iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50534

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Smart IoT Based Healthcare Sector

Sohit Kummar[1], Asutosh Mohanty[2], Manasvi Varshney[3], Amit Kumar[4]
[1, 2, 3, 4]*Department of Computer Science Sharda University Greater Noida, India*

Abstract: ***The Internet of Things (IoT) circumscribes the real-world commodity to communicate and interact with each other by the help of Internet. The enormous growth in the field of IoT devices has drawn wide attention towards wireless-based area networks (WBANs) to eliminate implications like lack of central entity, rigid security demands, mass data processing, low-latency service provision and resource limitation. Moreover, this paper represents a broad discussion over IoT healthcare protocols. This paper also brings us an extensive insight over the IoT surrounding healthcare over its privacy, challenges privacy, challenges, and security issues. This paper also proposes a solution to reduce potential causes of human error and to provide with the best-in-class efficiency in the healthcare sector. This paper highlights IoT based approach in the healthcare industry for higher reliability and efficiency.***

Keyword: IoT, Healthcare, Security, medical environment, sensors

I. INTRODUCTION

With the advancement in the technology day by day. The concept of IoT, Wireless Sensors and Data Science has undergone an advance development phase. The importance of these concepts has always proved its worth by playing vital role in the society. All these concepts have got prominent advantages like higher reliability, connectivity and communication. The IoT has brought us the emergence and requirement for smart nations, smart cities, smart grids, and smart healthcare [1]. The most widespread application of the IoT can be seen in the healthcare sector. The WBAN by the help of sensors help the healthcare sector in its day-to-day operations. Due to its high advantages, it lacks in certain aspects such as cyber-attacks, lack of central-controller, resource limitations and potential bottleneck. This paper also draws the attention towards the rigid security implications of the smart healthcare model. Data privacy in the healthcare model can through access control rules which will ensure that only people with authority has the right to make any necessary changes [2].

The major contributions of this research paper are presented below:

1) This paper presents the overview of the IoT applications for the healthcare system and provide a detail on its advantages and implications related with it [3].
2) This paper discusses about issues and challenges faced by the healthcare services [4].
3) This paper researches the key healthcare challenges and its open issues and it also discusses about the cyber-attacks and vulnerabilities [5].

This paper has been arranged in the following sequence such as: Section 2 discusses about standing IoT operations in the healthcare system and what all implications it faces. Section 3 elaborates the threats from the cyber-attacks and features of IoT which can be taken in account to overcome these vulnerabilities. The paper concludes in the Section 4 with future research direction.

II. OVERVIEW OF IOT-BASED SECURITY FOR HEALTHCARE SOFTWARE

Healthcare industries are one of the many industries that are under constant cyber threats therefore, one needs to have a good security system to tackle this problem. There are many reasons because of which healthcare systems are prone to cyber-attacks. For example, availability of sensitive data such as vaccine research information, medical formula, insurance, and medical details that bid high prices in black market. There are many susceptibilities of IoT security in healthcare industries. The FDA has mandated that medical device manufacturers incorporates security into their systems as of 2016 and 2018. But the attacks are becoming more sophisticated, in 2017, the Cry ransomware impacted numerous healthcare facilities operations by preventing staff from accessing crucial equipment's. There are many IoT threats present in healthcare to this day, for example, unauthorized access, DDOS attack, privacy violation, AI-driven security systems, data encryption, device hijack, and disclosure of personnel information [6 - 8]. Though IoT devices are prone to cyber hazards, still all attacks can be managed and healthcare industries can be secured from attacks. It can be achieved through implementing effective authentication, following standardized best practices, segmenting networks, and using inventory devices.

There is an urgent need of sophisticated system for fraud detection as well as protecting patients' data. This can be achieved by constant monitoring, automated discovery, and risk management system. As a healthcare organization your 'devoted to offering the best effective, efficient patients care [9].

A. *Security Requirements*

An innovative technology in this field is Internet of Things (IoT) which offers smart services and remote monitoring across healthcare systems in accordance with a collection of interconnected networks and devices. The nature of IoT based healthcare systems involves sensitive and personnel patients' information, making security a key concern. For the need of modern living IoT offers a wide range of applications in industries like agriculture, emergency services, transportation, logistics, and smart cities. Additionally, one of the most appealing IoT application sector is healthcare sectors. IoT base healthcare solutions have security needs that are comparable to those in traditional communication contexts [10]. To achieve the finest security systems in healthcare following requirements should be followed:

1) *Data Freshness:* It is necessary to make sure that communication is current because each IoT healthcare network offers sometimes varying measurements.
2) *Fault Tolerance*: A security system should remain working in the position of fraud detection such as device failure, or system glitch.
3) *Integrity:* It should maintain complete data integrity while data is being transferred to devices.
4) *Confidentiality*: It should not allow any unauthorized users the access towards medical data.
5) *Privacy*: Due to network sharing of sensitive data, privacy concerns are must.
6) *Authentication*: It is the verification between two users who are communicating.
7) *Resiliency*: Even if some of the connected health devices are insecure, A security plan should nevertheless shield the network device, and data from intrusion.
8) *Secure Booting:* A cryptographical signatures are generated when an item is powered at the first time for verification of its authenticity and integrity.

B. *IoT security Attacks based on Information Disruption and Host properties*

Healthcare industries incorporates every technology to itself to become bigger and better. As always good things come with their challenges, same goes with IoT in healthcare, it incorporates many challenges in it.

Due to connections, it has become a potential security loophole that are used by many hackers to hack into a system for sensitive information.

Therefore, disturbing the work of healthcare workers and becoming the threat to patients' life. Prone information's that are at constant risks of stealing are patients' personnel information, medical formula, vaccine research, etc.

There is hacking done in medical devices such as MRI and Xray machines because when these devices are made security is not taken as priority [11].

IoT security requirements cannot be fulfilled by traditional ways thus, as shown in figure 1, following requirements should be followed:

1) *Scalability:* More devices are being connected to global information network as a result of gradual development in IoT devices. Consecutively it becomes difficult to develop highly scalable security systems.
2) *Trust Mechanisms:* Identity management systems should be decided for private and sensitive medical data.
3) *Memory Limitations:* The majority of IoT systems has no memory and embedded operating system, systems software, and application binary are used to activate such devices. As a result, they might not have enough memory to carry out complex security processes.
4) *Dynamic Topology:* There should be a new topology for IoT devices that is both dynamic and should be present there any time anywhere.
5) *Multiple Devices:* An IoT healthcare network includes variety of health equipment's, from PCs, inexpensive RFIT tags. The capability of these devices in terms of memory, power, embedded software, compute vary. Designing software that can work with even most basic gadgets is a challenge.
6) *Multi-Protocol Network:* Through proprietary network protocol a health device can communicate through any device in a local network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

C. IoT Healthcare Services

As contact with doctors have grown simpler and more effective, thanks to IoT, this has also enhanced patients' engagement and happiness. Additionally, remote patients monitoring shortens hospital stays and avoid readmissions by keeping track of patient's health. It has also played an important role in improving treatments and reducing costs at a noticeable rate. IoT devices are used for everyone in healthcare industries that is hospitals, patients, insurance companies, doctors making their life simpler [12]. Range of field that are included in IoT healthcare services can include:

1) *Community Healthcare*: A network that is cooperative network structure and covers the area around municipal hospital, local community, a residential care is a service that IoT may offer. It has been suggested and discovered that cooperative IoT platform for monitoring rural healthcare is energy sufficient
2) *Sematic Medical Access*: In healthcare industries Otologist and Semantics provide a large amount of information that attracts the IoT designers for healthcare applications and services.
3) *Ambient Assisted Living*: It offers an ecosystem of IoT capable medical software programs, computers, sensors, and wireless networks for healthcare monitoring. In other words, unique IoT service is required.
4) *Adverse Drug Reaction*: It is a typical medical injury that occurs because of taking a dose of drugs or intaking it for a long period.
5) *Indirect Emergency Health*: Healthcare concerns can rise an indirect emergency caused by things like bad weather, transit mishaps involving trains, ships, cars, planes, and collapse of earthen structures and among the other things. As result, this service is known as indirect emergency healthcare, and can provide variety of options including information accessibility.
6) Early Prevention: IoT devices can be used for monitoring users' day to day activity like heart rate, temperature, blood pressure, etc. to maintain detailed report.

III. HEALTHCARE CHALLENGES AND OPEN ISSUES

No other industry can indulge technology like healthcare from patients' diagnosis to predicting and preventing diseases at early stage, it has proven its worth. According to a survey [18], it has been estimated that healthcare IoT sector market size will be $534.3 Billion till 2025. Implementing hospitals and clinics can present several problems that ultimately prevent them from maximizing the benefits of its most recent developments. With the use of technology, some of the major obstacles to healthcare that exist today can be overcome. However, when adopting cutting technology, such as IoT encounters difficulty, it creates new issues and barriers to accessing secure healthcare. Traditional treatment plans can be implemented with new framework and approaches to make it simpler and more accurate thus increasing survival rate. Big changes often come with huge constraints, what the people have dreamed for future is now coming but to properly apply to gain its maximum exploitation is one of the major tasks. Setting up a connection between all the present devices and maintaining that connection even when some appears to be faulty is a handful task. Difference in communication protocols of devices can be a headache because of difficulty in arranging and assembling data. Thus, it is a very difficult task to design an IoT system which can stand on all ground without any limitation. There are several challenges faced by an IoT systems that are both recognized and unrecognized [13].

A. Standardization

As IoT is making its grip on healthcare sectors so as in the market. In the recent decades a lot of competition has increased in a market of IoT. Many small businesses are growing to make new, efficient, and compatible IoT devices for healthcare but the major problem is arising is that that they do not have enough man power to support their business thus, lacking in the aspect. There are large number of devices connected through the network. There are different standards, protocols, languages that are used to connect devices. The ownership and control of data are unclear because there are no rules that are widely acknowledged. This makes the IoT integration of many devices in healthcare industries difficult.

The disparities in their network communication protocol makes it difficult for healthcare users to aggregate data, even when the devices are connected. There are no set protocols for these devices. The adaptation and functionalities of IoT healthcare systems are in doubt without device compatibility. Because of this, standardization in IoT healthcare is still an open issue. The secret to developing protocols that are universally approved intermobility across medical device is standardization. By ensuring that their software and hardware are compatible, companies can lower their overall cost of data collection while maintaining the system security and avoiding the protocols gaps. Therefore, there is a need to raise the issue to standardized communication and protocols [14].

B. Security Challenges

In the last few decades, healthcare industries are the victims of most cyber-attacks. Due to shared network in IoT it becomes easier for the hackers to hack into the system. Because of the use of cloud and web software, security concerns have come in the limelight. Securing any data transfer within an across business can be difficult. Basically, no health care facilities, no matter how strong its cyber security posture is completely impervious to intrusion.

Thus, making security the most debatable issue in healthcare. Securing patients personnel information is must, and privacy to their data should be maintain. IoT devices are designed in such a way it collects, store, and transfer data, anytime anywhere. Thus, hacker use this system to steal patients' information, sometimes selling or using the information against them. Hackers forged Ids to get narcotics so they can abuse their futures. IoT based healthcare are architecture is not effectively safeguard and fails to ensure the privacy and security of data because of the repeat's Ids.' It becomes necessary to safeguard medical devices that are connected to each from any kind of unauthorized access to protect their patient's welfare. Many other pieces of equipment's utilized in healthcare sectors are connected to cloud and as a result are the part of IoT along with connected medical devices. In order to protect patients and healthcare workers other gadgets like phones, cameras, etc. should be protected [15].

1) Ransomware Attacks

In recent years, hospitals have been the target of ransomware attacks. The healthcare industries experience the greatest number of ransomwares assaults, according to FBIs' 2021 internet crime reports. Healthcare got 148 complaints to the FBIs' internet crime complaints center more than twice as many as the financial sector. The use of ransomware is developing and becoming more complex. Software vulnerability, exploitation, Phishing, Remote Desktop protocol (RDP) exploitation are the most popular attack strategies. The Conti ransomware gang is responsible for numerous healthcare attacks. Conti conduct business as usual, complete with performance evaluation, an HR department and even an employee of the month [16].

2) Electronic Healthcare Records (EHRs) vulnerability

Electronic Health Records (EHR) usage is frequently viewed as a windfall to the industry. Though, health information exchanges both patients and doctors can quickly access their information. Although, it is efficient and effective to share this information there are inherit security issues. An enticing opportunity for cyber criminals is created by a network that maintains a lot of sensitive personnel health information (PHI). The dark web is really interested in PHI. Because it makes it simpler for threat actors to commit identity theft. It is very useful, even a single patients records can include details like insurance information, history, payment method, social security number that a cybercriminal could use for their advantage in the hopes that patients will pay ransom to have it erase. EHR are so difficult to secure even though they are very helpful in healthcare industry [17].

3) Quality of Services (QoS)

When talks come towards QoS healthcare requires highest quality because it comes with the risk of life and death. Healthcare comes in the list of many industries that should be reliable, available, and should strictly maintain QoS in IoT based healthcare network. In the healthcare sectors IoT is mainly used in rea-time application. The system requires timely collection, transport. Processing, analyzing, and utilization of sensor data. However, IoT device usually fails to deliver the information on schedule. QoS is therefore viewed as a barrier for the IoT healthcare systems. By offering differentiating treatment and capacity allocation to network traffic flows, QoS achieves that. The most innovative and alluring technology present today is IoT, combines software, embedded device, Artificial Intelligence, and sensors. That is why QoS is very important whenever there is a talk for IoT. IoT comes with an endless network capability hence, maintaining that network to provide the top-notch service comes with challenges and completing it is challenging as well as an important task. QoS is therefore viewed as a barrier for healthcare system where wearable devices handled real-time life critical applications, it is also becoming increasingly difficult to produce a valid diagnosis within reasonable time-period ensuring QoS is crucial to overcome these difficulties [19].

4) Data Protection

The healthcare industry is a networked environment allowing the patients information to be exchanged and controlled by the varieties of parties and from several end points, each with its own level of securities for securing that information. Medical data is considered especially valuable for cyber criminals because of its sensitivity. Therefore, it is essential that businesses employ healthcare data security that will enhance patients care, safeguards key resources, and satisfy regulatory requirements. Due to an increase in data protection violation, data security in healthcare application is becoming a bigger problem.

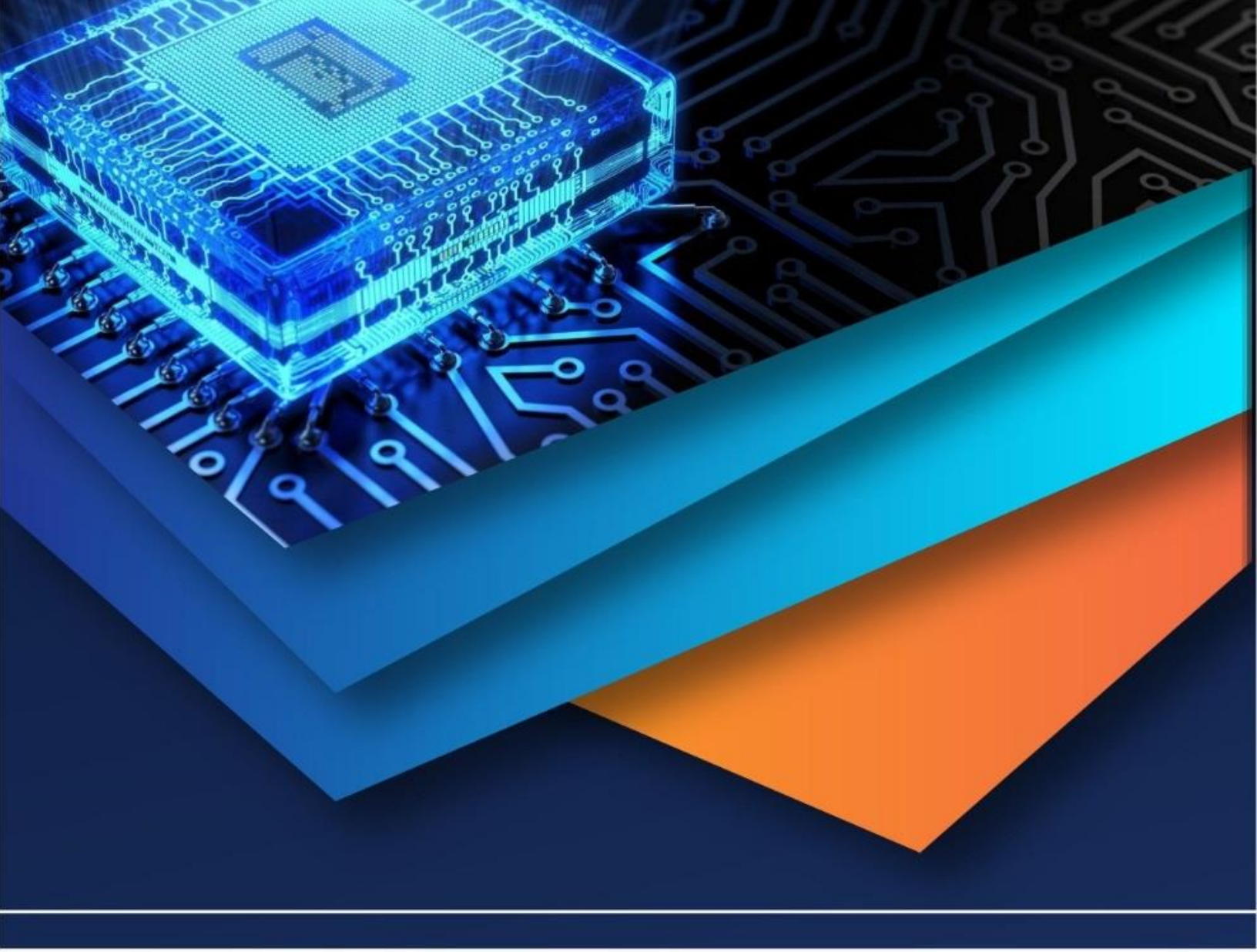
Providing the incidence has the potential to result in considerable harm or substantial distress to those effective, the act being reported to the Information Commissioner Office (ICO) can serve as a financial penalty for a major violation of data protection act. To make a system secure and protect the data from breaches industry should focus on the loopholes and weak spots that are most vulnerable and likely to be used by cyber criminals for data breaching. To secure data industries should not go for various system that design by different IoT designers because the diverse will be the system more loopholes it will create giving better opportunities to the criminals to hack into the system. To harm patients and doctors, hackers attempt to hack data. When working with sensitive information while on the go, both patients and doctors are vulnerable to the threat of a data breach [20].

IV. CONCLUSION

IoT has revolutionized all the industries. It has highly impacted the medical industry with two major outcomes lowered costs and increased efficiency. The regular improvisation in medical sector by the IoT has resulted in improved patient care. The IoT has evolved from building machine to machine communication and automation towards the smallest and best quality of sensors. Our research paper has elaborated a review on the security of the IoT based healthcare systems. In this paper we have briefly discussed the challenges of the IoT based healthcare system. Our paper reviews the potential challenges and threats in the IoT based healthcare sector and it suggests the opportunities which are yet to be overcome in the healthcare marks.

REFERENCES

[1] Bhatt and S. Chakraborty, “Real-time healthcare monitoring using Smart Systems: A step towards healthcare service orchestration Smart Systems for futuristic healthcare,” 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021.
[2] D. Anand and A. Kumar, “IOT-based Automated Healthcare System,” Advanced Healthcare Systems, pp. 335–350, 2022.
[3] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IOT security: An exhaustive survey on IOT vulnerabilities and a first empirical look on internet-scale IOT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702–2733. https://doi.org/10.1109/comst.2019.2910750
[4] H. Yüksel, “IOT-based Smart Healthcare Monitoring System,” Healthcare Monitoring and Data Analysis using IoT: Technologies and applications, pp. 71–98, 2022.
[5] Y. Maleh, M. Shojafar, A. Darwish, and A. Haqiq, “Cyber-physical systems: Vulnerabilities, attacks and threats,” Cybersecurity and Privacy in Cyber-Physical Systems, pp. 1–1, 2019.
[6] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IOT: Internet of threats? A survey of practical security vulnerabilities in real IOT devices. IEEE Internet of Things Journal, 6(5), 8182–8201. https://doi.org/10.1109/jiot.2019.2935189
[7] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IOT World: Present and future challenges. IEEE Internet of Things Journal, 5(4), 2483–2495. https://doi.org/10.1109/jiot.2017.2767291
[8] Taimoor, N., & Rehman, S. (2022). Reliable and resilient AI and IOT-based personalised healthcare services: A survey. IEEE Access, 10, 535–563. https://doi.org/10.1109/access.2021.3137364
[9] D. Roach, “Use of comparative vacuum monitoring sensors for automated, wireless health monitoring of bridges and infrastructure,” Maintenance, Safety, Risk, Management and Life-Cycle Performance of Bridges, pp. 2747–2751, 2018.
[10] Y. Yang and C. Stohl, “The appropriation of traditional media content in online contexts: A South Korean textbook case,” Communication Monographs, vol. 87, no. 1, pp. 92–113, 2019.
[11] M. S. Husain and D. M. Haroon, “An enriched information security framework from various attacks in the IOT,” International Journal of Innovative Research in Computer Science & Technology, vol. 8, no. 4, 2020.
[12] D. Gupta, S. Rani, and S. H. Shah, “ICN-Fog computing for iot-based Healthcare,” IoT-Enabled Smart Healthcare Systems, Services and Applications, pp. 19–37, 2022.
[13] Kashyap, A. Kumar, A. Kumar, and Y.-C. Hu, “A systematic survey on fog and IOT Driven Healthcare: Open challenges and research issues,” Electronics, vol. 11, no. 17, p. 2668, 2022.
[14] N. K. Narang, “IOT standards: Mentor's musings on ‘Standardization imperatives for digital transformation of healthcare,’” IEEE Internet of Things Magazine, vol. 4, no. 2, pp. 52–59, 2021.
[15] B. Chander, “Wireless Body Sensor Networks for Patient Health Monitoring,” Advances in Healthcare Information Systems and Administration, pp. 132–154, 2020.
[16] N. A. Hassan, “Enterprise defense strategies against ransomware attacks,” Ransomware Revealed, pp. 115–154, 2019.
[17] I. P. McLoughlin, K. Garrety, R. Wilson, P. Yu, and A. Dalley, “The troubled history of implementing ehrs,” The Digitalization of Healthcare, pp. 23–40, 2017.
[18] A. Sabban, “Wearable antennas in vicinity of human body for 5G, IOT and medical applications,” Wearable Systems and Antennas Technologies for 5G, IOT and Medical Systems, pp. 491–517, 2020.
[19] A. Sawabe and T. Iwai, “A QoS model to identify required qos for guaranteeing quality of internet video streaming services,” ICC 2021 - IEEE International Conference on Communications, 2021.
[20] D. Hallinan, “Opinions · data protection without data: Could data protection law apply without personal data being processed?,” European Data Protection Law Review, vol. 5, no. 3, pp. 293–299, 2019



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY