

Facilitating Healthcare Sector through IoT: Issues, Challenges, and Its Solutions

Ruby Dahiya¹, Arunkumar B², Virender Kumar Dahiya³, Nidhi Agarwal^{1,*}

¹School of Computing Science and Engineering, Galgotias University, Greater Noida, UP, India

²School of Computer Science and Engineering, VIT-AP University, India

³School of Business, Galgotias University, Greater Noida, UP, India

Abstract

INTRODUCTION: Nowadays, the Internet of Things (IoT) is one of the thriving technologies which incredibly enhances the standardization and modernization of any field. Healthcare has been facing so many conundrums that now could be catered to by the technology of IoT. IoT has found its application in the healthcare sector in the form of various health monitoring devices as well as smart wearables for efficiently monitoring the health status of patients and improving upon the traditional infrastructure. Further, IoT in healthcare introduces and identifies the intelligent trend and directions by which one can be aware of health, fitness, and ailments. In this way, IoT progressively adds to the medical field and healthcare. At the same time, there are some challenges which are pertaining to IoT in healthcare which include the breaching of confidential information such as patient data.

OBJECTIVES: The paper aims to discuss the solutions to this problem in detail.

METHODS: The paper fulfils its objectives through the deployment of technology such as blockchain and fog computing. This paper delineates the comparative study of how IoT assimilates healthcare.

RESULTS: The paper discusses various identified technologies to overcome the challenges in IoT for healthcare.

CONCLUSION: The amalgamation of IoT with healthcare shows efficacious outcomes. It can even create the difference between life and death. IoT overcomes the shortcomings of the traditional healthcare system. However, there are some challenges of securities associated with the IoT technology which can be coped with some measures such as cryptography, and blockchain etc.

Keywords: iot, healthcare, wearable devices, security, blockchain, fog computing

Received on 29 July 2023, accepted on 02 November 2023, published on 06 November 2023

Copyright © 2023 R. Dahiya *et al.*, licensed to EAI. This is an open access article distributed under the terms of the [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/), which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetiot.v9i4.4317

*Corresponding author. Email: nidhiagarwal82@gmail.com

1. Introduction

The healthcare system has been in a great dependency state. The causes for the same can be given to factors such as a rise in the number of an aging population, increased expenditure of hospitals and clinics and a rise in the variety of chronic diseases. However, over a period, technology somehow bolsters and overcomes many issues. Similarly, IoT (Internet of things) is such a technology that is biblically corroborated in the field of healthcare and aids it to help resolve issues that are pertaining to the present-day healthcare system. IoT now becomes the centre of interest as it has been incorporated into smart cities, smart homes,

environmental monitoring, and healthcare, etc. IoT has remarkable benefits which it serves the health sector. IoT can connect with several sensors, vehicles, and home appliances, etc. together with the internet [1]. The paradigm of IoT brings the most efficient and reliable solutions. It facilitates real-time health monitoring of patients which is of utmost significance to patients suffering from chronic diseases such as high blood pressure, diabetes since their health conditions are required to be continuously monitored and the critical data so generated can then be transferred to the medical staff who can then act upon based on the insights gained from the data [2].

However, there are some challenges pertaining to this system such as the management of big data generated by these IoT-enabled sensor devices and other factors related to security in the form of managing the confidentiality, integrity, availability, and authentication of the generated data. However, IoT technology somewhat has security issues that can lead to leakage of private data. It breaches confidentiality which is quite dangerous to trust. So, it requires sky-scraping security to maintain confidentiality. The system should have high-security encryption/decryption algorithms like AES (Advanced Encryption Standard) which provides the utmost security to the devices associated with IoT [3]. This paper is organized in five sections. Section 2 presents the detailed literature survey for related works has been discussed. Section 3 of the paper highlights the applications of IoT in healthcare. Section 4 points out the various challenges of IoT application in healthcare sector. Section 5 suggests solutions to the challenges with the aid of variety of technologies. Section 6 concludes the paper.

2. Literature review

The IoT becomes the epicentre which assists us in formulating the integrated and synchronized wearables that directly convey and guide us for our health. On the other side, there is an IoT gateway which acts as an intermediate hub in between wearables and IoT servers. And at the same time, physicians appear as the real time observer of patients and have the control of sensors of their wearables [2]. IoT has extraordinary potential which is completely intertwined with our lives. Like the OSI model, it also has several layers on which its functionalities depend, which are: 1. Sensing layer 2. Access layer 3. Network layer 4. Middleware Layer 5. Application Layer.

IoT technology predominantly depends upon sensors by which it collects data from the physical surroundings and our body. Further, this data will be pre-processed and used for analysis and treatment [4]. However, there are also some privacy shortcomings associated with the contrivance of IoT technology and it is quite challenging to impede the data without affecting data utility, data sharing and model learning etc. Wearable devices allow transfer of data which comprises personal information as well which can be tracked and attacked which needs to be protected with the strong security algorithm [3,5]. Ghosh et al. (2023) embarked on a comprehensive study to assess water quality through predictive machine learning. Their research underscored the potential of machine learning models in effectively assessing and classifying water quality. The dataset used for this purpose included parameters like pH, dissolved oxygen, BOD, and TDS. Among the various models they employed, the Random Forest model emerged as the most accurate, achieving a commendable accuracy rate of 78.96%. In contrast, the SVM model lagged behind, registering the lowest accuracy of 68.29% [35].

Alenezi et al. (2021) developed a novel Convolutional Neural Network (CNN) integrated with a block-greedy algorithm to enhance underwater image dehazing. The method addresses color channel attenuation and optimizes local and global pixel values. By employing a unique Markov random field, the approach refines image edges. Performance evaluations, using metrics like UCIQE and UIQM, demonstrated the superiority of this method over existing techniques, resulting in sharper, clearer, and more colorful underwater images [36].

Sharma et al. (2020) presented a comprehensive study on the impact of COVID-19 on global financial indicators, emphasizing its swift and significant disruption. The research highlighted the massive economic downturn, with global markets losing over US \$6 trillion in a week in February 2020. Their multivariate analysis provided insights into the influence of containment policies on various financial metrics. The study underscores the profound effects of the pandemic on economic activities and the potential of using advanced algorithms for detection and analysis [37].

3. Applications in IoT sector of healthcare

With this crucial technology trend, the future of medicine and the healthcare system is invariably revolutionized and provides innumerable benefits. The Internet of Things is considered as a gigantic network which is formulated to extend the connectivity of the internet into physical devices. Figure 1 illustrates various applications of IoT in the healthcare sector which are highly prevalent and are evident in the form of various health monitoring systems and smart wearables which are utilized nowadays to enable remote monitoring of patients suffering from chronic diseases like diabetes, hypertension, chronic obstructive pulmonary disease.

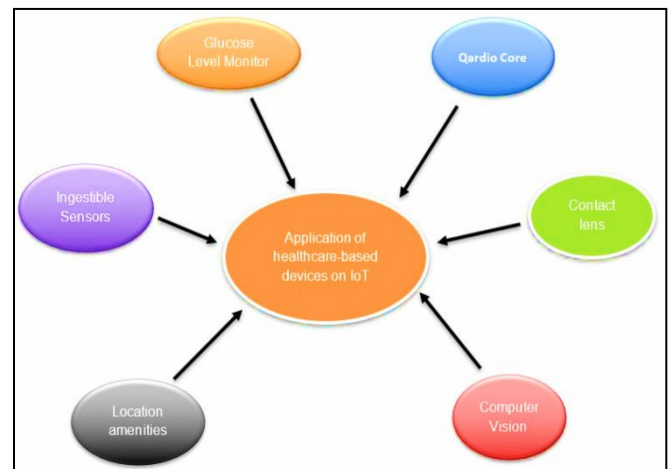


Figure 1. Application of healthcare-based devices on IoT

3.1. QardioCore

QardioCore is a wireless ECG Monitor which records the complete heart performance of a patient on a smartphone and the data so generated can be sent to the doctor for further analysis. With real-time data sharing and analysis, QardioCore offers a new way of chronic conditions and physical activity performance management. Via this technology, the wearables have the tendency to raise the alerts for patients who are experiencing palpitations, strokes, arrhythmias, etc. so that without any delay hospitals can dispatch the ambulance which absolutely creates the difference between life and death. It is particularly suited for people with increased health risks caused by family predisposition, a history of heart attacks or strokes, high blood pressure, high cholesterol, diabetes, and excess weight [11].

3.2. IoT Based Glucose Level Monitor

Diabetes is a metabolic disease that proliferates the glucose level of a patient. Proper monitoring of glucose levels can help with medication, physical activity, and meal planning. Continuous glucose monitoring works through a minuscule sensor inserted under the skin which continuously tests the glucose level and the information generated is sent wirelessly to a monitor which may be a part of an insulin pump or a separate device. Some CGMs transmit the data directly to a smartphone or tablet.

3.3. IoT Based Contact Lenses

The IoT-based contact lens consists of a micro camera and sensors that support Wi-Fi signals, and the device is connected to a smartphone to monitor human health conditions such as diabetes. The patient's sugar level can be measured by tears and if any abnormal situation is found, then the necessary health alert may be sent to the health consultant.

3.4. Ingestible Sensors

This is one of the incredible developments in the field of IoT in healthcare wherein patients now can swallow devices with sensors that seem like sensors. And these sensors are outrightly ingestible. Once they are ingested, then the information can be tracked via the patient's mobile application. Many times, patients forgot to take their proper medication on time which leads to uncertainties and inconsistencies in their health. These sensors perfectly eradicate this issue as it is successfully able to inform patients about their medication.

3.5. Location Amenities

Several times, items like wheelchairs, defibrillators, nebulizers, pumps, and other medical paraphernalia can be misplaced or not able to be found on time which could lead to many problems and time delays for the treatment of patients. So, here again, IoT comes into the picture wherein sensors can be tagged to each specific piece of equipment so that health staff can be located and found easily.

4. Challenges in IoT on Healthcare

Despite having so many merits and advanced technology which undoubtedly bolsters our medical and healthcare system, at the same time it has some disadvantages as well which hampers the growth of IoT technology with healthcare. Cyberattacks have catastrophic effects on the domain of healthcare. Even the medical devices which assuage the patients and tackle their diseases are not secure. They are also vulnerable.

4.1. Vulnerabilities in Privacy

This is one of the consequential threats when it comes to IoT as this technology captures and transmits data in real-time via sensors. The data comprises valuable and confidential information about the patient. And there is a high possibility of breaching this information which is a contravention act. Most IoT devices lack the data protocols and standards. Also, it has been found that there is vagueness regarding data ownership and regulation which makes that data more susceptible to cybercriminals. As a result, patients, and doctors both must compromise Personal Health Information (PHI). Cybercriminals have been posing the biggest obstruction as they can misuse the patient's data to generate fake IDs to buy drugs and other stuff pertaining to medicine. They can also forge insurance claims in the name of a patient [1].

4.2. Severity of Big data

Umpteen data is generated and regulated daily which is considered as Big Data. And it has its merits and demerits as well. It significantly helps in predicting the epidemics, solutions for the various disorders, and may prevent the deaths. Big data also promotes well-being and improves the quality of life. Furthermore, it offers a variety of services including industrial automation, system health monitoring, predictive maintenance, and remote monitoring. But despite these advantages, it encompasses some serious drawbacks which hampers the IoT in healthcare.

4.3. Coalescing multiple devices

It has been found that the amalgamation of multiple devices and protocols causes impediments which restricts the implementation of IoT in the healthcare sector. The reason being is that the device manufacturers still have not reached a consensus about the communication protocols and standards. As a result, they create their own separate ecosystem of IoT devices which causes the integration problems and breaching of confidential information by unauthorized users which degrades the overall security mechanism of the system. Therefore, this non-uniformity hampers the process and dwindles the opportunity to obtain the efficiency and scalability of IoT in healthcare [16].

4.4. Med Jacking

The healthcare sector is the most targeted sector and prone to vulnerabilities in which hackers tamper with the medical devices by which patients and doctors both suffer and create unnecessary conundrums. Some cases also witnessed this Med jacking wherein hackers and unauthorized users hijack the medical devices. They purposely infected the medical devices with different types of malwares, and this can create the difference between life and death. The hackers can get the outright access and can control the patient's drug dosage and other stuff which causes damage to the patient. From a survey, in Aug 2015, The FDA recommended that all the hospitals in California deter the utilization of medical devices which are prone to cyber-attacks [17].

4.5. Network Segmentation

Segmentation plays a vital role in maintaining the quality of security strategy. In this, there is a splitting of networks into subnets to enhance or ameliorate the performance and security of medical IoT. This contrivance enables us to divide traffic into external and internal users. But the dearth of network segmentation can affect the hospitals and medical departments severely with respect to the patient's data. Without a network segmentation hackers and unauthorized users easily break the system and gain the controls.

4.6. Hackable Devices

Insulin and Infusion pumps: This is profoundly useful in the sector of healthcare as it administers blood, saline, and other fluids with the control of IoT. But, at the same time, it accompanies lots of malicious threats and vulnerabilities.

Cardiac Devices: These days, a lot of implantable devices available, among all implantable devices is common which is now considered as a disruptive one as it is associated with security vulnerabilities and poses a cybersecurity

challenge. Researchers even found that even simple denial-of-service (Dos) attacks break into the device.

Security Cameras: In this, the botnet plays a significant role in creating the disruption. It has the capability to launch the largest DDOS (Distributed denial-of-service) attack on connected devices via IoT. This will be accessed by default usernames and passwords which leads to the breach of the patient's data [20].

5. Technologies to overcome the challenges in IoT for Healthcare

5.1. Cloud Computing

Cloud Computing refers to the shared pool of configurable computing resources which is ubiquitous, dynamic in nature, and facilitates on-demand access of computing resources such as network infrastructures, servers, storage, applications, etc. It supports an expandable, coherent, and coordinated business model which supports mobile devices [21].

Software-as-a-Service (SaaS): SaaS consists of industrial applications with web or program interface providing subscribe-and-use features to industry clients with the final product where everything is managed by the service provider. In SaaS, end users do not possess the control of the cloud infrastructure and the applications are available as services which can be accessed via different types of client devices such as web-browser, app. Industry Machinery Catalyst from Siemens is a SaaS designed for industrial use [21].

Platform-as-a-Service (PaaS): PaaS allows industries for self-development of applications where the clients have the control over the application and the configuration environment. It provides a facility for the consumer to execute consumer-created or acquired applications onto the cloud infrastructure where the user does not control the cloud infrastructure and can only control the deployed applications using given configurations. Software firms including Cumulocity, Bosch IoT, and Carriots offer PaaS for IoT industries [21].

Infrastructure-as-Service (IaaS): IaaS offers a facility to access computing resources such as network, storage, and operating system where users can deploy, execute, and control any software like operating system and other applications. In some cases, the user can control selected networking components. In IaaS, clients can use the cloud to operate a virtual data centre. It is widely used to deploy PaaS and SaaS as well. Software companies like Microsoft Azure, Google Compute Engine, and IBM Smart Cloud Enterprise are some of the firms that offer IaaS for IoT industries [23].

5.2. Network Controlling

It is the fundamental part that one needs to have an outright dominance over the network so that one can monitor the breaches and malicious activities. This scheme assists in reducing the risks as the network has high intelligence, scanners and varieties of conducive solutions which ensures the safeguarding against the cyber-attacks. In a way, it impedes the interception of data by the intruders as they cannot decrypt it. Hence, there should be absolute conspicuousness over the network so that they can identify the anomalies at the earliest and further the vulnerabilities can be addressed [23].

5.3. Security via Cryptography

Cryptography is always considered as the promising solution when it comes to preventing security as it has the capability to counteract both hardware and software. It covers all three components of security: Confidentiality, Integrity, and Authentication. In hardware, the various devices and sensors store asymmetric keys in themselves to establish secure connections in the form of HTTP which acts as a tunnel between sensors and consumers. Also, to deal with the various intricacies associated with insecure encrypted IoT networks, there is an authentication pattern for implantable healthcare devices that has been decided to use an albeit password system. This allows the ultraviolet light to seal encrypted keys in the patient's body [24]. Cryptography ensures the data security and data privacy and enhances the reliability of any network. There are several algorithms pertaining with cryptography to tackle the security issues of medical IoT. But two major algorithm which supremely address the problems are:

- AES (Advanced Encryption Standard)
- DH (Diffie–Hellman) Algorithm

5.4. Fog Computing

The basic idea of fog computing is to extend the cloud near to the deployed IoT devices. It solves the problems faced by cloud computing during IoT data processing and acts as an intermediate layer between clouds and devices. The requirement for the adoption of fog technology in IoT emerges from the consistent release of time-sensitive and critical data from machines and sensors which needs immediate action and rapid response. The detailed working of fog is shown in figure 3. Any delay in action at proper time may create a perilous situation for medical staff. The major challenges including handling the diversity of data, different protocols, and different data sources are handled by the implementation of fog computing technology in IoT. This technology addresses the weakness of industrial automation by enabling new functionalities along with the additional features and helps in enriching the current functionalities [27].

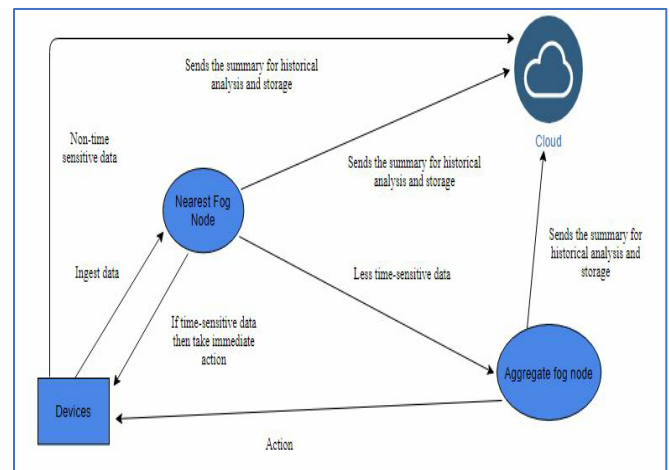


Figure 2. Figure depicting the working of Fog

5.5. Blockchain

Blockchain is a term typically used to describe a collection of records, linked with each other which is strongly resistant to alteration and is protected by cryptography. This property of blockchain could prove to be of utmost usefulness to the healthcare sector where the data needs to be fully secured from any kind of inconsistency, redundancy, and corruption. Blockchain technology can be used to store the critical data so that the data does not get stored at a centralized database. Moreover, blockchain technology can also be used in the pharmaceutical sector to reduce the discrepancy regarding the medicines since most of the pharmaceutical companies suffer huge losses due to this problem as the hospitals tend to return fake products back to the company in place of the original ones.

5.6. Big Data on medical IoT

Data is everywhere and since the world is constantly revolutionizing with digital means as a result, associated data is also generating tremendously. Similarly, data in huge volume is generated in the healthcare sector. Big data in healthcare is a term which refers to enormous volumes of information generated by digital technologies which can be structured, semi-structured and unstructured. In essence, big data is highly beneficial as it gives us data to analyse, helps in predicting various epidemics etc [32]. Cloud storage also manages with the help of Big Data technology [30].

Big Data Analytics: Big data analytics (BDA), the combination of two produces effective outcomes with respect to data management. Analysing with respect to big

data is the mechanism of scrutinizing and investigating the huge volumes of data which pile up from the various sources in different formats. There are various analytics technologies available which assist us in analysing the useful insights or information from the large chunks of data which are data mining, deep learning, deep learning algorithms, nature language processing tools (NLP), artificial intelligence (AI) and predictive analytics etc. These tools incredibly support data analytics and help in contextualizing the data or data sets. Further, it extends the flexibility by which an individual can draw important conclusions.

Big Data in healthcare can be explained through its fundamental characteristics which are:

Volume: It is the amount of data, which is generated by X-rays, ultrasounds, MRI (magnetic resonance imaging) and many others.

Velocity: It is referred to as the speed at which the data is generated which widens the scope analysis.

Variety: The data obtained from healthcare domain can be of different formats

Big Data in biomedical research: In a biological system, even a human cell exhibits a lot of intricacies which poses many challenges to study and requires umpteen amounts of data to interpret the processes or mechanism. Now, here Big Data bolsters the scenario as it gives a widened field to study data sets. The more data we have, the better understanding we gain. Analysis of big data can be a great help in imparting strategic ideas for the healthcare system. It highly supports the omics discipline in which instead of studying a single gene, it paves the way to study the whole genome of an organism [32].

EMR (Electronic medical record): It adds on to the digitization of healthcare and big data which is an electronic version of a patient's medical history which is accessed by authorized users. The scheme of EMR automates the access to information which helps in strengthening the relationship between patients and clinicians. The main advantage of EMR is it has the capability to reduce medical errors and indeed improves the accuracy and clarity of data [33].

Authentication: Authentication has a special power to conquer the hackers. It plays a critical role in the security of web applications. User needs to provide a login name or password to authenticate his identity. Through the credentials, we can verify the authenticated users and hence prevent the third party or unsanctioned users. The authentication rules operate with HTTP, SSL or TLS embedded within the request. For the authentication process, strongest passwords should be a prerequisite. There should be proper assuring the authentication to the application, server, and device. There should be the

security of password recovery mechanisms [34]. These ways can assist in validating the specific user and that user can be patient and doctor. Hence, to some extent, mitigate the security challenges. Here are some IoT based solutions which effectively deal with the cybersecurity challenge and create the extra layer of security. In a way, it safeguards the healthcare domain. This is specifically designed for hospitals as it safeguards the assets of healthcare IoT such as inventory management and vulnerability research etc. It certainly impedes from malwares and ransomware attacks from breaking into the system.

6. Conclusion

Healthcare is one of the most critical and prominent domains which is incredibly supported by IoT technology. The sensors of IoT play a crucial role and cater to varieties of facilities such as remote operating of patients and tracking their health status from any corner. The amalgamation of IoT with healthcare shows efficacious outcomes. It can even create the difference between life and death. IoT overcomes the shortcomings of the traditional healthcare system. However, there are some challenges of securities associated with the IoT technology which can be coped with some measures such as cryptography, and blockchain etc. In a way, medical IoT is progressively evolving and solving the unprecedented problems pertaining to healthcare and the medical field.

References

- [1] Haghi, M., Neubert, S., Geissler, A., Fleischer, H., Stoll, N., Stoll, R., & Thurow, K., A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring. *IEEE Internet of Things Journal*, 7(6), 5628-5647 (2020)
- [2] Patel, N. Internet of things in healthcare: applications, benefits, and challenges. (2017) Internet: <https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-andchallenges.html>, [Accessed May 25, 2021].
- [3] Sharma, S., Chen, K., & Sheth, A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing*, 22(2), 42-51(2018).
- [4] Vijayakumar, K., & Bhuvanewari, V.. A Ubiquitous first look of IoT Framework for Healthcare Applications in International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-7). IEEE (2020).
- [5] Alharam, A. K., & El-madany, W., Complexity of cyber security architecture for IoT healthcare industry: a comparative study in 5th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 246-250). IEEE (2017).
- [6] Ugrenovic, D., & Gardasevic, G. , CoAP protocol for Web-based monitoring in IoT healthcare applications. In 2015 23rd Telecommunications Forum Telfor (TELFOR) (pp. 79-82). IEEE (2015).

- [7] Singh, I., & Kumar, D., Improving IOT Based Architecture of Healthcare System in 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 113-117). IEEE (2019).
- [8] Hamim, M., Paul, S., Hoque, S. I., Rahman, M. N., & Baqee, I. A., IoT based remote health monitoring system for patients and elderly people in International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 533-538). IEEE (2019).
- [9] Anand, S., & Routray, S. K.. Issues and challenges in healthcare narrowband IoT in International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 486-489). IEEE, (2017).
- [10] Bansal, M., & Gandhi, B., IoT based development boards for Smart Healthcare Applications in 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-7). IEEE (2017).
- [11] Smart Wearable ECG EKG Monitor - QardioCore (2021) <https://www.getqardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone>
- [12] IoT Security in Healthcare: What You Need to Know Before Development Start | Aimprosoft. (2021). <https://www.aimprosoft.com/blog/iot-security-in-healthcare-software-development/>
- [13] Overcoming the Legacy Systems Challenge in Software Development for the Healthcare Industry - VARTEQ Inc. (2021), <https://varteq.com/overcoming-the-legacy-systems-challenge-in-software-development-for-the-healthcare-industry/>
- [14] Bohn, R. & Messina, John & Liu, Fang & Tong, Jin & Mao, Jian. , NIST Cloud Computing Reference Architecture. 594-596. 10.1109/SERVICES.2011.105. (2011).
- [15] Gilchrist, A.. Industry 4.0: the industrial internet of things. Apress (2016).
- [16] Mell, P., & Grance, T.The NIST definition of cloud computing. National Institute of Standards and Technology. Information Technology Laboratory, Version, 15(10.07) (2009).
- [17] IoT Security in Healthcare: What You Need to Know Before Development Start | Aimprosoft. (2021). www.aimprosoft.com/blog/iot-security-in-healthcare-software-development/
- [18] Rani, D. J., & Roslin, S. E. Light weight cryptographic algorithms for medical internet of things (IoT)-a review. In 2016 Online International Conference on Green Engineering and Technologies (IC-GET) (pp. 1-6). IEEE (2016)
- [19] Aazam, M., Zeadally, S., & Harras, K. A. Deploying fog computing in industrial internet of things and industry 4.0. IEEE Transactions on Industrial Informatics, 14(10), 4674-4682, (2018).
- [20] Dastjerdi, A. V., & Buyya, R. Fog computing: Helping the Internet of Things realize its potential. Computer, 49(8), 112-116, (2016).
- [21] How Using Blockchain in Healthcare Is Reviving the Industry's Capabilities. (2021). <https://builtin.com/blockchain/blockchain-healthcare-applications-companies>
- [22] Selvaraj, S., Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl. Sci. 2, 139 <https://doi.org/10.1007/s42452-019-1925-y> (2020).
- [23] Electronic Health Record Systems: Features, EHR Vendors, and Adoption Advice. (2021). <https://www.altexsoft.com/blog/electronic-health-record-systems/>
- [24] The Top 19 Internet of Things (IoT) Security Solutions - Security Boulevard. (2021). <https://securityboulevard.com/2020/12/the-top-19-internet-of-things-iot-security-solutions/>
- [25] Dimitrov, D. V. Blockchain applications for healthcare data management. Healthcare informatics research, 25(1), 51. (2019).
- [26] Naresh, V. S., Pericherla, S. S., Murty, P. S. R., & Reddi, S. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions
- [27] Shareem Thahir on BuzzFeed. (2021), <https://www.buzzfeed.com/cabotsolutions>
- [28] Blockchain in healthcare use cases - Itransition. (2021), <https://www.itransition.com/blog/blockchain-in-healthcare>
- [29] 12 Tell-Tale Signs of Blockchain Adoption Amidst COVID-19. (2021), <https://appinventiv.com/blog/blockchain-adoption-amidst-coronavirus/>
- [30] Agarwal N., Jain A., Gupta A., Tayal D.K. Applying XGBoost Machine Learning Model to Succor Astronomers Detect Exoplanets in Distant Galaxies. In: Dev A., Agrawal S.S., Sharma A. (eds) Artificial Intelligence and Speech Technology. AIST 2021. Communications in Computer and Information Science, vol 1546. Springer, Cham. https://doi.org/10.1007/978-3-030-95711-7_33, (2022). Information Science, 2021.
- [31] Agarwal, N., Srivastava, R., Srivastava, P., Sandhu, J., Singh, Pratap P. Multiclass Classification of Different Glass Types using Random Forest Classifier. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 1682-1689.
- [32] Agarwal, N., Singh, V., Singh, P. Semi-Supervised Learning with GANs for Melanoma Detection. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 141-147.
- [33] Tayal, D.K., Agarwal, N., Jha, A., Deepakshi, Abrol, V. To Predict the Fire Outbreak in Australia using Historical Database. 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2022. p. 1-7.
- [34] Agarwal, N., Tayal, D.K. FFT based ensemble model to predict ranks of higher educational institutions. Multimed Tools Appl 81, 2022.
- [35] Ghosh, H., Tusher, M.A., Rahat, I.S., Khasim, S., Mohanty, S.N. (2023). Water Quality Assessment Through Predictive Machine Learning. In: Intelligent Computing and Networking. IC-ICN 2023. Lecture Notes in Networks and Systems, vol 699. Springer, Singapore. https://doi.org/10.1007/978-981-99-3177-4_6
- [36] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. <https://doi.org/10.3390/w13233470>
- [37] G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 614-617, doi: 10.1109/CSNT.2015.76.