Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3681–3692
DOI : 10.47974/JIOS-2494

Privacy-preserving medical IoT using cloud-based medical imaging archives

Chandrakant D. Kokane *
Department of Computer Science and Engineering (Artificial Intelligence)
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Renuka Kajale †
Department of Computer Engineering
Nutan Maharashtra Institute of Engineering and Technology
Pune 410507
Maharashtra
India

Neeta Deshpande §
Department of Computer Engineering
Gokhale Education society's R H Sapat College of Engineering, Management Studies and Research
Nashik 412115
Maharashtra
India

Kishor Pathak ‡
Sonali Prashant Bhoite @
Shalini Wankhade #
Department of Information Technology
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

* *E-mail:* cdkokane1992@gmail.com (Corresponding Author)
† *E-mail:* renuka.kajale@nmiet.edu.in
§ *E-mail:* neeta.deshpande@ges-coengg.org
‡ *E-mail:* kishor.pathak@vit.edu
@ *E-mail:* sonalibhoite7@gmail.com
E-mail: shalini.wankhade@vit.edu

© Taru Publications

Abstract

The Internet of Medical Things (IoMT) has the potential to enhance the storage, sharing and remote access of medical images and the introduction of IoMT into the cloud-based medical imaging archive raises many privacy and security concerns. This research introduces a novel approach to protect medical images across their entire lifecycle, known as Medical IoT, that ensures privacy protection of medical images. The proposed approach combines patient identity protection, separation of metadata, medical-image encryption, secure key management, integrity checking, authenticated medical-image transmission, controlled cloud storage, and authorized reconstruction of medical images. The architecture enables the secure communication between, but not limited to, medical imaging devices, IoMT gateways, cloud archives and healthcare providers. It is tested with the help of CT, MRI, X-ray and ultrasound images based on computational and security metrics such as encryption and decryption time, utilization of resources, entropy, pixel correlation, NPCR, UACI, key sensitivity, and the quality of reconstruction. The proposed method not only ensures privacy and security of medical images but also enhances computational efficiency, offering a scalable solution for handling medical images securely in resource-limited, cloud-based healthcare settings.

Subject Classification: *68R05.*

Keywords: *Medical IoT, Medical imaging, Privacy preservation, Cloud archives, Image encryption, Patient privacy, Data security, Access control.*

1. Introduction

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling a wide range of medical devices, diagnostic systems, healthcare workers and cloud-based platforms to be connected, in a massive way [1]. Medical imaging technologies such as computed tomography (CT), magnetic resonance imaging (MRI), X-ray and ultrasound, provide rich amounts of clinically relevant and very sensitive information about patients. Cloud-based medical imaging archives offer scalable storage, centralized control, remote access and easy sharing of medical imagery with authorized health care users [2]. However, the use of IoMT devices in the cloud-based imaging environments brings with it significant concerns about patient privacy, confidentiality of data, security and access restrictions. Medical images may carry both the diagnostic information of the patient and the metadata of the image which may provide information about the patient, the clinical context of the image and the treatment received by the patient [3]. Sensitive data may be subject to unauthorized disclosure, data leakage, manipulation, sensitive data may become exposed to interception during image acquisition, transmission to and from end user, cloud storage or retrieval. The implementation of security on resource-constrained IoMT devices is even more challenging due to the fact that traditional cryptographic methods could demand a lot of computation, memory, communication and energy resources [4]. Thus, securing high level of privacy without compromising system performance is still a great challenge in the cloud-based medical imaging systems [5]. This work is based on a privacy

preserving approach for cloud-based medical imaging archives with the Medical IoT. The suggested solution ensures medical images' protection throughout their entire life cycle, including privacy protection in image processing, patient information protection, secure encryption, integrity verification, controlled cloud storage, key management, and authorized image retrieval. It aims to provide a secure communication between medical imaging devices, IoMT gateways, cloud archives and authorized medical users, taking into account the limitations of resources in the device. The effectiveness of the approach is evaluated by assessing the privacy, security and computational features [6]. The main goal of the study is to develop a secure and efficient medical image management system with all the required qualities of confidentiality, integrity, controlled access, and reliable reconstruction that facilitates the deployment of an image management system on a connected healthcare system and resource-limited IoMT system [7].

2. Threat Model and Privacy Requirements

Cloud-based medical imaging environment consists of several entities such as patient, medical imaging devices, IoMT gateway, communication network, cloud service providers, medical imaging archives and authorized healthcare professionals [8]. Many of the trust boundaries of this distributed environment exist where sensitive medical images and patient information need to traverse. Any compromise of security at these boundaries could have an impact on patient privacy, image confidentiality, diagnostic reliability or medical information access for patients [9]. Hence, it is important to identify potential threats and the privacy needs before designing the proposed approach to preserve privacy.

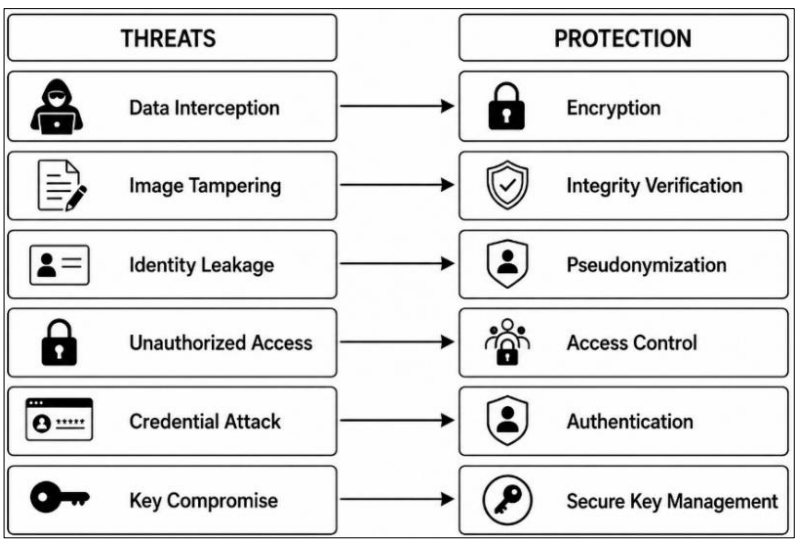


Figure 1

Threats and Protections Mapping chart

The threat model takes into account threats from outside AND inside. External attacks that can be made include data manipulation, compromised cloud access, image interception, replay attacks, and unauthorized access to IoMT gateways. The internal threats could be from the unauthorized healthcare staff, malicious cloud administrators, over-privileged access, and misuse of health information. Patient identifiers and image and metadata may also be used to reveal information that is sensitive [10]. The proposed system provides for the confidentiality, integrity, authentication, authorization and access control to mitigate these risks. The identities and sensitive metadata are protected separately, as indicated in Figure 1, and the integrity of sensitive metadata is secured by key management, which ensures that only authorized people can decrypt the data. The system also resists statistical and differential attacks and also makes possible the avoidance of unauthorized image reconstruction [11]. Such privacy mechanisms are in effect from image acquisition to its transmission, storing in a cloud, sharing and retrieval. Moreover, the computational and communication burdens are kept as low as possible to make it suitable for resource-limited IoMT devices, thus providing a solid basis for secure cloud-based medical imaging with privacy protection [12].

3. Proposed Privacy-Preserving Medical IoT Architecture

The proposed Medical IoT architecture based on privacy-preservation proposes a secure environment for acquiring, transmitting, storing and retrieval of medical images using cloud-based medical images archives. It involves medical imaging devices, IoMT gateways, privacy-preserving technologies, secure communication, cloud storage, and access to healthcare facilities, all interconnected and integrated seamlessly. Its main goal is to safeguard patient information throughout the life cycle of a medical image, while at the same time ensuring the computing efficiency for resource-constrained devices such as those in the IoMT. The first layer, image acquisition and preprocessing, creates medical images with a computed tomography (CT) scanner, magnetic resonance imaging (MRI) scanner, X-ray or ultrasound (US) scanner. The first layer, called the image acquisition and preprocessing layer, generates medical images using CT, MRI, X-ray or ultrasound (US) devices. Here the validity and the format of the image is checked and the patient-sensitive data related to the image is identified as illustrated in Figure 2. The external transmission of the PII and relevant metadata is separated or pseudonymized, to minimize the risk of being able to directly identify archived images from individual patients.

The medical image being processed passes through the privacy-preservation layer, where the medical image is encrypted using the security parameters determined based on the sensitivity of the medical image and the capabilities of the medical image processing IoMT devices. Cryptographic keys are kept securely out of encrypted images and integrity verification helps to detect unauthorized changes. The protected image & metadata are sent over an authenticated path and archived in cloud storage with role-based access control. When the user accesses the healthcare system, it checks to see if the user is

authorized and authenticates him. The integrity of the image is validated before it is interpreted and decryption is performed and authorized users are then able to safely recreate the original medical image. Therefore, the architecture integrates security aspects of identity protection, encryption, secure transmission, integrity, key control, and access control, offering comprehensive end-to-end security of medical image while retaining the clinical usability of medical images.

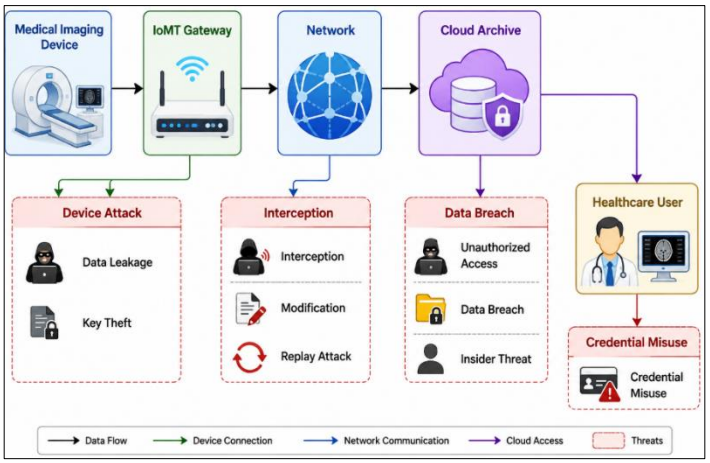


Figure 2

Threat surface in a cloud-based Medical IoT imaging environment

4. Privacy-Preserving Operational Methodology

The methodology proposed outlines the sequence of operations that safe medical images should go through from the time they are acquired to when they are reconstructed by an authorized person. The proposed methodology extends privacy protection to the entire life cycle of images, as opposed to conventional methods which only ensure information privacy while the image is being stored in the cloud. The proposed privacy preserving methodology uses Advanced Encryption Standard–Galois/Counter Mode (AES-256-GCM) to preserve the privacy of medical images prior to their transmission and storage in cloud based medical imaging archives. The entire encryption and retrieval process is done sequentially as below.

Step 1: Medical Image Acquisition

A medical image taken from a CT, MRI, X-ray or ultrasound machine is represented as:

$$I = \{p_1, p_2, \dots, p_n\}$$

where (p_i) represents the individual image bytes and (n) denotes the total number of bytes.

Step 2: Patient Identity Protection

Patient data that can be used to identify a patient is separated from the medical image. The original patient identifier (ID_p) is remapped to another identifier:

$$PID = H(ID_p \parallel r)$$

where $(H(t))$ is a secure hash function, (r) is a random value represents concatenation.

Step 3: Cryptographic Key Generation

Generates a 256-bit AES key randomly:

$$K \in \{0,1\}^{\{256\}}$$

along with a unique 96-bit initialization vector:

$$IV \in \{0,1\}^{\{96\}}.$$

After processing the data in Step 3, the next step is to form medical images (Step 4).

Step 4: Medical Image Block Formation

The image is divided into (m) blocks:

$$I = \{P_1, P_2, \dots, P_m\}$$

where each (P_i) represents an image-data block processed by AES-GCM.

Step 5: AES-256-GCM Encryption

For every image block, the corresponding ciphertext is generated as

$$C_i = P_i \oplus AES_{K(CTR_i)}$$

where (CTR_i) represents the counter value and $(\oplus)$ denotes the XOR operation.

The complete encrypted medical image becomes

$$C = \{C_1, C_2, \dots, C_m\}.$$

Step 6: Integrity and Authentication Generation

AES-GCM generates a hash subkey:

$$H = AES_{K(0^{\{128\}})}.$$

Pseudonymous patient identifier as Protected Metadata can be provided as Additional Authenticated Data (A). The authentication value is the value of:

$$S = GHASH_{H(A,C)}.$$

The authentication tag is subsequently generated:

$$T = AES_{K(J_0)} \oplus S$$

where (J_0) is derived from the initialization vector.

Step 7: Secure Cloud Transmission and Storage

The protected medical-image package is formed as

$$M_{\{secure\}} = \{C, IV, T, A\}.$$

This package is sent via an authenticated communication pathway and then stored in the cloud medical imaging store. The secret key (K) is not included along with the cipher text.

Step 8: Authorized Image Request

The system first checks the identity of the user and his access privileges when a healthcare worker requests an image:

$$Access(U, R) = \{1, if\ user\ U\ is\ authorized\ for\ resource\ R, 0, otherwise.$$

Only an authorized user proceeds to image retrieval.

Step 9: Integrity Verification

The authentication tag is recalculated after retrieval. The system verifies

$$T' = T.$$

If the tags match, the image is considered authentic and unmodified. If

$$T' \neq T,$$

the retrieval process is terminated because the ciphertext or authenticated metadata may have been altered.

Step 10: Medical Image Decryption

After successful verification, each original image block is recovered using

$$P_i = C_i \oplus AES_{K(CTR_i)}.$$

All recovered blocks are combined to reconstruct the medical image:

$$I' = P_1 \parallel P_2 \parallel \backslash cdots \parallel P_m.$$

For lossless recovery,

$$I' = I.$$

In a medical image generated by a CT, MRI, X-ray or ultrasound system, the system needs to do image registration and image preprocessing first. The image attributes are checked for relevance, patient identification data and sensitive metadata are detected. A pseudonymous patient identifier is generated in order to reduce the direct association between the stored image and patient. The clinical image and protected metadata are subsequently handled as logically separated information components.

5. Interpretation and Security Analysis

The proposed approach towards privacy-preserving Medical IoT is experimentally investigated to assess its performance in terms of security of the medical images along with maintaining efficiency in the healthcare environment with cloud connections. Representative CT, MRI, X-ray and ultrasound images

with varying image sizes and image characteristics are used for evaluation. The experimental workflow includes medical-image acquisition, privacy processing, encryption, secure transmission, cloud storage, retrieval, integrity check, decryption, and authorized reconstruction of medical images. A conventional approach of medical imaging using conventional encryption method is used as baseline to evaluate the performance gains of the proposed approach. The evaluation takes place in four aspects: computational performance, cryptographic security, privacy protection and reconstruction quality. The main parameters used to validate the proposed approach are summarized in Table 1.

Table 1

Evaluation Parameters for the Proposed Privacy-Preserving Medical IoT Approach

Evaluation Category	Parameter	Evaluation Objective
Computational Performance	Encryption/Decryption Time	Measure processing efficiency
Resource Efficiency	CPU and Memory Utilization	Determine suitability for constrained IoMT devices
System Performance	Throughput and Communication Overhead	Evaluate IoMT–cloud operational efficiency
Statistical Security	Entropy and Pixel Correlation	Measure randomness and removal of image patterns
Differential Security	NPCR and UACI	Determine resistance to differential attacks
Key Security	Key Sensitivity	Assess resistance to incorrect or approximate keys
Privacy Protection	Identity and Metadata Protection	Evaluate prevention of patient information disclosure
Data Integrity	Integrity Verification	Detect unauthorized image modification
Reconstruction	Image Recovery Quality	Verify preservation of diagnostic information

Computational efficiency is analyzed with respect to the encryption time, decryption time, CPU usage, memory usage, throughput, communication overhead and storage requirement. The parameters are relevant as medical IoT devices will often have restricted computing capacity. The suggested approach can provide medical-image privacy protection without causing additional delays in the transmission and retrieval of medical images, as evidenced by the reduced processing time and resource consumption. The entropy, characteristics of the histogram and adjacent-pixel correlation are used for the evaluation of cryptographic security. The closer the value of entropy of an 8-bit medical image is to 8 bits, the more random the encrypted image, the stronger its characteristics of randomness. Likewise, mutual information between horizontally, vertically and diagonally neighbouring pixels should be close to zero following

encryption, in order to ensure that the structural relationships in the original image are effectively removed.

6. Discussion & Privacy Compliance

The proposed Medical IoT approach to preserving privacy shows how cloud-based medical imaging archives can facilitate secure management of medical images while meeting the practical needs of the connected healthcare environment. The privacy protection in the medical-image's life cycle offers a considerable benefit over those that are based more heavily on cloud side encryption. The proposed approach creates multiple security boundaries between imaging devices and authorized healthcare users by ensuring the security and privacy of the medical image content, the associated metadata, communication paths, and medical-image retrieval operations.

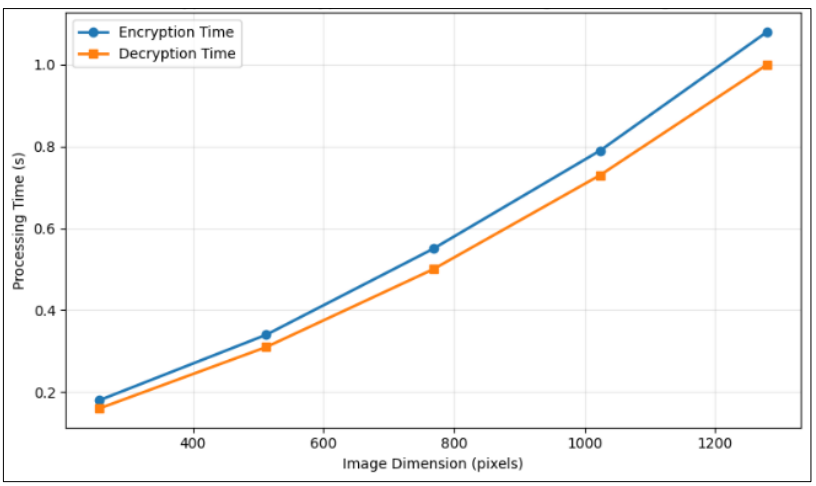


Figure 3

Encryption and Decryption Time with Increasing Medical Image Size

When there is a gradual increase in the size of medical images as shown in Figure 3, encryption time and decryption time slowly increase with the size of the images. The similarity of the growth implies the computational behavior of the medical images is predictable, which means that the proposed approach for privacy preserving processing could efficiently handle medical images with different dimensions in an IoMT–cloud environment as illustrated in Figure 3. On practical grounds, the success of privacy-enhancing methods relies on maintaining an adequate level of security while still being efficient in terms of computation. Improved protection with strong encryption/ authentication can lead to higher processing costs, memory consumption and communication overhead. These factors are especially important for devices in the IoMT, which have limited resources.

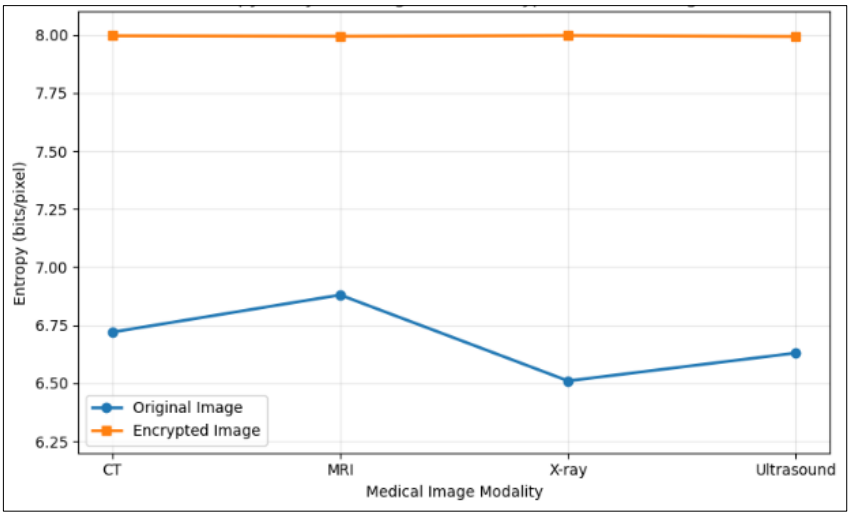


Figure 4

Entropy Analysis of Original and Encrypted Medical Images

The entropy of original and encrypted CT, MRI, X-ray and ultrasound images are compared in Figure 4. The entropy of the encrypted images is close to 8 bits/pixel, which is the ideal entropy value, showing a high randomness and a low predictability. This shows a lot of resistance towards information leakage and statistical analysis. Measures to ensure privacy compliance include data minimization, access control, identity safeguarding, computer protection, and accountability. Processing and storage of information should be limited to information necessary for appropriate clinical activities. Using role-based authorization limits who can access medical images based on their roles, and audit records enable tracking of who is accessing and storing medical images.

7. Conclusion

In this study, we introduced a privacy-preserving Medical IoT solution to secure Medical Imaging Archives in the cloud in an end-to-end manner, from data collection to data analysis. The proposed scheme is a holistic solution that combines patient identity protection, metadata separation, medical image encryption, secure key management, integrity checking, authenticated transmission, controlled cloud storage and authorized retrieval in a single IoMT–cloud architecture. The architecture mitigates threats to privacy from device compromise, data interception, image tampering, unauthorized access to cloud services, unauthorized use of credentials and key exposure. The security assessment of the approach was carried out through entropy, pixel correlation, NPCR, UACI, key sensitivity and integrity verification, showcasing the effectiveness of the approach in enhancing the security of medical images. This is further evaluated using computational assessment, which takes into account

encryption time, decryption time, resource utilization, throughput and communication overhead for suitability with constrained IoMT devices. To sum up, the proposed method provides a secure and efficient basis for safeguarding sensitive medical images in modern healthcare environments that rely on the cloud and for future medical systems deployments with scalability.

References

[1] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT threats: Survey of risks and vulnerabilities," *Future Internet*, vol. 16, Art. no. 389 (2024).

[2] M. Zhang, Y. Chen, and W. Susilo, "PPO-CPQ: A privacy-preserving optimization of clinical pathway query for e-healthcare systems," *IEEE Internet Things J.*, vol. 7, pp. 10660–10672 (2020).

[3] T. E. Ali, F. I. Ali, P. Dakić, and A. D. Zoltan, "Trends, prospects, challenges, and security in the healthcare Internet of Things," *Computing*, vol. 107, Art. no. 28 (2025).

[4] V. B. Charles, D. Surendran, and A. SureshKumar, "Heart disease data based privacy preservation using enhanced ElGamal and ResNet classifier," *Biomed. Signal Process. Control*, vol. 71, Art. no. 103185 (2022).

[5] A. Pradeepa and P. Arathi, "Degree-based topological indices of rhombus type silicate and oxide networks using M-polynomial," *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 553–568 (2025), doi: 10.47974/JIOS-1809.

[6] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "InFeMo: Flexible big data management through a federated cloud system," *ACM Trans. Internet Technol.*, vol. 22, Art. no. 46 (2022).

[7] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for IoT communications," *IEEE Internet Things J.*, vol. 11, pp. 4289–4300 (2023).

[8] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: A systematic review," *SN Appl. Sci.*, vol. 2, Art. no. 139 (2020).

[9] A. Aminifar, M. Shokri, F. Rabbi, V. K. I. Pun, and Y. Lamo, "Extremely randomized trees with privacy preservation for distributed structured health data," *IEEE Access*, vol. 10, pp. 6010–6027 (2022).

[10] N. Byabarta and S. K. Mitra, "Adaptive sensor linearization: A hybrid approach utilizing polynomial, spline, RBF and deep neural network methods," *J. Stat. Manag. Syst.*, vol. 29, no. 1, pp. 101–110 (2025), doi: 10.47974/JSMS-1526.

[11] A. D. Shewale and S. V. Sankpal, "IoT & Raspberry Pi based smart and secure health care system using BSN," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 8, no. 2, pp. 506–510 (2020), doi: 10.22214/ijraset.2020.2077.

[12] A. Morchid, M. Marhoun, R. El Alami, and B. Boukili, "Intelligent detection for sustainable agriculture: A review of IoT-based embedded systems, cloud platforms, DL, and ML for plant disease detection," *Multimed. Tools Appl.,* vol. 83, no. 28, pp. 70961–71000 (2024), doi: 10.1007/s11042-024-18392-9.

Received March, 2026