Progression and Challenges of IoT in Healthcare: A Short Review

S M Atikur Rahman
Department of Industrial, Manufacturing and Systems Engineering
University of Texas at El Paso, El Paso, TX 79968, USA

Sifat Ibtisum
Department of Computer Science
Missouri University of Science and Technology,
Rolla, Missouri

Priya Podder
Dhaka National Medical College
Dhaka 1100, Bangladesh

S.M. Saokat Hossain
Department of CSE
Jahangirnagar University
Savar 1342, Bangladesh

ABSTRACT
Smart healthcare, an integral element of connected living, plays a pivotal role in fulfilling a fundamental human need. The burgeoning field of smart healthcare is poised to generate substantial revenue in the foreseeable future. Its multifaceted framework encompasses vital components such as the Internet of Things (IoT), medical sensors, artificial intelligence (AI), edge and cloud computing, as well as next-generation wireless communication technologies. Many research papers discuss smart healthcare and healthcare more broadly. Numerous nations have strategically deployed the Internet of Medical Things (IoMT) alongside other measures to combat the propagation of COVID-19. This combined effort has not only enhanced the safety of frontline healthcare workers but has also augmented the overall efficacy in managing the pandemic, subsequently reducing its impact on human lives and mortality rates. Remarkable strides have been made in both applications and technology within the IoMT domain. However, it is imperative to acknowledge that this technological advancement has introduced certain challenges, particularly in the realm of security. The rapid and extensive adoption of IoMT worldwide has magnified issues related to security and privacy. These encompass a spectrum of concerns, ranging from replay attacks, man-in-the-middle attacks, impersonation, privileged insider threats, remote hijacking, password guessing, and denial of service (DoS) attacks, to malware incursions. In this comprehensive review, we undertake a comparative analysis of existing strategies designed for the detection and prevention of malware in IoT environments.

Keywords
Internet of Things (IoT), Internet of Medical Things (IoMT), cloud computing, medical signals, malware threats, smart health care, artificial intelligence, machine learning (ML).

1. INTRODUCTION
The role played by information systems has grown significantly, particularly within the healthcare industry [1]. From electronic health records to cloud-based systems, information technology (IT) has consistently benefited the healthcare sector. As IT continues to advance, information systems have emerged as pivotal tools for enhancing healthcare and its management [2]. Consequently, there is a growing emphasis on developing new business models aimed at facilitating access to healthcare services for all stakeholders through improved information dissemination [3].

One of the most recent applications of IT in healthcare is the Internet of Things (IoT). The IoT can be defined as the interconnection of intelligent objects or devices via the Internet, leading to novel applications and innovative services [4]. These devices, equipped with extensive human detection capabilities, find utility in the medical field for remote health monitoring, early diagnosis, and elderly care [5, 6]. IoT applications in healthcare have the potential to enhance patient well-being and reduce service costs, for instance, by preventing unnecessary hospitalizations and ensuring better care for individuals in critical conditions. IoT-based healthcare services, spanning the entire value chain, are poised to revolutionize the healthcare sector [7].

Over recent years, substantial research has been conducted on IoT projects within the healthcare domain. IoT research, especially in relation to innovative healthcare applications, has witnessed rapid growth [8, 9]. For instance, Islam et al. [10] conducted an analysis of IoT-based industrial applications and trends in healthcare. Their study scrutinized various IoT and eHealth policies and regulations. Gundala et al. conducted a comprehensive review, identifying critical factors that enable a deeper understanding of the potential and challenges of implementing IoT applications in healthcare [11]. Bhuiyan et al. presented a review that classified existing IoT-based healthcare networks and provided an overview of prospective networks [12]. In this context, they analyzed IoT healthcare protocols and engaged in an extensive discussion. Furthermore, they initiated a comprehensive survey of IoT healthcare applications and services, offering profound insights into IoT healthcare security, its requisites, challenges, and privacy concerns within the healthcare IoT landscape [12].

2. IOMT AND MEDICAL SIGNALS

In [13], a research study employed a multi-sensor platform, encompassing two-channel pressure pulse wave (PPW) signals and one-channel ECG, to estimate blood pressure (BP). From the acquired signals, they extracted 35 physiological and informative features. To mitigate dimensionality and identify the most pertinent indicators for individual subjects, a weakly supervised feature (WSF) selection method was introduced. Furthermore, they harnessed a multi-instance regression algorithm to amalgamate these features, thus enhancing the BP

prediction model. Another study, delineated in [14], introduced a method for emotion recognition and classification across diverse individuals. This approach integrated significance testing and sequential backward selection with a support vector machine (ST-SBSSVM) to heighten the accuracy of emotion recognition. Gu et al. [15] put forth a real-time monitoring system designed to bolster precision and mitigate risks for mine workers. This system involved the fusion of data from multiple sensors, integrating concepts from situation awareness and the Internet of Things (IoT). A random forest (RF) SVM-based model was employed to assess situation levels and merge data. Through simulation analysis, they demonstrated an RMSE below 0.2 and a TSQ (Time Series Quality) not exceeding 1.691 after 200 iterations. In a distinct approach, [16] introduced an ensemble method with data fusion capabilities. This technique fused data sourced from a body sensor network (BSNs) and incorporated it into an ensemble classifier for the prediction of heart disease. Steenkiste et al. [17] presented a robust model aimed at enhancing the performance and reliability of sleep apnea prediction via sensor fusion. They collected and integrated multi-sensor data, including oxygen saturation, heart rate, thoracic respiratory belt, and abdominal respiratory belt, utilizing a method that incorporated backward shortcut connections. In the domain of IoT applications, an event-driven data fusion tree routing algorithm was introduced in [18]. This paper delved into health and sports information gathering systems, comprised of terminal nodes and client management systems. The algorithm was tailor-made to accommodate IoT communication characteristics and incorporated visual modeling, yielding superior accuracy and timeliness compared to alternative methods.

Chiuchisan et al. [19] outlined the design of a healthcare network for monitoring at-risk patients in smart intensive care units (ICUs) through an IoT model. They leveraged sensors and the Xbox Kinect to track patient movements and facilitate real-time alerts to physicians, thus enhancing patient care. Sharipudin and Ismail [20] proposed a healthcare monitoring system for data management in patient monitoring, integrating healthcare sensors to measure vital parameters, with data transmission to cloud storage for medical reference.

Dimitrov [21] expounded on IoMT (Internet of Medical Things) applications and Big Data in healthcare, illustrating their potential to support innovative commercial models, streamline work processes, improve customer experiences, and enhance outcomes. The usage of wearable sensors and mobile applications played a pivotal role in addressing various health needs and gathering patient data for health education.

In [22], early warning score systems were established based on vital sign characteristics, supporting health state estimation and informed critical care decision-making. The study explored diverse machine learning techniques for risk prediction based on medical data inputs. Sanyal et al. [23] introduced a federated filtering framework (FFF) for central fog server data forecasting using aggregated models from IoMT devices. This framework addressed critical concerns regarding energy efficiency, privacy, and latency for resource-constrained IoMT devices.

Finally, Luna-del Risco et al. [24] deliberated on the recognition, implementation challenges, and threats to wearable technology adoption in the Latin American healthcare system. The analysis revealed key challenges related to human resource allocation, healthcare connectivity, funding for health programs, and healthcare disparities. Wearable sensors were considered a valuable component of the solution to address healthcare challenges in the region.

3. ARCHITECTURE OF HEALTH IOT SYSTEM

Advancements in IoT and wearable technology are driving the adoption of personalized healthcare systems. These technologies create a connected environment, enabling various healthcare services such as remote health monitoring, fitness tracking, and nutrition programs. Figure 1 depicts the service-oriented architecture of a personalized Health IoT system, with each layer representing specific services.
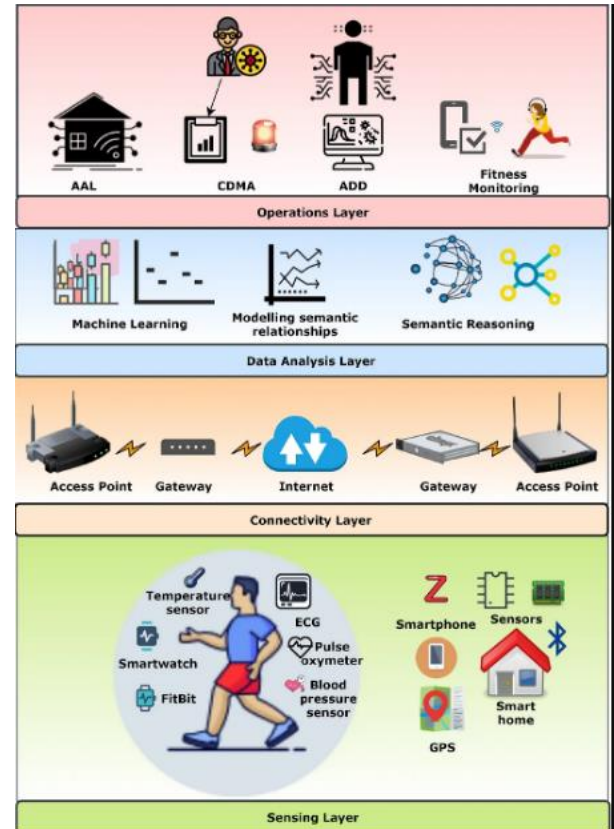

Figure 1: Service-oriented architecture of a personalized Health IoT system (Adopted from [25])

The Sensing layer comprises wearable sensors responsible for tracking body parameters, along with wireless communication technologies like Bluetooth and Zigbee. The Connectivity layer transfers sensor data to the Internet using devices like routers and gateways. The Data Analytics layer, positioned between the cloud and connectivity layers, ensures quality of service (QoS) requirements, reduces latency by caching data closer to users, and conducts data processing and analytics using machine learning. The topmost layer, the Operations layer, is primarily composed of cloud servers. It performs advanced processing and analysis of sensory data, delivering healthcare services like active alerts, fitness monitoring, and more.

Figure 2 illustrates the conventional three-tier architecture of an H-IoT system, comprising the Sensing layer, Network layer, and Cloud layer. The Sensing layer records vital body data using sensors and performs minimal computation before forwarding it to the Edge layer through the network. Various wireless communication protocols like Bluetooth, Wi-Fi, and Zigbee transmit data to the Edge/Fog Node via gateway devices. These nodes perform initial data processing near the Sensing end. The Cloud Layer analyzes the extensive data collected from sensing layer sensors to provide essential H-IoT

applications. A tele rehabilitation system based on IoT was demonstrated in [28] the system's capabilities in real-time remote health monitoring, enhancing the quality of life for older and disabled individuals, disease prediction, preventive medication, and healthcare service management in hospitals and emergency rooms [29, 30].

Moreover, the integration of blockchain with IoT devices in the IoMT ecosystem greatly facilitates the global sharing of patient medical data. By securely sending IoMT data to the blockchain through smart contracts, the system effectively reduces data tampering and information manipulation [31-33]. Blockchain security policies establish trust among stakeholders. Utilizing blockchain's decentralized storage concept simplifies and enhances the transparency of data collection, sharing, storage, and maintenance [34, 35]. Moreover, it ensures rigorous control over patient privacy policies.
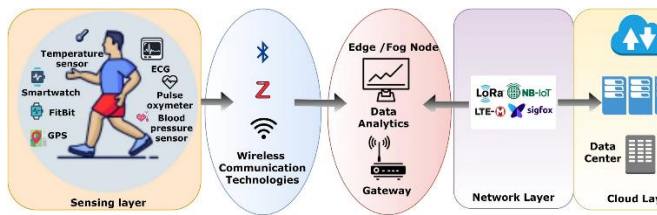

Figure 2: The three-layer generic architecture of H-IoT system (Adopted from [25])

4. ROLE OF CLOUD COMPUTING IN HEALTHCARE

Cloud computing (CC) has a positive impact on healthcare by enhancing efficiency and reducing costs. It offers advantages such as easy storage, sharing, and maintenance of medical data, as well as automated backend processes. To address the challenges of handling large datasets and providing physicians with access to patient health information, cloud infrastructure integrated with IoT devices is a viable solution [36]. However, two key concerns in a cloud based IoT system are data security and privacy, as well as the ability to support machine learning (ML) and deep learning (DL) models.

(a) Cloud Data Storage: This is a CC model that stores data on the Internet. Data plays a crucial role in diagnosing and analyzing diseases, making it necessary to store data in a repository (database) for research purposes. It allows hospitals and clinics to store vast amounts of patient and staff data that can be retrieved in case of emergencies. Cloud storage comes in three types: object storage, block storage, and file storage. Its advantages include efficient data maintenance and management, quick deployment, and cost-effectiveness [37].

(b) Data Processing and Analysis: The cloud provides various data processing techniques, including computer offloading, online data processing, electronic data processing, real-time processing, and machine learning. Among these, machine learning, specialized data mining, and offloading processing are the most relevant methods. Computational offloading involves transmitting raw data to the cloud for further processing, particularly suitable for handling complex data. Machine and deep learning techniques such as SVM, KNN, decision trees, random forests, CNN, LSTM, and autoencoders are employed for data analysis, while data mining techniques are used to extract valuable information from repositories. High-performance computing integrated with smartphone processing allows for the execution of sophisticated algorithms,

resulting in accurate outcomes and extended smartphone service life due to reduced internal computations.

(c) Data Cleaning: Noise, or significant modifications in image pixel values, can degrade diagnosis performance, particularly when noise is introduced during data acquisition and transmission. Data cleaning is essential, and filters such as mean filters, median filters, Gaussian filters, and Wiener filters can be applied for denoising. Image filtering replaces pixel values with the average values of neighboring pixels, resulting in smoother images. Figure 3 describes the advantages of the cloud in the healthcare system. Characteristics of cloud based IoT systems are as follows:
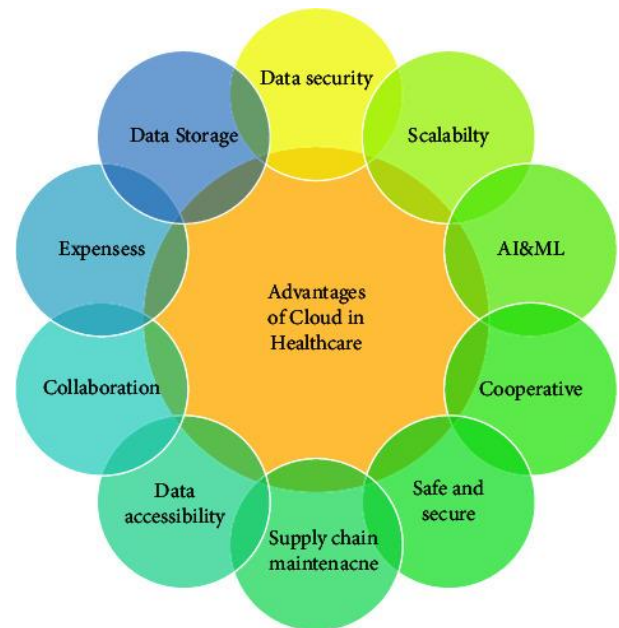

Figure 3: Cloud Computing in Healthcare (Adopted from [38])

5. APPLICATIONS OF CC AND IOMT IN DISEASE DETECTION

5.1 IoMT in Breast Cancer Detection

A significant volume of research has been conducted in the field of breast cancer detection and diagnosis, with some notable studies outlined here. Spanhol et al. [39] developed a system employing a variant of Convolutional Neural Network (CNN) known as ALexNet to classify malignant and benign cases using histopathological images. In [40], Ertosun and Rubin introduced a model to identify the presence of masses in mammography images and subsequently locate these masses within the images. In [41], a deep learning model was designed to detect mitosis, utilizing feature extraction techniques like CNN. The output from this was fed into a Support Vector Machine (SVM) classifier to identify breast tumors. For mitosis detection in breast histopathology scans, a deep contour-aware network was introduced [42]. Xu et al. [43] proposed a classification model using a Stacked Sparse Autoencoder (SSAE) to classify nuclei in histopathological breast images. A greedy algorithm was applied to optimize the SSAE. Additionally, breast cancer detection was performed using a mammography image dataset. In [44, 45], a hybrid model combining CNN and SVM was developed to detect masses in mammographic scans. CNN was trained on mammogram abnormalities, and the fully connected layer was used to extract high-level features, which were then employed to train the

SVM classifier. Kim et al. [46] suggested a 3D multi-view approach using CNN to analyze bilateral features via Digital Breast Tomosynthesis (DBT). Volume of Interest (VOI) was extracted from the input volume, and two different CNN algorithms were employed to extract features from the VOI. Yu et al. [47] proposed a deep learning-enabled system for breast cancer diagnosis in remote healthcare settings using 5G technology. This approach involves three steps: acquiring input data from hospitals via 5G, applying a transfer learning algorithm to develop a diagnostic system, and deploying this model on an edge server for remote diagnosis. Modified VGG (MVGG) was proposed in [26] to detect breast cancer from 2D and 3D images of mammograms.

5.2 IoMT in Diabetes Detection

Numerous methods and techniques have been proposed for the detection of diabetes. In [48], various machine learning techniques, including SVM, decision trees, and Naive Bayes, were applied.

In [49], a hybrid approach utilizing Principal Component Analysis (PCA) and the Adaptive Neuro-Fuzzy Interface System (ANFIS) was employed. The development of ResNet to tackle the vanishing gradient problem is discussed in [50]. In [51], an Artificial Neural Network (ANN) architecture was introduced for diabetes prediction. This model aimed to minimize the error rate during training and achieved an 87% accuracy rate with an estimated error rate of 0.01%. In [52] a computer-aided system was presented for the detection of diabetic retinopathy using digital signals obtained from retinal images. The primary objective was to classify nonproliferative diabetic retinopathy from retinal images. A Convolutional Neural Network (CNN) approach was introduced in [53] for segmenting blood vessels in diabetic patients, followed by classification and the extraction of discriminant patterns. [54] developed a shallow CNN framework for this purpose. Finally, in [55], a residual network (ResNet) was developed for the automatic classification of retinopathy images.

6. MALWARE THREATS IN IOMT

Security concerns related to IoT devices are on the rise due to the rapid development and widespread deployment of IoT systems. This trend has created opportunities for various types of cyberattacks within the IoT environment, facilitated by internet connectivity. The situation becomes particularly critical in the context of the Internet of Medical Things (IoMT), which involves communication and control of smart medical devices [56-59]. For instance, if an attacker gains remote control over a smart medical device, they can pose a serious threat to the patient's life, such as causing a smart pacemaker to deliver a potentially lethal shock.

The emergence of various types of IoT malware compounds these security challenges. These evolving malware strains have the potential to compromise the communication within IoMT systems and manipulate smart medical devices. In the IoMT context, malfunctions of smart medical devices may also occur, such as the unintended release of insulin from an implanted blood glucose monitoring system [60].

Several categories of malware are pertinent to this discussion [61]-[64]:

(a) Spyware: This type of malware operates by covertly monitoring a user's activities without their consent. It engages in malicious activities like collecting keystrokes, tracking user behavior, and harvesting data, including account credentials and financial information like credit card numbers. Spyware often exploits software vulnerabilities and can attach itself to legitimate programs.

(b) Keylogger: Keyloggers are malicious code designed to record a user's keystrokes. This means that everything a user types, including login information and passwords, can be captured. Keylogger attacks are particularly potent and can bypass strong password protection. To mitigate this threat, it is recommended to implement multi-factor authentication (MFA), which combines username, password, smart card, and biometric data.

(c) Trojan Horse: This malware disguises itself as a legitimate program to deceive users into downloading and installing it. Once installed, it provides unauthorized remote access to the infected system, enabling hackers to steal sensitive data like account and credit card numbers. Trojan Horses can also introduce additional malicious software into the system for various illicit purposes.

(d) Virus: Viruses are malicious programs capable of replicating themselves and spreading to other systems. They achieve this by attaching themselves to different programs, activating their code when a user launches one of the infected programs. Viruses can be employed to steal information, damage host systems, and create botnets.

(e) Worm: Worms propagate across networks by exploiting vulnerabilities in operating systems. They can disrupt host networks through excessive bandwidth usage and server overloads. Some worms carry payloads designed to harm host systems. Hackers frequently use worms to steal sensitive data, delete files, or establish botnets.

These security threats underscore the importance of robust security measures and continuous vigilance in the IoMT and broader IoT ecosystems.

7. FUTURE DIRECTIONS

The Internet of Things (IoT) is rapidly transforming the healthcare industry, offering promising future directions for progression [65-73].

(a) **Remote Patient Monitoring:** IoT devices enable real-time monitoring of patients' vital signs, chronic conditions, and overall health. This can significantly improve the quality of care and reduce the need for frequent in-person visits, particularly in the context of an aging population.

(b) Enhanced Data Analytics: IoT-generated data allows for advanced analytics and predictive modeling. Machine learning and AI can identify trends and predict potential health issues, aiding in early intervention and personalized treatment plans.

(c) Wearable Technology: Wearable IoT devices, like smartwatches and fitness trackers, are becoming increasingly sophisticated. They offer continuous health tracking, including ECG, blood pressure, and sleep patterns, empowering individuals to take control of their health.

(d) Telemedicine: The integration of IoT in telemedicine enables secure, real-time video consultations and the remote exchange of patient data. This is especially valuable in providing healthcare access to underserved or remote areas.

(e) Drug Adherence Monitoring: IoT can improve medication adherence by providing reminders and tracking dosages. This is crucial for chronic disease management.

8. CONCLUSION

Smart healthcare is a well-explored field encompassing IoT, IoMT, medical data, AI, edge and cloud computing, each with its own strategies and speeds. This tutorial paper aims to categorize and compare IoT, IoMT, AI, cloud computing, and malware threats in smart healthcare. Traditional AI-based healthcare systems might not be readily accepted by medical professionals. Hence, employing explainable AI systems allows doctors to visualize disease detection or classification. Edge resources can be optimized effectively using intelligent algorithms. Furthermore, the evolution of next-gen wireless networks, including 5G and beyond, accelerates global healthcare accessibility. Additionally, federated deep learning and edge computing are simplified and strengthened.

9. REFERENCES

[1] Belfiore, A., Cuccurullo, C., & Aria, M. (2022). IoT in healthcare: A scientometric analysis. Technological Forecasting and Social Change, 184, 122001.

[2] Khan, M. M., Alanazi, T. M., Albraikan, A. A., & Almalki, F. A. (2022). IoT-based health monitoring system development and analysis. Security and Communication Networks, 2022.

[3] Verdegem, P., De Marez, L., 2011. Rethinking determinants of ICT acceptance: towards an integrated and comprehensive overview. Technovation 31 (8), 411–423.

[4] Lu, Y., Papagiannidis, S., Alamanos, E., 2018. Internet of things: a systematic review of the business literature from the user and organisational perspectives. Technol. Forecast. Soc. Chang. 136, 285–297.

[5] Bharati, S., Mondal, M. R. H., Podder, P., & Kose, U. (2023). Explainable Artificial Intelligence (XAI) with IoHT for Smart Healthcare: A Review. Interpretable Cognitive Internet of Things for Healthcare, 1-24.

[6] Bharati, S. & Hossain Mondal, M. (2021). 12 Applications and challenges of AI-driven IoHT for combating pandemics: a review. In A. Khamparia, R. Hossain Mondal, P. Podder, B. Bhushan, V. Albuquerque & S. Kumar (Ed.), Computational Intelligence for Managing Pandemics (pp. 213-230). Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110712254-012.

[7] Dey, N., Ashour, A.S., Bhatt, C., 2017. Internet of things driven connected healthcare. In: Internet of Things And Big Data Technologies for Next Generation Healthcare. Springer, Cham, pp. 3–12.

[8] Papa, A., Mital, M., Pisano, P., Del Giudice, M., 2020. E-health and wellbeing monitoring using smart healthcare devices: an empirical investigation. Technol. Forecast. Soc. Chang. 153, 119226.

[9] Martínez-Caro, E., Cegarra-Navarro, J.G., García-P´erez, A., Fait, M., 2018. Healthcare service evolution towards the internet of things: an end-user perspective. Technol. Forecast. Soc. Chang. 136, 268–276.

[10] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. IEEE Access 3, 678–708.

[11] J. R. Gundala, S. S. Varsha Potluri, S. V. Damle and M. F. Hashmi, "IoT & ML-Based Healthcare Monitoring System-Review," 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal, India, 2022, pp. 623-626, doi: 10.1109/iSES54909.2022.00137.

[12] M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10474-10498, 1 July1, 2021.

[13] F. Miao, Z.-D. Liu, J.-K. Liu, B. Wen, Q.-Y. He, and Y. Li, "Multisensor fusion approach for cuff-less blood pressure measurement," IEEE J. Biomed. Health Informat., vol. 24, no. 1, pp. 79 91, Jan. 2020.

[14] F. Yang, X. Zhao, W. Jiang, P. Gao, and G. Liu, "Multi-method fusion of cross-subject emotion recognition based on highdimensional EEG features," Frontiers Comput. Neurosci., vol. 13, p. 53, Aug. 2019. Accessed: Jul. 1, 2020. [Online].

[15] Q. Gu, S. Jiang, M. Lian, and C. Lu, "Health and safety situation awareness model and emergency management based on multi-sensor signal fusion," IEEE Access, vol. 7, pp. 958 968, 2019.

[16] M. Muzammal, R. Talat, A. H. Sodhro, and S. Pirbhulal, "A multi-sensor data fusion enabled ensemble approach for medical data from body sensor networks," Inf. Fusion, vol. 53, pp. 155 164, Jan. 2020.

[17] T. Van Steenkiste, D. Deschrijver, and T. Dhaene, "Sensor fusion using backward shortcut connections for sleep apnea detection in multi-modal data," 2019, arXiv:1912.06879.

[18] Y. Zhang, Y. Zhang, X. Zhao, Z. Zhang, and H. Chen, "Design and data analysis of sports information acquisition system based on Internet of medical things," IEEE Access, vol. 8, pp. 84792 84805, 2020.

[19] I. Chiuchisan, H.-N. Costin, and O. Geman, "Adopting the Internet of Things technologies in health care systems," in Proc. Int. Conf. Expo. Electr. Power Eng. (EPE), Iasi, Romania, Oct. 2014, pp. 532 535.

[20] A. Sharipudin and W. Ismail, "Internet of medical things (IoMT) for patient healthcare monitoring system," in Proc. IEEE 14th Malaysia Int. Conf. Commun. (MICC), Selangor, Malaysia, Dec. 2019, pp. 69 74.

[21] D. V. Dimitrov, "Medical Internet of Things and big data in healthcare," Healthcare Inform. Res., vol. 22, no. 3, pp. 156 163, 2016.

[22] A. Pazienza, R. Anglani, G. Mallardi, C. Fasciano, P. Noviello, C. Tatulli, and F. Vitulano, "Adaptive critical care intervention in the Internet of medical things," in Proc. IEEE Conf. Evolving Adapt. Intell. Syst. (EAIS), Bari, Italy, May 2020, pp. 1 8.

[23] S. Sanyal, D. Wu, and B. Nour, "A federated filtering framework for Internet of medical things," in Proc. IEEE Int. Conf. Commun. (ICC), Shanghai, China, May 2019, pp. 1 6.

[24] M. Luna-delRisco, M. G. Palacio, C. A. A. Orozco, S. V. Moncada, L. G. Palacio, J. J. Q. Montealegre, and I. Diaz-Forero, "Adoption of Internet of medical things (IoMT) as an opportunity for improving public health in Latin America," in Proc. 13th Iberian Conf. Inf. Syst. Technol. (CISTI), Caceres, Spain, Jun. 2018, pp. 1 5.

[25] Krishnamoorthy, S., Dua, A. & Gupta, S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. J Ambient Intell Human Comput 14, 361–407 (2023).

[26] Khamparia, A., Bharati, S., Podder, P., Gupta, D., Khanna, A., Phung, T. K., & Thanh, D. N. (2021). Diagnosis of breast cancer based on modern mammography using hybrid transfer learning. Multidimensional systems and signal processing, 32, 747-765.

[27] A.H.M Shahariar Parvez, Bipasha Sarker, "Role of IoT and Cloud Computing in Digital Healthcare", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 11, Issue 4, April 2022.

[28] Yin Y, Zeng Y, Chen X, Fan Y (2016) The internet of things in healthcare: AN overview. Ind Inf Integr 1:3–13.

[29] Gardasevic G, Veletić M, Maletić N, Vasiljević D, Radusinović I, Tomović S, Radonjić M (2016) The IOT architectural framework, design issues and application domains. Wirel Pers Commun 92:127–148.

[30] Nauman A, Qadri YA, Amjad M, Zikria YB, Afzal MK, Kim SW (2020) Multimedia internet of things: a comprehensive survey. IEEE Access 8:8202–8250.

[31] Sarker, B., Sharif, N. B., Rahman, M. A. & Parvez, A. S. (2023). AI, IoMT and Blockchain in Healthcare. Journal of Trends in Computer Science and Smart Technology, 5(1), 30-50. doi:10.36548/jtcsst.2023.1.003.

[32] Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and Communication Networks, 2022, 1-41.

[33] Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). Review on the security threats of internet of things. arXiv preprint arXiv:2101.05614.

[34] Ahmed, R., & Deng, H. (2023). Ground Moving Target Detection Using Multi-Features under Antenna Array Crabbing. arXiv preprint arXiv:2304.08716.

[35] Ibtisum, S. (2020). A Comparative Study on Different Big Data Tools.

[36] Aguzzi S., Bradshaw D., Canning M., et al. Definition of a research and innovation policy leveraging cloud computing and IoT combination. Final Report, European Commission, SMART . 2013;37

[37] Siarry P., Jabbar M. A., Aluvalu R., Abraham A., Madureira A. The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care . Berlin, Germany: Springer; 2021.

[38] Saba Raoof S, Durai MAS. A Comprehensive Review on Smart Health Care: Applications, Paradigms, and Challenges with Case Studies. Contrast Media Mol Imaging. 2022 Sep 29;2022:4822235.

[39] Spanhol F. A., Oliveira L. S., Petitjean C., Heutte L. Breast cancer histopathological image classification using convolutional neural networks. Proceedings of the international joint conference on neural networks (IJCNN); July 2016; Vancouver, British Columbia, Canada.

[40] Ertosun M. G., Rubin D. L. Probabilistic visual search for masses within mammography images using deep learning. Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine (BIBM); July 2015; Washington, DC, USA.

[41] Albayrak A., Bilgin G. Mitosis detection using convolutional neural network based features. Proceedings of the IEEE 17th International symposium on computational intelligence and informatics (CINTI); November 2016; Budapest, Hungary.

[42] Chen H., Qi X., Yu L., Heng P.-A. DCAN: deep contour-aware networks for accurate gland segmentation. Proceedings of the IEEE conference on Computer Vision and Pattern Recognition; June 2016; Las Vegas, Nevada, USA.

[43] Xu B., Wang N., Chen T., Li M. Empirical evaluation of rectified activations in convolutional network. 2015. https://arxiv.org/abs/1505.00853.

[44] Wichakam I., Vateekul P. Combining deep convolutional networks and SVMs for mass detection on digital mammograms. Proceedings of the international conference on knowledge and smart technology (KST); January 2016; Chon buri, Thailand.

[45] Allugunti V. R. Breast cancer detection based on thermographic images using machine learning and deep learning algorithms. International Journal of Engineering in Computer Science . 2022;4(1):49–56.

[46] Kim D. H., Kim S. T., Ro Y. M. Latent feature representation with 3-D multi-view deep convolutional neural network for bilateral analysis in digital breast tomosynthesis. Proceedings of the IEEE international conference on acoustics, speech and signal processing (ICASSP); March 2016; Shanghai, China.

[47] Yu K., Tan L., Lin L., Cheng X., Yi Z., Sato T. Deep-learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health. IEEE Wireless Communications, 2021; 28(3):54–61.

[48] D. Sisodia and D. S. Sisodia, "Prediction of diabetes using classification algorithms," Procedia Computer Science, vol. 132, pp. 1578–1585, 2018.

[49] Polat K., Güneş S. An expert system approach based on principal component analysis and adaptive neuro-fuzzy inference system to diagnosis of diabetes disease. Digital Signal Processing . 2007;17(4):702–710.

[50] He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition. Proceedings of the IEEE conference on computer vision and pattern recognition; June 2016; Las Vegas, Nevada, USA.

[51] El_Jerjawi N. S., Abu-Naser S. S. Diabetes prediction using artificial neural network. International Journal of Advanced Science and Technology . 2018;121.

[52] Carrera E. V., González A., Carrera R. Automated detection of diabetic retinopathy using SVM. Proceedings of the IEEE XXIV international conference on electronics, electrical engineering and computing (INTERCON); June 2017; Cusco, Peru.

[53] Girard F., Kavalec C., Cheriet F. Joint segmentation and classification of retinal arteries/veins from fundus images.

Artificial Intelligence in Medicine . 2019;94:96–109. doi: 10.1016/j.artmed.2019.02.004.

[54] Pratt H., Coenen F., Broadbent D. M., Harding S. P., Zheng Y. Convolutional neural networks for diabetic retinopathy. Procedia Computer Science . 2016;90:200–205.

[55] Zhang D., Bu W., Wu X. Diabetic retinopathy classification using deeply supervised ResNet. Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing; August 2017; San Francisco, CA, USA. pp. 1–6.

[56] Sirajul Islam, M., Rouf, M. A., Shahariar Parvez, A. H. M., & Podder, P. (2022). Machine Learning-Driven Algorithms for Network Anomaly Detection. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2021 (pp. 493-507). Singapore: Springer Nature Singapore.

[57] Paul, P., Bharati, S., Podder, P. & Hossain Mondal, M. (2021). 10 The role of IoMT during pandemics. In A. Khamparia, R. Hossain Mondal, P. Podder, B. Bhushan, V. Albuquerque & S. Kumar (Ed.), Computational Intelligence for Managing Pandemics (pp. 169-186). Berlin, Boston: De Gruyter.

[58] Robel, M. R. A., Bharati, S., Podder, P., Raihan-Al-Masud, M., & Mandal, S. (2021). Fault tolerance in cloud computing-an algorithmic approach. In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 10th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2019) held in Gunupur, Odisha, India during December 16-18, 2019 10 (pp. 307-316). Springer.

[59] Sarker, B., Sarker, B., Podder, P., & Robel, M. R. A. (2020). Progression of Internet Banking System in Bangladesh and its Challenges. International Journal of Computer Applications, 177(29), 11-15.

[60] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE access, 7, 182459-182476.

[61] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," Softw. Qual. J., vol. 26, no. 3, pp. 891919, 2018.

[62] H. Takase, R. Kobayashi, M. Kato, and R. Ohmura, "A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information," Int. J. Inf. Secur., 2019.

[63] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for Internet of (battleeld) things devices using deep Eigenspace learning," IEEE Trans. Sustain. Comput., vol. 4, no. 1, pp. 8895, Jan./Mar. 2019.

[64] E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, "A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions," IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 1145-1172, 2nd Quart., 2017.

[65] Kamal, Tamanna, Fabiha Islam, and Mobasshira Zaman. "Designing a Warehouse with RFID and Firebase Based Android Application." Journal of Industrial Mechanics 4.1 (2019): 11-19.

[66] Parvez, Md Shohel, et al. "Anthropomorphic investigation into improved furniture fabrication and fitting for students in a Bangladeshi university." Journal of The Institution of Engineers (India): Series C 103.4 (2022): 613-622.

[67] S. Vishnu, S. R. J. Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview," 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2020, pp. 101-104, doi: 10.1109/ICDCS48716.2020.243558.

[68] Parvez, M. S., et al. "Are library furniture dimensions appropriate for anthropometric measurements of university students?." Journal of Industrial and Production Engineering 39.5 (2022): 365-380.

[69] Hossain, Md Zakir, et al. "Evaluating the Effectiveness of a Portable Wind Generator that Produces Electricity using Wind Flow from Moving Vehicles." Journal of Industrial Mechanics 8.2 (2023): 44-53.

[70] Mondal, M. Rubaiyat Hossain, et al. "Data analytics for novel coronavirus disease." informatics in medicine unlocked 20 (2020): 100374.

[71] Bharati, S., Mondal, M., Podder, P., & Prasath, V. B. (2022). Deep learning for medical image registration: A comprehensive review. arXiv preprint arXiv:2204.11341.

[72] S M Atikur Rahman, Sifat Ibtisum, Ehsan Bazgir, Tumpa Barai, "The Significance of Machine Learning in Clinical Disease Diagnosis: A Review", International Journal of Computer Applications (0975 – 8887), October 2023 (Accepted).

[73] S. Y. Wong, M. Y. Soh and J. M. Wong, "Internet of Medical Things:Brief Overview and the Future," 2021 IEEE 19th Student Conference on Research and Development (SCOReD), Kota Kinabalu, Malaysia, 2021, pp. 427-432.