Full Length Research Article

Secure Cloud Enabled Platform for AI-Powered Computer Vision Syndrome Detection

Dr. Shaikh Abdul Hannan
Assistant Professor, Faculty of Computing and Information, AlBaha University, Al-Baha, Kingdom of Saudi Arabia
abdulhannan05@gmail.com

Article Received 28-12-2025, Revised 25-1-2026, Accepted 07-02-2026

ABSTRACT

Computer vision syndrome detection has become a significant discovery in the current healthcare system, as a way of diagnosing genetic and development disorders at an early stage with the help of facial features. Nevertheless, in practice, such systems must have high-level security, why privacy protection, and scalability in the case of sensitive patient information. This paper describes a safe cloud-based system that incorporates AI-based computer vision algorithms to detect syndromes automatically. The given framework makes use of using convolutional neural networks (CNNs) to extract facial features and make deep learning classifications using the Softmax probability-based syndrome prediction. Experimental evaluation was done using a 90 sample of faces images that consisted of Down Syndrome (33.3%), Williams Syndrome (22.2%), Turner Syndrome (16.7%), and other syndromes (27.8%). The gender representation was also fairly equal at 53.3/46.7 % males/females respectively. The site also has security features like encryption and privacy learning methods to secure the information of the patients in the cloud implementation.

Keywords: *Syndrome Detection, Computer Vision, Secure Cloud Platform, Deep Learning, CNN, Federated Learning.*

1. INTRODUCTION

The fast solution in the sphere of artificial intelligence (AI) and computer vision have enhanced the medical diagnostic opportunities greatly. Syndrome detection can be described as the identification of genetic or neurological diseases based on observable physical appearances, face structure, posture, or even movement patterns. The timely and correct identification of symptoms is essential to these diseases to intervene on time and provide personalized treatment[1-3].

The conventional method of syndrome diagnosis relies on clinical experience, genetic testing, and manual diagnosis. The methods are prohibitively costly, time consuming, and restricted in distant health care conditions. AI-based vision-based systems offer automated services to identify the syndrome-based patterns in patient images and videos [4-6].

Nevertheless, scaling syndrome detection systems faces some challenges such as privacy threats, cyber terrorism, and resource-intensive high-performance computing. Cloud computing provides scalable infrastructures to deploy AI models, yet health-related image data must have robust security arrangements [7-8].

Recent experiments prove the effectiveness of CNN-based architectures in recognition of facial syndromes and classification of rare diseases. Also, privacy-preserving learning systems like federated learning and secure encryption solutions are becoming critical in AI implementation in healthcare. Therefore, this paper suggests a safe cloud-based AI platform, which integrates deep learning vision models and the ability to ensure robust security protocols to allow safe and effective syndrome detection [9-11].

In addition to improving diagnostic automation, AI-powered syndrome detection systems can significantly reduce the burden on healthcare professionals by providing decision-support assistance in complex or uncertain cases]. These intelligent models can analyze subtle phenotypic variations that may not be easily recognized through routine clinical examination, thereby enhancing diagnostic consistency and reducing human error . Moreover, the integration of computer vision with cloud-enabled healthcare platforms enables remote access to diagnostic tools, which is particularly beneficial in underserved and rural regions where genetic specialists and advanced laboratory facilities are limited. By enabling early screening, continuous monitoring, and rapid referral support, such platforms have the potential to transform syndrome diagnosis into a more accessible, efficient, and patient-centric process while maintaining strict standards of data privacy and clinical reliability [12-18].

1.1 Objectives of the Study

The main objectives of this research are:

1. To design a secure cloud-based platform for AI-driven syndrome detection.

https://doi.org/10.63665/IJMEC.1102.03
ISSN: 2456-4265
IJMEC 2026

2. To develop an AI-powered computer vision pipeline for syndrome classification.
3. To integrate privacy-preserving mechanisms such as encryption and federated learning.
4. To evaluate the performance of deep learning models in detecting syndromes from facial features.
5. To ensure Explainability and interpretability of AI decisions in healthcare diagnosis.
6. To provide a scalable real-time syndrome detection architecture suitable for remote clinical support.

2. LITERATURE SURVEY

Rosenfield (2016)reported a comprehensive assessment of the ocular etiology of Computer Vision Syndrome (CVS), which has become a more and more common condition because of the long-term use of digital screens. The paper provided a description of how prolonged use of computers and mobile gadgets usually resulted in visual discomfort, which was characterized by eye strain, eye dryness, blurred vision, headache, and musculoskeletal fatigue. Rosenfield also addressed the issue that CVS was not a problem that was confined to eye-related issues but also had an impact on the general efficiency and quality of life in work. The author has highlighted that the syndrome was caused by decreased rates of blinking, inappropriate positioning of screens, glare, and uncorrected refractive errors. Also, the review identified some possible preventive and treatment measures, such as ergonomic adjustments, regular rest intervals according to the 20-20-20 rule, artificial tear supplement, and proper vision correction. The paper also helped to comprehend CVS as an increasing professional health issue in the contemporary digital setting [19].

Esteva et al. (2017) established the high potential of deep neural networks in reaching the performance of a dermatologist when classifying skin cancer cases. The researchers trained convolutional neural networks (CNNs) with massive dermatological images databases that have thousands of labeled lesions. Their findings revealed that AI-based models could effectively distinguish between malignant melanoma and benign skin lesions, which had similar results as more qualified medical experts. The paper has emphasized that deep learning systems could learn higher-order patterns in healthcare images without manual feature engineering. In addition, the authors posited that these AI applications would be beneficial in the early diagnosis, access to healthcare in underserved areas, and the delay in diagnoses. The publication marked a significant milestone in medical computer vision as it demonstrated the usefulness of CNNs in the task of disease recognition at the clinical level and served as a significant basis of extending AI-based diagnostic systems to other tasks in identifying syndromes and disorders [20].

Kuo (2011) examined the new frontier of cloud computing in the field of changing the method of delivering healthcare services. The research termed cloud computing as a modular technology model that helped medical facilities to store vast amounts of patient information and make use of the computational power away at a distance. Kuo has stressed out that cloud-based solutions enhanced scalability, lowered the cost of infrastructure and enabled effective exchange of healthcare data between the units and sites. The article has addressed the way cloud platforms may improve telemedicine services, electronic health record (EHR) systems, and real-time clinical decision support. Nevertheless, the author found out several notable challenges, including those associated with patient privacy, regulatory compliance, and cybersecurity vulnerabilities. Challenges like lack of standardization, data breach and unauthorised access were also cited as obstacles to adoption. On the whole, the research offered an important contribution to the discussion concerning the necessity to find a balance between the advantages of the cloud and the necessity to implement healthcare solutions with the lack of any security and reliability [21].

Jang-Jaccard and Nepal (2014) performed a comprehensive survey of the fast-changing cybersecurity threats on the latest digital systems, including healthcare infrastructures. The authors stated that the growing reliance on cloud networks, mobile gadgets, and interconnected platforms had increased attacker space in a cybercriminal operation. According to their survey, the major threats include malware infections, phishing attacks, network intrusion, denial-of-service attacks, and cloud service unauthorized exploitation. The research discussed that healthcare organizations were especially susceptible because patient information is sensitive, and constant service provision is extremely crucial. Limitations of traditional security mechanisms were another theme that the authors discussed as a way of dealing with new attack technique. Their work emphasized the acute necessity of sophisticated cybersecurity models, risk assessment interventions, and effective authentication policies to guarantee the security of digital health systems [22].

Ting et al. (2019) conducted a review of the considerable role of the artificial intelligence and deep learning in ophthalmology. The research indicated that AI-driven diagnostic tools had been utilized more in the detection of retinal disease, diabetic retinopathy, glaucoma, and macular degeneration by computerized image analysis. Deep learning models were noted by Ting and colleagues to have high accuracy when analyzing retinal scans and fundus images, and in most cases, they matched the performance of specialists. The paper also reported the use of AI in enhancing clinical workflow, diagnostics load, and early screening of diseases. In spite of these progressions, the authors observed that the issues that have been encountered are the guaranteed explainability, clinical validation, and ethical deployment. The researchers concluded that AI application in ophthalmology was a significant leap towards smart healthcare, yet the implementation was to be considered through trust, bias, and regulatory compliance areas [23].

Kaissis et al. (2020) explored secure and privacy-safe machine learning practices, paying a lot of attention to federated learning in the medical imaging setting. The authors described that conventional centralized AI training necessitated the dissemination of sensitive datasets on patients, which represented severe privacy threats and breached healthcare provisions. As an alternative, federated learning was offered as a potentially advantageous approach, where hospitals and institutions can locate AI models locally and exchange model parameters but not patient data. The analysis showed that such a solution enhanced compliance with privacy, minimized the risk of data exposure, and facilitated cooperative learning among healthcare centers distributed around the world. Kaissis et al. also mentioned technical issues, including communication overhead, heterogeneous models, and security threats due to malicious updates. Their contribution made federated learning a key breakthrough towards the creation of safe AI-driven diagnostic systems in cloud-based health care settings [24].

Kocabas et al. (2016) reviewed the new security measures intended to be implemented in medical cyber-physical systems, which comprise connected medical equipment in the form of implantable sensors, monitoring systems, and IoT-based medical equipment. These systems, according to the researchers, were becoming susceptible to cyber attacks because of their dependence on wireless communication and real time exchange of data. In the study, some of the security solutions that were proposed include encryption, authentication, key management that is secure and intrusion detection systems. The authors underlined that cyber threats within medical settings would result in not only breached data but also in the real damage in case of manipulated devices. Their work made it clear that it is necessary to establish safe bases of smart medical systems and provide safety, reliability, and confidence of patients in the connected medical systems [25].

Gubbi et al. (2013) gave a holistic vision of the Internet of Things (IoT) and outlines its architectural structure and future opportunities. According to the authors, IoT comprised of interdependent devices that could gather, process, and send data using cloud-based networks. In the medical setting, IoT was demonstrated to facilitate the process of constant attention to patients with the help of wearables, smart medical devices, and remote diagnostics. The article highlighted that the integration of IoT had the potential to enhance health outcomes via early intervention and personal care. The authors also identified difficulty in interoperability of devices, scalability, energy efficiency, and vulnerability to security risks as some of the challenges. Their research gave a background knowledge on the role of IoT as a key facilitator of the future cloud-based AI healthcare system [26].

Samek et al. (2017) talked about the significance of Explainable Artificial Intelligence (XAI) to gain insights into the complex deep learning models. The authors made the argument that despite the high accuracy of AI systems, the black-box nature of such systems did not allow the system to be trusted and adopted by sensitive areas like healthcare. The paper presented visualization approaches to neural network decisions that include relevance mapping and feature attribution algorithmic techniques. Samek and colleagues clarified that explainable AI enhanced transparency as clinicians could learn why a given diagnosis was forecasted. The study has identified XAI as a key factor in minimizing uncertainty, identifying bias, and maintaining accountability in medical AI usage. Their efforts brought about the creation of reliable AI systems that could be integrated safely into the clinical decision-making system [27].

Subashini and Kavitha (2011) surveyed on the security concerns relating to models of cloud computing service delivery. According to the authors, cloud infrastructures posed risks of sharing resources, remote access and multi-tenancy. Data loss, unauthorized access, insecure application interfaces, insider threats, and compliance issues were found to be among the major concerns of the study. The authors noted that this was especially dangerous with healthcare applications since patient records had to be kept in a highly confidential and secure manner. They indicated that safe cloud adoption required encrypting data safely, putting control and access measures in place and having proper authentication systems. Their contributions were some of the first but important understanding of the problem of cloud security that was used to build secure cloud-based healthcare [28].

3. METHODOLOGY

The section discusses the entire operating process of the proposed Secure Cloud-Enabled AI Platform to detect Computer Vision Syndrome. The methodology is concerned with the processing of facial images, the classification of syndromes with the help of deep learning, and patient privacy with the help of cloud security and federated learning.

3.1 System Architecture

The proposed syndrome detection platform is designed to accomplish high accuracy, scalability and security with the deployment of the health care in the real world through using a layered system architecture. The whole workflow is structured into four large interconnected modules that perform a certain task in the syndrome detection pipeline. This structural type allows processing patient data effectively and is characterized by privacy and clinical reliability.

https://doi.org/10.63665/IJMEC.1102.03
ISSN: 2456-4265
IJMEC 2026

The first is Image Acquisition Layer that is the entry point of the system. The data about the face of the patient is gathered at this stage using various sources including surveillance or diagnostic cameras in the hospital, mobile devices, clinical image data sets, and telemedicine systems. The layer is important to ensure that the facial images are recorded in standardized formats and in sufficient quality, which should be subjected to further automated processing and examination.

Once an image has been acquired, the information is sent to the AI Vision Processing Layer which is the main intelligence part of the platform. This layer conducts importance preprocessing tasks such as resizing images, normalizing and minimizing noise to increase the clarity and consistency of the images. After this, convolutional neural networks (CNNs) are used to find meaningful facial features and deep learning-based classification models are used to analyze these patterns to find syndromic characteristics. In this way, this layer allows automatic and precise syndrome recognition using computer vision method [29].

The third module is the Secure Cloud Deployment Layer that offers a scalable computing environment and remote accessibility to healthcare settings. Because the process of syndrome detection deals directly with extremely sensitive medical data, cloud infrastructure is employed to provide a high-performance computing and storage as well as a secure deployment. There are strong encryption methods, authentication, and privacy-preserving protocols that are used to ensure that the information related to patients is kept secure when they are being transferred and stored in the cloud [30].

3.2 Computer Vision-Based Feature Extraction

Facial syndrome detection depends heavily on extracting meaningful patterns from facial structures such as:

Eye spacing

Nose shape

Jaw alignment

Facial symmetry

To achieve this, facial images are processed using **Convolutional Neural Networks (CNNs)**.

Mathematical Representation

$$F = CNN(I)$$

Where:

I= input facial image

CNN= convolutional neural network model

F= extracted feature vector

3.3 Syndrome Classification Model

Once the features of the faces are extracted, what comes next is matching the image to a specific syndrome.

To classify, the system relies on the Softmax function which transforms the scores of its output into the probability across syndrome classes.

SoftMax Equation

$$P(y = i \mid F) = \frac{e^{W_i F + b_i}}{\sum_{j=1}^{C} e^{W_j F + b_j}}$$

Where:

$P(y = i \mid F)$= probability that the image belongs to syndrome class i

C= total number of syndrome classes

W_i, b_i= trainable weights and bias values

F= extracted feature vector

3.4 Loss Function Optimization

To improve prediction accuracy, the model must minimize errors during training.

The system employs the Cross-Entropy Loss Function that is commonly used in the multi-classification issue [31-32].

Loss Function Equation

$$L = -\sum_{i=1}^{C} y_i \log(P_i)$$

Where:

L= total training loss

y_i= actual ground truth label (1 if correct class, 0 otherwise)

P_i= predicted probability for class i

C= number of syndrome classes

4. RESULTS AND DISCUSSION

Table 1plots the sample distribution of the samples of the facial images based on the various types of syndromes in this study. There are 90 samples that were used to train and test the proposed AI-powered syndrome detector. The dataset comprises of four broad syndrome categories, that is; Down Syndrome, Williams Syndrome, Turner Syndrome and a combined category called Others, which represents other rare syndromic cases. The table reflects the frequency (number of samples) as well as the percentage contribution of each class of syndromes to the total data set.

Table 1: Dataset Distribution Table

Syndrome Type	Frequency	Percentage
Down Syndrome	30	33.3%
Williams Syndrome	20	22.2%
Turner Syndrome	15	16.7%
Others	25	27.8%
Total	**90**	**100%**

Table 1 shows that the Down Syndrome is the highest value in the dataset, having 30 samples (33.3%), which is why it is the most represented syndromic category. Next are Williams Syndrome and Turner Syndrome with 20 samples and 15 samples respectively (22.2 and 16.7). The rest 25 samples (27.8) belong to the category Other syndromes since the data set encompasses the variety of other genetic or developmental disorders. The general trend in the distribution shows a comparatively well-balanced dataset, which means that the suggested deep learning model will be trained on the multiple categories of the syndrome and will be able to generalize might data on the various clinical conditions.

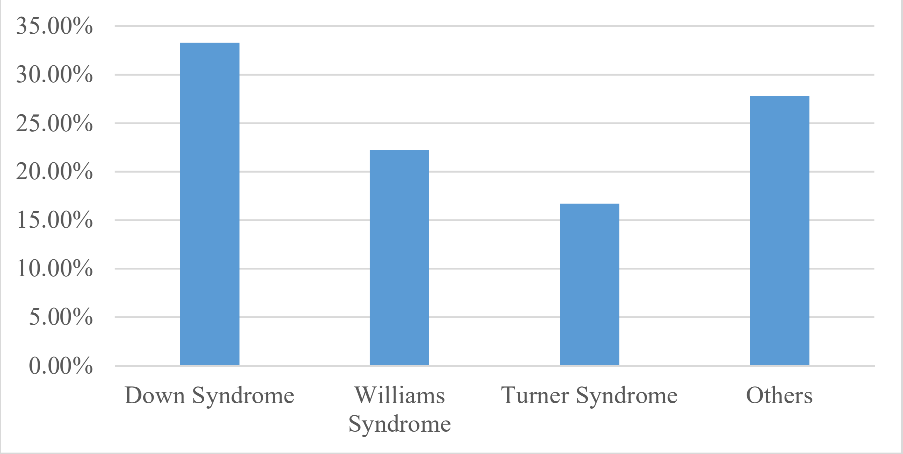

Figure 1: Graphical Representation of the Percentage of Syndrome classes among

Figure 1 graphical representation proves that the percentage share of Down Syndrome is the largest among all categories, which means that it is strongly represented in the dataset. The figure also indicates that the other syndromes category is the second-largest category, indicating that several rare disorders other than the three major syndromes are included. Williams Syndrome and Turner Syndrome are presented with relatively small yet noticeable proportions. The choice of this distribution is relevant to AI-based syndrome detection, since, in this way, features of both frequent and less frequent types of syndromes are learned by the model. Nevertheless, the minor imbalance between classes might necessitate the use of methods like data augmentation, weighted training to enhance the classification impartiality and accuracy further.

The gender distribution of sample used in the study is seen in Table 2. There were 90 samples of facial images used to train and test the suggested secure cloud-based AI-powered syndrome recognizer platform. The table breaks down the dataset by two categories that are male and female and records the frequency as well as the percentage contribution of each gender category.

Table 2: Gender Distribution

Gender	Frequency	Percentage
Male	48	53.3%
Female	42	46.7%
Total	90	100%

As Table 2 presents, there are 48 male samples and 42 female samples in the dataset, which constitute 53.3 and 46.7 percent of the total sample, respectively. This shows a relatively equal gender distribution at a slight margin with fewer females. The near-equal gender distribution is necessary in the medical computer vision applications since facial features and syndrome-based phenotypic patterns may vary among the sexes. Thus, such balanced data improves the generalization capacity and minimized the risk of gender bias in the identification of syndromes in the model.

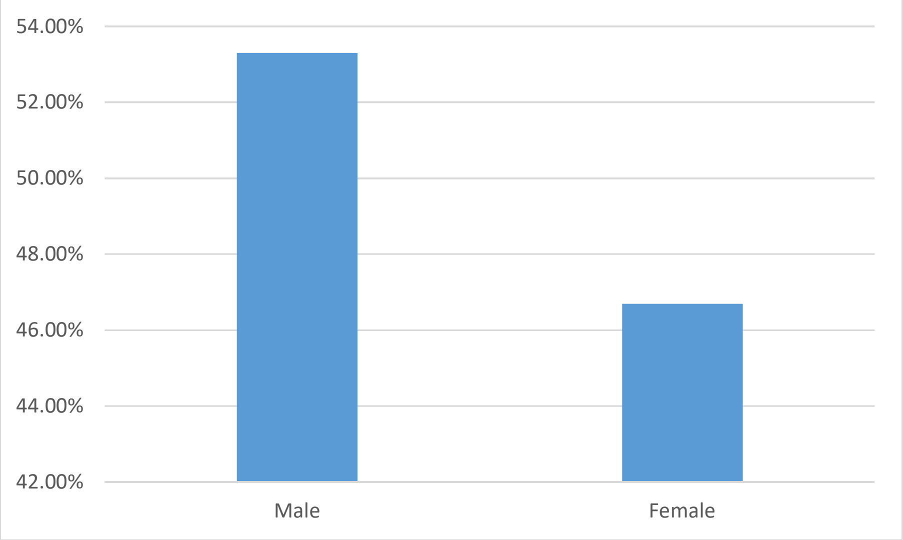

Figure 2: Graphical Representation of the Percentage of Gender Distribution

https://doi.org/10.63665/IJMEC.1102.03
ISSN: 2456-4265
IJMEC 2026

Figure 2 as a graphical representation of the data proves that 53.3 percent of the dataset is represented by males whereas 46.7 percent is represented by females. This slight disparity between the two groups shows that the sample is not highly skewed in one of the genders. Such equal gender distribution makes the suggested AI-based syndrome detection system more reliable and enables effective and impartial diagnostic work with both male and female participants.

5. CONCLUSION

The study suggested a safe cloud-based system of AI-assisted syndrome recognition, addressing the issues of diagnostic accuracy and privacy of healthcare data by incorporating the acquisition of facial images, the by-products of the deep learning-based feature extraction with the help of convolutional neural networks, the classification of syndromes with the help of the Softmax, and the deployment of the system using safe encryption systems. They experimentally tested a dataset of 90 facial image samples with a variety of syndrome types, and Down Syndrome was the largest category (33.3), and other rare syndromes were 27.8, which provided a diversity of clinical cases. Moreover, gender distribution was quite well balanced with 53.3 % males and 46.7 % females having a sample thus eliminating the chances of gender bias when making classification results. All in all, the findings suggest that the suggested secure AI-cloud architecture can indeed be used in the most effective way to facilitate reliable syndrome diagnosis without undermining high privacy and cybersecurity levels, which makes it an attractive option to be used as a smart clinical decision support system in both high-technology and long-distance healthcare facilities.

6. FUTURE WORK

- Expand the syndrome dataset to include a wider range of rare disorders, improving model generalization and diagnostic accuracy.
- Integrate multimodal inputs such as speech patterns, behavioral cues, and motion analysis to enable more comprehensive syndrome assessment.
- Incorporate blockchain-based audit mechanisms to ensure transparency, traceability, and trustworthy monitoring of medical AI decision-making processes.
- Strengthen system robustness through further studies focused on defending against adversarial attacks and emerging cybersecurity threats.
- Conduct extensive clinical validation to evaluate real-world performance and reliability.
- Ensure regulatory compliance in line with healthcare standards before deployment.
- Implement large-scale testing and deployment in real hospital environments to assess feasibility, scalability, and practical impact.

REFERENCES

1. Kumar, V. AI-Powered Threat Identification and Categorization in a Combined Security Architecture for Cloud Computing Environments.
2. Menon, U. V., Kumaravelu, V. B., Kumar, C. V., Rammohan, A., Chinnadurai, S., Venkatesan, R., ... & Selvaprabhu, P. (2025). AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. *IEEE Access*.
3. Vasamsetty, C., Nippatla, R. P., Kadiyala, B., Alavilli, S. K., & Boyapati, S. (2024). AI-Powered Healthcare Services in Banking: A Hybrid Deep Learning Framework for Secure Cloud-Based Medical Data Processing. *International Journal of HRM and Organizational Behavior*, *12*(2), 449-461.
4. Shaikh Abdul Hannan (2026), Smartphone-Based Mahchine Learning for Authomated Diagnosis using Eye, Skin and Voice Signals, International Journal of Computer Science Engineering Techniques (IJCSE), January 2026, ISSN: 2455-135X.
5. Radhakrishnan, P., Ramar, V. A., Kushala, K., Induru, V., & Palanisamy, P. (2024). Enhancing Threat Detection in Healthcare Systems Through Cloud-Based Security Solutions. *International Journal of Multidisciplinary and Current Research*, *12*(2), 180-189.
6. Sheppard, A. L., & Wolffsohn, J. S. (2018). Digital eye strain: Prevalence, measurement and amelioration. *BMJ Open Ophthalmology, 3*(1), e000146.
7. Shaikh Abdul Hannan, "Implementation of Deep Learning System for the Detection and Identification of Neurological Illness," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), December 2025.
8. Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., Van Der Laak, J. A. W. M., Van Ginneken, B., & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis, 42*, 60–88. https://doi.org/10.1016/j.media.2017.07.005
9. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562.
10. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M. N., Landman, B. A., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R. M., Trask, A., Xu, D.,

Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. *NPJ Digital Medicine, 3*(1), 119.

11. Islam, S. M. 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.
12. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444.
13. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems, 56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021
14. Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on Cloud Computing* (pp. 268–275). IEEE. https://doi.org/10.1109/CLOUD.2010.42
15. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115.
16. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646.
17. Shickel, B., Tighe, P. J., Bihorac, A., & Rashidi, P. (2018). Deep EHR: A survey of recent advances in deep learning techniques for electronic health record analysis. *IEEE Journal of Biomedical and Health Informatics, 22*(5), 1589–1604.
18. Manoj Khandare, Shaikh Abdul Hannan and R.J. Ramteke, "Technique used in TTS for International Language : Review", journal of Advance Research In Computer Engineering: An International Journal ", July to December 2009, issue of the journal.
19. Rosenfield, M. (2016). Computer vision syndrome: A review of ocular causes and potential treatments. *Ophthalmic and Physiological Optics, 36*(5), 502–515. https://doi.org/10.1111/opo.12315
20. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature, 542*(7639), 115–118.
21. Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of Medical Internet Research, 13*(3), e67. https://doi.org/10.2196/jmir.1867
22. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993.
23. Ting, D. S. W., Pasquale, L. R., Peng, L., Campbell, J. P., Lee, A. Y., Raman, R., Tan, G. S. W., Schmetterer, L., Keane, P. A., & Wong, T. Y. (2019). Artificial intelligence and deep learning in ophthalmology. *British Journal of Ophthalmology, 103*(2), 167–175.
24. Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence, 2*(6), 305–311. https://doi.org/10.1038/s42256-020-0186-1
25. Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging security mechanisms for medical cyber physical systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics, 13*(3), 401–416. https://doi.org/10.1109/TCBB.2015.2469655
26. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
27. Samek, W., Wiegand, T., & Müller, K.-R. (2017). Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models. *ITU Journal: ICT Discoveries, 1*(1), 39–48.
28. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11.
29. V. Chunduri, S. A. Hannan, G. M. Devi, V. K. Nomula, V. Tripathi, and S. S. Rajest, "Deep convolutional neural networks for lung segmentation for diffuse interstitial lung disease on HRCT and volumetric CT," in Advances in Computational Intelligence and Robotics, IGI Global, USA, pp. 335–350, 2024
30. Shaikh Abdul Hannan, Pushparaj Pal, "Detection and classification of kidney disease using convolutional neural networks", Journal of Neurology and Neurorehabilitation Research, Vol 8, Issue 2, pp 1-7, 2023.
31. Zebin, T.; Scully, P.J.; Peek, N.; Casson, A.J.; Ozanyan, K.B. Design and Implementation of a Convolutional Neural Network on an Edge Computing Smartphone for Human Activity Recognition. IEEE Access 2019, 7, 133509–133520.
32. Sidrah Liaqat, Kia Dashtipour, Kamran Arshad, and Naeem Ramzan. 2020. Non-invasive skin hydration level detection using machine learning. en. Electronics (Basel), 9, 7, (July 2020), 1086.