Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

The Internet of Medical Thing: A Comprehensive Survey

Noor Mohd[1], Arnav Kotiyal[1], Deepak Upadhyay[2]

[1]Department of Computer Science & Engineering Graphic Era Deemed to be University, Dehradun, Uttarakhand, India
[2]Department of Computer Science & Engineering, Graphic Era Hill University, Dehradun, Uttarakhand India, 248002

ABSTRACT
Internet of things (IoT) technology have gained importance in very short time span and now used everywhere because of its cost efficiency, easy to use and easy to install nature. IoT devices are now part of our daily life, these smart devices made our life easier and reduced our efforts. Internet of Thing technology supports diverse applications and services in various areas. IoT is now being used in Medical field also. The term IoMT or Internet of Medical things are used for IoT devices and services that are being used in healthcare domain. IoT in health care plays an important role as it helps to increase accuracy, productivity and reliability of electronic devices. Many researchers are working towards the usage of IoMT technology in medical field. IoMT technologies will be helpful to build a digitalized Health care system. IoMT have various advantages but we cannot neglect the challenges of using IoMT technology in medical field

Keywords: IoT, IoMT, 5G, Security;

INTRODUCTION

Internet of things technologies are not new to the world; billions of devices are using this technology. IoT have changed our way of controlling the devices, IoT have numerous service and application domain. IoT is also used in medical field and it is helping to increase accuracy, reliability and productivity of health care system. Health Care IoT or Internet of Medical things are the terms used to describe the application of IoT in medical industry. IoMT allows the hospital staff to interact, control and monitor the health care devices and it also helps to monitor the condition of the patient. Health care industry have rapidly evolving and adopting new technologies to enhance the health facilities, IoMT technology is one of the modern technology which is being adopted by the medical industry and have increase the facilities and these facilities are helping in treatment of the patient, but as the time passes new chronic diseases are evolving and have increase the pressure in the health care system due to lack of resources [2]. IoMT technologies have helped health care industry in many aspects but we cannot fully depend on this as these technologies have some issues related to privacy and security. Hence we need to consider these aspects as well and work toward to resolve these issues as soon as possible.

Internet of medical things

Internet of Medical things or Health care IoT is an application of Internet of things Technology. 'Things' in Internet of Medical things are the medical devices that are connected and communicate

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

with each other and these devices are controlled and monitored by the hospital staff in real time. IoMT technology helps medical staff to monitor the patient's condition in real time, doctors can also give tele health assistance in case of an emergency. Any smart medical devices whether it's a smart wearable device that can monitor heart rate or oxygen level can help doctors to understand the condition of a patient's health condition and give him treatment according to the data. IoMT technology helps to give health assistance remotely, doctors can treat their patient if the patient or doctor cannot be present in the hospital.

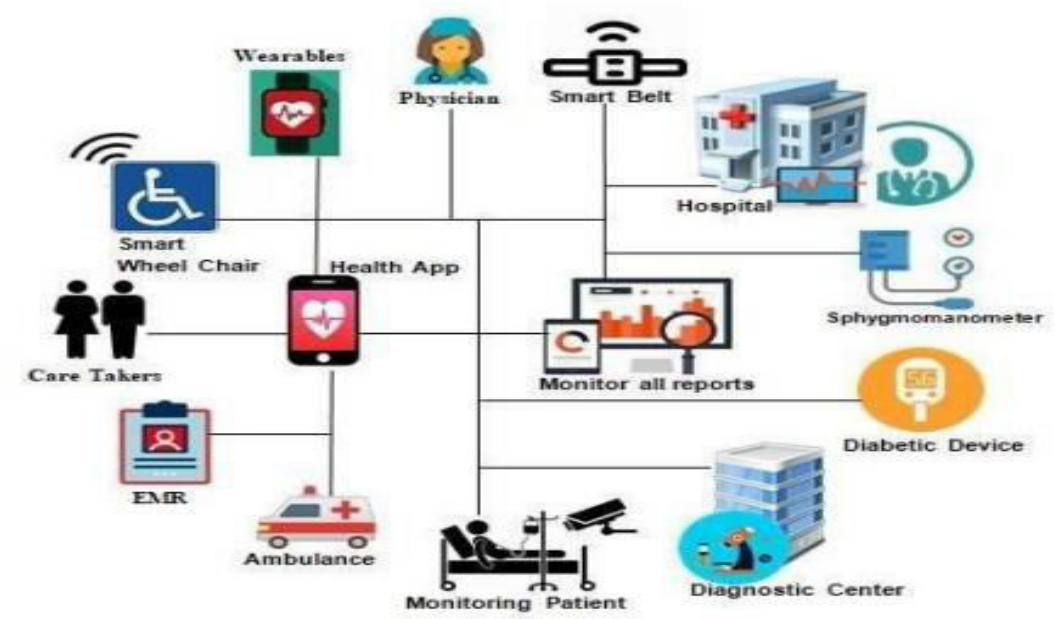

Figure. 1: Internet of medical things [1]

Figure 1 show the various parts that comes under Internet of Medical Things. let us understand what the use of IoT in medical field in next section is.

use of iot in medical field

Internet of Things have heterogeneous architecture where each device communicates with each other and these devices can be controlled and monitored all at once without any problem. IoT system is independent and the devices present in the system share real time data and owner of that system can control, monitor the devices in real time even access these devices remotely. IoT technologies are fast, cost efficient, reliable and have numerous advantages therefore we can find IoT technology in almost every domain. Health Care domain is also adopting IoT technology and it allows Medical professional to give best treatment to the patients. Using IoT technology in medical field increase the accuracy, productivity and reliability in health care system. As talked in [30] about 5G and IoT.

benefits of iomt

IoT technology is transforming many real world sectors like manufacturing unit, smart home automation and so on. Medical field is also a part of this segment which is taking advantages of IoT

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

Technology. IoMT (Internet of Medical Things) is a term used for health care application of IoT Technology. IoMT technology allow doctor to understand the condition of his patient in real time. Health condition is recorded by wearable devices like Smart band that read Heart rate, oxygen levels and that data will be sent to a cloud storage and will be sent to the Doctor and then doctor will analyses the data and if there is a need of any treatment he can assist the patient real time. Using IoMT will reduce the infrastructure cost and save time on consulting as the patient can be treated online, IoMT technology is human-machine real time interaction that make health monitoring easy, fast and cost efficient as it reduces the follow up visits.

literature review

In this section we will discuss about the research paper and give an overview about the related work relevant to our research work. Alam et al. [3] explore at the several communication protocols and standards that can be used in IoMT. The report focused on five scenarios in which IoT in healthcare services can be useful. This survey covers the primary security difficulties that are present in health care Iot network related to security and privacy, However, it excludes the primary methods of communication used in identifying difficulties in healthcare. M. M. Mutlag et al. [4] give an overview of fog computing in the IoMT or Healthcare IoT system. This survey paper discusses about various frameworks and models based on fog computing. survey also covers various objective such as improvement on data security and real time data processing. In survey H. Baali et al. [5] authors provide a detailed overview on different sensor that are used in IoMT Devices. This paper explores about sensors used in Health Care IoT and discuss about the working principals and the operations. Security aspect on health care IoT system were missing in this survey paper and author doesn't discuss about implementation of energysaving methods at device level. In survey S. B. Baker et al. [6] gives an overview of the components, applications and architecture of Internet of Medical Things (IoMT) technology. This survey focuses at how communication technologies like cloud computing and Big Data are being used in IoMT. Since the study focuses solely on the different parts of IoMT, it neglects to address several key issues such as security and privacy. S. Seneviratne et al. [7] authors talk about smart wearable devices that will be used in medical field.in addition to this authors explores security threats that are present in the wearable device. In the context of wearable device authors have discussed it in depth but they have not provided functional use case. They have discussed threats present on wearable in short range communication medium but they haven't talked about the threats on security at long range communication medium. R. Li et al. [8] the authors try to fix the gap and issues that are present in wearable devices. The survey paper talks about architecture, components and use case of health monitoring devices in IoMT. in this survey they haven't discussed about crucial part of these health monitoring system or wearable devices which is to maintain the data integrity and security. The researchers talk about feedback control mechanisms, but they don't mention future technologies. The survey [9] manages the execution of IoT according to the medical care point of view. Architecture, services, security, and IoT standards are all discussed in the survey. IoMT architecture and a security model are presented in this paper. Although the survey focuses on the security of IoT systems, yet doesn't extensively cover the security vulnerabilities, countermeasures methods and techniques, and rise of the new security hazards as per the new standards. M. Sain et al. [10] aim to identify security at three stages of IoMT: machine, communication, and information. Paper on focuses to identify the potential threats at different layers, but it doesn't provide solutions to rectify these security risks. Many medical technologies are being designed to respond to the development of the pervasive

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

environment to provide facilities. majority of these services utilize Techniques of digital signal processing and wireless networks to send healthcare information for inspection and treatment over existing medical devices [11]. One of the trendiest study areas in global health care is the Biomedical signal transfer system based on the Zigbee wireless network [12] [13]. Many studies on the field of biomedical signal processing, also experiments with BAN (Body Area Network)-based bio-information systems were carried out using close transmission systems [14]. The survey [15] provides a complete overview of works that focus on various aspects of a health-care IoT system, such as communication technology, security issues, and use cases. On the other hand, this research, concentrates on the emerging technologies that will drive future Health care IoT systems. In [16], the researchers explain how big data and blockchain can be used to handle medical data in an IoMT scenario. The usage of blockchain, according to the researchers, improves the reliability and security of data gathered by sensor network. In [17] A. Siddique et al. use compressive sensing (CS) to compress the data sensed. By assuming data redundancies, the proposed technique optimizes the power system., which make up a substantial component of biomedical data. The proposed system's edge node is where CS is implemented.

application of iomt

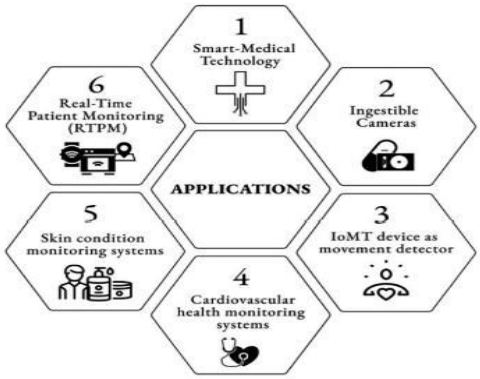

Figure 3: Application of IoMT

Present Health care equipment can be converted into IoMT devices to sense real time patient monitoring by adding few sensors and modems. IoMT devices can be seen easily for example smart wearable devices, smart health care kit, health care mobile application that can be used for medical assistance and medical professional can assist or treat the patient in Real time.

Figure 3 show the various application of IoMT, apart from this some of the IoMT applications are discussed below: -

Chronic disease treatment

IoMT enable devices allows medical professionals to monitor the patient suffering from chronic diseases like hypertension, diabetes and heart related disease. The patient's blood pressure, heart rate, and blood sugar are all tracked using these smart devices and other vital data needed for understanding the medical condition. The information gathered by the smart devices will be used to improve medical treatment. It will be used to monitor the progress of a patient and will be used to decide the future treatment.

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

Tele health assistant

IoMT technology helps medical professional to give treatment to the patient without being physically present at the home of the patient. IoMT give remote monitoring feature that helps to monitor and assist the patient remotely and it will increase the productivity of health care system.

Lifestyle Assessment

IoMT technology makes health supervision easy by remote monitoring in real time. We can monitor the physical activities, calculate the calories burnt, and quality of sleep in the real time this is possible because of the data which is collected by smart wearable device. the data will be used to plan the diet and helps to enhance our health on the go.

security threats to iomt

IoMT Technology gained rapid growth in health sector as it is easy to use, cost efficient and reliable but we have to consider the challenges and security risks that are present in IoMT technology. Present IoMT technology faces some challenges that are discussed below: -

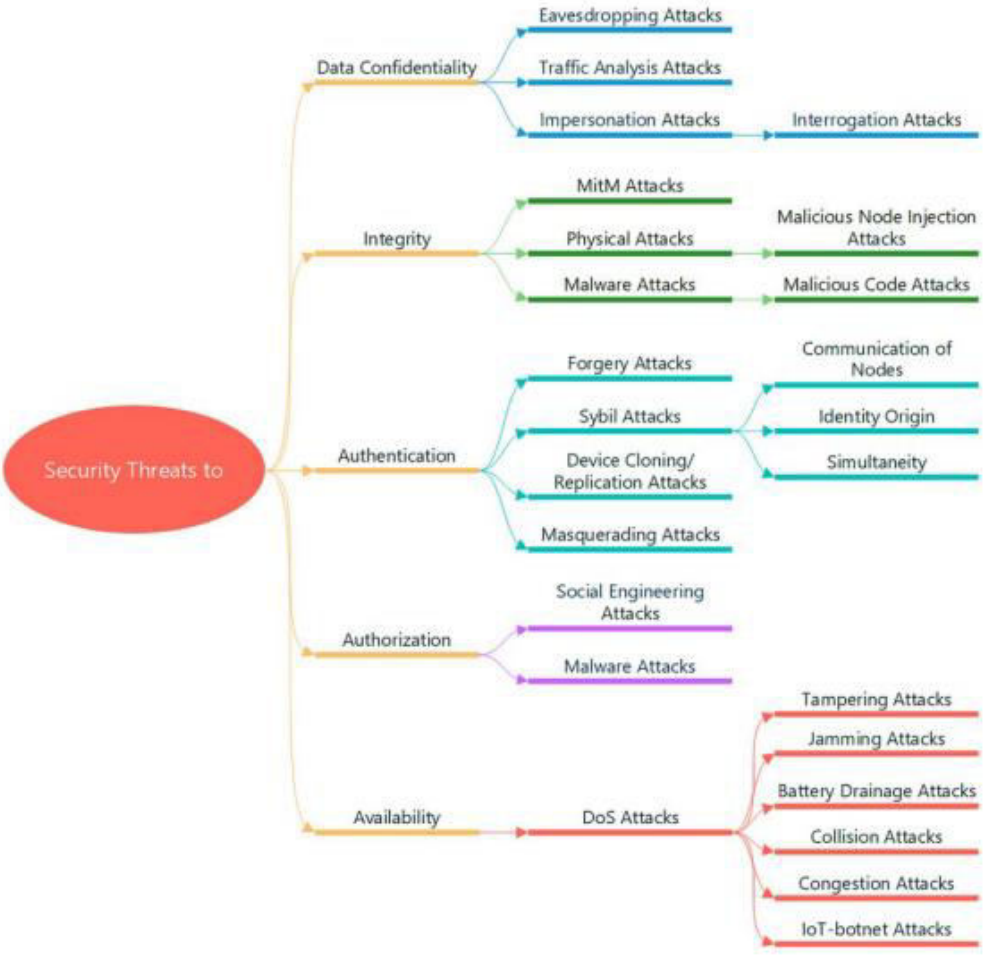

Figure 4. IoMT security threats [24]

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

Confidentiality Threat

Ensures that secret data isn't shared or exposed with anyone who are not authorized to access it [18]. Confidentiality means the protection of a patient's medical information shared with a doctor or medical staff from being revealed to illegal third parties in the context of the IoMT network. [19]. For example, if the confidentiality of transmitted data is breached, an attacker could intervene between the sender (e.g., a healthcare equipment) and the receiver (e.g., a mobile phone) to intercept medical data and steal information [18].

Authentication Threat

One of the most critical safety requirements for an IoMT healthcare system is authentication. Because of the IoMT devices' universal features, PKI (public key infrastructure) -based authentication methods are ineffective and non-extensible [20]. Furthermore, hackers take advantage of a system's poor authentication to gain access to sources based on users' credentials even if they do not have legitimate credentials [21].

Authorization threats

Attackers may use a poor authorization mechanism on an IoMT network to get access to the network without having the proper authorization. As a result of users' lack of security training and awareness Social engineering attacks may be possible with IoMT devices. As a result, a hacker might mislead the IoMT network and pass themselves off as authorized in order to gain control to users' medical equipment. [22]. At the case of medical instruments that monitor health status, this might put the patient's life at risk [23].

Integrity threats

Integrity Assures that data hasn't been tampered with or destroyed unauthorized permission. Integrity maintains the accuracy of patient-related data such as private health information like health reports, medical records, and lab results in the IoMT network. Moreover, since IoMT devices are generally used in untrustworthy environments, Physical hacks that try to compromise device integrity are a threat to them. The integrity of IoMT networks can be compromised by a man-in-the-middle (MitM) attack, in which attacker interposes in the connection between the two users and may alter the transferred data without being detected [25]. Clinical data acquired by an IoMT network, for example, can be transferred to a remote server or maintained locally in the smart device's internal memory.

Availability threats

Availability Helps ensure that systems are in good working order and that access to authorised users is not restricted [26]. As a result, medical data is always available and usable when requested by a valid authority. When a patient requires uninterrupted care services.In an IoMT network, it's critical to ensure the availability of device and network resources. [27] [28]. Due to limited resources, IoMT network is becoming extremely vulnerable to denial-of-service (DoS) attack. Tampering attacks, battery drainage attacks and congestion are all kinds of DoS attacks that can be used on different network tiers and have different impacts on the IoMT network [29]

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

Conclusion and future work

IoT based health care system or IoMT technology are in developing stage, many researches have been done to enhance the performance and increase the usage of IoMT technology, side by side the researchers are looking after at the drawback of health care IoT system. Many researchers have proposed solution to increase the capabilities of IoMT and they also work to resolve the challenges present in IoMT technology. Using IoMT technology increases the health care facilities by remote monitoring and other features but we cannot neglect the issues like data theft, these challenges are matter of concern and it will be resolved in near future. IoMT networks are sensitive to a series of security vulnerabilities, posing a substantial danger to the privacy and safety of patients. Government bodies should also enforce some strict law that will protect the critical data, and should monitor the law enforcement frequently. This small act can increase the security and privacy while using IoMT technology and build trust among people to use these health care facilities fearlessly.

References

1. Dilawar, Nimra & Rizwan, Muhammad & Akram, Saima & Ahamd, Fahad. (2019). Blockchain: Securing Internet of Medical Things (IoMT).
2. D. Yach, C. Hawkes, C. L. Gould, and K. J. Hofman, "The global burden of chronic diseases: overcoming impediments to prevention and control," Journal of the American Medical Association, vol. 291, no. 21, pp. 2616–2622, 2004.
3. M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. L. Moullec, "A survey on the roles of communication technologies in IoT-based personalized healthcare applications," IEEE Access, vol. 6, pp. 36611–36631, 2018.
4. M. M. Mutlag, M. K. A. Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," Future Gener. Comput. Syst., vol. 90, pp. 62–78, Jan. 2019.
5. P. Chavan, P. More, N. Thorat, S. Yewale, and P. Dhade, "ECG - Remote patient monitoring using cloud computing," Imperial Journal of Interdisciplinary Research, vol. 2, no. 2, 2016.
6. 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.
7. S. Seneviratne, "A survey of wearable devices and challenges," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2573–2620, 4th Quart.,2017.
8. R. Li, D. T. H. Lai, and W. Lee, "A survey on biofeedback and actuation in wireless body area networks (WBANs)," IEEE Rev. Biomed. Eng., vol. 10, pp. 162–173, 2017.
9. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, "The Internet of Things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.
10. M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," in Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT), Bongpyeong, South Korea, 2017, pp. 699–704.
11. W. Ryu, E. Kim, K. An, S. Woo and Y. Chang, "A bluetooth based 5-HD measurement system for u-Healthcare," International Journal of Control and Automation, vol. 6, no. 1, (2013), pp. 141-150.
12. Y. Cha and G. Yoon, "Ubiquitous health monitoring system for multiple users using a zigbee and WLANuual-network," telemedicine and e-Health, vol. 15, no. 9, (2009), pp. 891 897.

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

13. Y. Chang and B. Kim, "A wireless ECG measurement system based on zigbee USN," The Korea Information Processing Society Transactions: Part C, vol. 18-C, no. 3, (2011), pp. 195- 198.
14. C. Otto, A. Milenkovic, C. Sanders and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," Journal of Mobile Multimedia, vol. 1, (2006), pp. 307-326.
15. M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," Comput. Netw., vol. 153, pp. 113–131, Apr. 2019.
16. M. Simic, G. Sladic, and B. Milosavljevi´c. (Jun. 2017).(PDF) A Case Study IoT and Blockchain Powered Healthcare. Accessed: Apr. 13, 2019. [Online]. Available: https://www.researchgate.net/publication/317433655_A_Case_Study_IoT_and_Blockchain_powered_Healthcare
17. A. Siddique, O. Hasan, F. Khalid, and M. Shafique, "ApproxCS: Nearsensor approximate compressed sensing for IoT-healthcare systems," 2018. [Online]. Available: arXiv: 1811.07330 v1.
18. Menezes Alfred J, Oorschot Paul C, Vanstone Scott A. Handbook of applied cryptography; 1996.
19. Hash Joan, Bowen Pauline, Johnson Arnold, et al. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule Technology Administration. Illinois: American Health Information Management Association; 2008.
20. Munir-Kashif A, Mohammed L. Biometric Smartcard Authentication for Fog Computing. Int J Netw Sec Appl. 2018;10(6):35-45. https://doi.org/10.5121/ijnsa.2018.10604.
21. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the Internet of Things: security and privacy issues. IEEE Internet Comput. 2017;21(2):34-42. https://doi.org/10.1109/MIC.2017.37
22. Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the Internet of Things. IEEE Commun Surv Tutor. 2019;21(2):1636-1675. https://doi.org/10.1109/COMST.2018.2874978.
23. Halperin D, Heydt-Benjamin TS, Ransford B. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. 2008 IEEE Symposium on Security and Privacy. IEEE; 2008:129-142.
24. M. Papaioannou et al., "A survey on security threats and countermeasures in internet of medical things (IoMT)," Trans. emerg. telecommun. technol., 2020.
25. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the Internet of Things: security and privacy issues. IEEE Internet Comput.2017;21(2):34-42. https://doi.org/10.1109/MIC.2017.37.
26. Deogirikar Jyoti, Vidhate Amarsinh. Security Attacks in IoT: A Survey. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC); 2017:32-37.
27. WHO. What do We Mean by Availability, Accessibility, Acceptability and Quality (AAAQ) of the Health Workforce?. Geneva, Switzerland: WHO; 2014.
28. Scholl M, Stine K, Hash J, et al. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Vol 1; 2008.

Webology, Volume 18, Number 4, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I4/145

29. Mantas G, Stakhanova N, Gonzalez H, Jazi HH, Ghorbani AA. Application-layer denial of service attacks: taxonomy and survey. Int J Inf Comput Sec. 2015;7(2-4):216-239
30. Upadhyay, D., Tiwari, P., Mohd, N., & Pant, B. (2022, April). Capacity Enhancement for Cellular System using 5G Technology, mmWave and Higher order Sectorization. In 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 422-427). IEEE.