry best practices, including the HITRUST CSF or ISO/IEC 27001. HITRUST or ISO 27001 certifications show commitment to security and help to build the trust of patients and partners [13].

6. EMERGING TECHNOLOGIES AND TRENDS

Thanks to continuous improvement of cybersecurity threats in the IoT driven healthcare, cutting edge technologies and trends for security and resiliency are developed. These new solutions resolve the distinct healthcare IoT challenges and provide new methods to protect patients' sensitive data, medical devices' security, and risks mitigation.

6.1.Blockchain for Healthcare IoT Security

Decentralized Data Management: One of the advantages of blockchain tech is that it provides a decentralized way of managing data which does not

require a central authority; this further helps reduce the chances of single points of failure. Blockchain may be used in a secure way to store and share patient data across multiple devices and stakeholders in the healthcare IoT to maintain data integrity and transparency [29].

Immutable Audit Trails: Blockchain immutable ledger maintains a tamper, proof record of all transactions making it ideal for healthcare system where audit trail is needed. A benefit of this feature is that it also enhances accountability and traceability in order to allow the healthcare providers to identify who has had access to patient data and what the data has been changed [12].

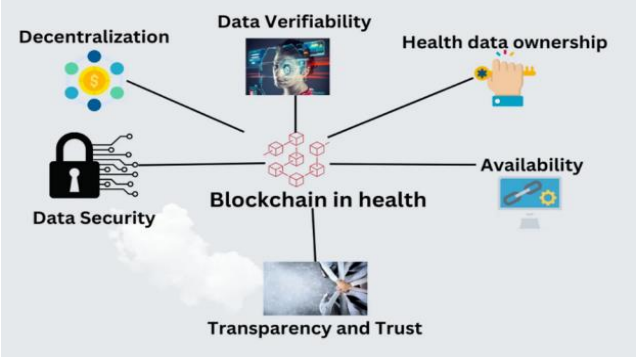

Figure-4: Advantages of Block-chain.

6.2.Artificial Intelligence and Machine Learning

Anomaly Detection and Predictive Analytics: With the help of AI and ML algorithms vast amount of data from the IoT devices can be analyzed to find patterns and identify the anomaly which could indicate the cyber threat. For instance, predictive analytics may highlight abnormal device behavior, for instance, oversending of data or unauthorized access attempt, and alerts to mitigate the threat proactively.

6.3.Edge Computing

Reducing Latency and Enhancing Data Processing: Instead, data is processed nearer to the source (i.e., IoT devices) rather than being sent to centralized cloud servers [10]. Latency and efficiency of real time application like remote patient monitoring and emergency response systems are reduced.

Improving Security by Processing Data Locally: Crossing them (data) during transmission is the first risk that edge computing can minimize it in pasting sensitive data locally. Additionally, attacks surface is reduced as fewer data points are accessible by external networks.

6.4 Zero Trust Architecture

Continuous Verification of Devices and Users: The basis of Zero Trust Architecture (ZTA) is 'never trust, always verify'. It demands it to be continuously authenticated and authorized for all devices and users, regardless of the location or network. In healthcare IoT, this is of particular tenacity since the propensity of dynamically connected devices heightens security risks [11].

Minimizing Attack Surfaces: It reduces the attack surface by chopping networks up into network segments and tightly controlling access to them where. This could be exemplified in that a compromised device in one segment cannot easily attack other portions of the network, thus reducing the types of damage that a breach can carry.

7. CONCLUSION

IoT technologies have rapidly brought the integration of IoT technologies into healthcare, making medical services more effective through the real-time monitoring, gained treatments and increased operational efficiency. While IoT enablers for healthcare applications have contributed a great deal in myriad ways, they have also brought along a wider range of cybersecurity challenges that have led to the exposure of vitally important patient data as well as critical medical infrastructure to a continually increasing number of cyber threats. Based on a review of the existing cybersecurity frameworks in literature, and their strengths and weaknesses, this review paper has spanned the current context of cybersecurity frameworks for healthcare IoT systems and proposed key components to be incorporated into a step towards such a cybersecurity framework.

The results underscore the necessity of developing unified and adaptable cybersecurity methods dedicated to the particular issues of healthcare IoT including information solitude, machine security, and viability of the network. Recent technologies like blockchain, artificial intelligence, edge computing, and Zero Trust Architecture are potentially suitable solutions to improve security and reliability of IoT enabled healthcare system. But by integrating such innovations with adherence to regulatory standards and industry best practices, healthcare organizations can mitigate the risks associated with healthcare, safeguard patient data and maintain integrity of medical devices and networks.

But, there are still significant challenges such as the lack of standardized security protocols, limited resources and the shortage in cybersecurity specialists. To address these challenges there is a need of collaboration between the stakeholders such as healthcare providers, device manufacturers, policymakers, and researchers. Future work should concentrate on contributing towards lightweight security solutions for resource constrained devices, interworking and a culture of cybersecurity awareness amongst the in the healthcare organisation.

REFERENCES

1. S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

2. D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," Healthcare Informatics Research, vol. 22, no. 3, pp. 156–163, 2016, doi: 10.4258/hir.2016.22.3.156.

3. S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.

4. B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards Fog-Driven IoT eHealth: Promises and Challenges of IoT in Medicine and Healthcare," Future Generation Computer Systems, vol. 78, pp. 659–676, 2018, doi: 10.1016/j.future.2017.04.036.

5. National Institute of Standards and Technology (NIST), "Cybersecurity Framework for IoT," NIST Special Publication 800-82, 2020. [Online]. Available: https://www.nist.gov.

6. International Organization for Standardization (ISO), "ISO/IEC 27001: Information Security Management," 2013. [Online]. Available: https://www.iso.org.

7. HIPAA Journal, "HIPAA Compliance and IoT Devices," 2023. [Online]. Available: https://www.hipaajournal.com.

8. HITRUST Alliance, "HITRUST CSF: A Comprehensive Framework for Healthcare Cybersecurity," 2023. [Online]. Available: https://www.hitrustalliance.net.

9. M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1094–1122, 2018, doi: 10.1109/COMST.2017.2782348.

10. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," IEEE International Conference on Pervasive Computing and Communications (PerCom), 2017, doi: 10.1109/PERCOM.2017.7916924.

11. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.

12. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

13. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

14. P. K. D. Pramanik, S. Pal, and M. Mukherjee, "Healthcare Big Data: A Comprehensive Overview," IEEE Access, vol. 7, pp. 73961–73988, 2019, doi: 10.1109/ACCESS.2019.2920483.

15. G. K. Sandhu, "Edge Computing for IoT-Enabled Healthcare: A Survey," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9479–9495, 2021, doi: 10.1109/JIOT.2021.3059987.

16. R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018, doi: 10.1016/j.future.2016.11.009.

17. NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. [Online]. Available: https://www.nist.gov.

18. M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang, "A Survey on Cybersecurity for Smart Grid: Threats, Solutions, and Challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2954003.

19. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016, doi: 10.1002/sec.1748.

20. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy, and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

21. M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A Hybrid Deep Learning Model for Efficient Intrusion Detection in Big Data Environment," Information Sciences, vol. 513, pp. 386–396, 2020, doi: 10.1016/j.ins.2019.10.069.

22. S. H. Ahmed, G. Kim, and D. Kim, "Cyber-Physical System Security for the Internet of Medical Things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2182–2194, 2019, doi: 10.1109/JIOT.2018.2873349.