PRIVACY-PRESERVING MEDICAL IMAGE SHARING AND FEDERATION DISEASE DIAGNOSIS USING ECC WATERMARKING

[1]Arthi R, [2]Sadhana S, [3]Dinesh S, [4]Hariharan R, [5]Prasanth V

[1]Assistant Professor, Department of CSE(Cyber Security),, Muthayammal Engineering College.

[2]Assistant Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[3,4,5]Student, Department of CSE(Cyber Security), Muthayammal Engineering College.

[1]arthiramcse@gmail.com, [2]sadhana.s.cyber@mec.edu.in, [3]dineshsasikumar63@gmail.com, [4]anburajesh011@gmail.com, [5]prashanthdhana1829@gmail.com

ABSTRACT - The rapid digitization of healthcare has increased the reliance on medical imaging for disease diagnosis. However, sharing sensitive medical images across scan centers, hospitals, and doctors poses significant privacy and security risks. In the current scenario, patient data and scan images are often transmitted or stored without strong identity protection, making them vulnerable to unauthorized access, tampering, and data breaches. Existing systems rely on traditional encryption of images or central storage of raw data, which can compromise privacy and violate regulatory compliance standards.Patient-controlled access is enforced by verifying the login ID against the watermark embedded in the scan image; ECC-secured federated learning, and controlled access mechanisms, the proposed system establishes a privacy-preserving, secure, and efficient framework for medical image sharing and distributed disease diagnosis

KEYWORDS - Web Security, SQL Injection, Cross-Site Scripting (XSS), Cybersecurity, Vulnerability Assessment, Ethical Hacking, Penetration Testing, Security Frameworks, Automated Threat Detection

1. INTRODUCTION

The rapid advancement of digital healthcare and telemedicine has dramatically increased the volume of medical images generated daily, including CT scans, MRI, X-rays, and ultrasound images. These images are crucial for accurate disease diagnosis and treatment planning. However, sharing such sensitive data between scan centers, doctors, and patients introduces significant privacy and security challenges. Traditional systems often rely on storing raw images or encrypting entire datasets without embedding patient identity, which can lead to un Moreover, centralized disease prediction models require access to raw data authorized access, data tampering, and breaches of confidentiality.

In the current scenario, medical images are transmitted across networks or stored in servers without robust identity binding, making it difficult to verify whether the individual requesting access is the legitimate patient.

1.1 SCOPE OF THIS PROJECT

This project aims to:

- The scope of this project encompasses the secure management, sharing, and access of medical images while preserving patient privacy.
- By embedding the patient's original ID into scan images using robust watermarking.
- The system ensures that only authorized individuals can verify and access the images and related diagnostic reports.
- The project also incorporates patient-controlled access mechanisms and alert systems for unauthorized attempts, making it suitable for hospitals, diagnostic centers, and telemedicine platforms where secure and traceable access to medical data is critical.
- It provides a framework that can handle multiple imaging modalities such as CT, MRI, X-ray, and ultrasound scans without compromising image integrity.

The project extends to privacy-preserving disease prediction using federated learning, where doctors train models locally and only encrypted updates are shared with the central server.

2. PROPOSED WORK

The proposed system addresses the privacy and security challenges of existing medical imaging frameworks by embedding the patient's original ID into the scan images using robust watermarking.

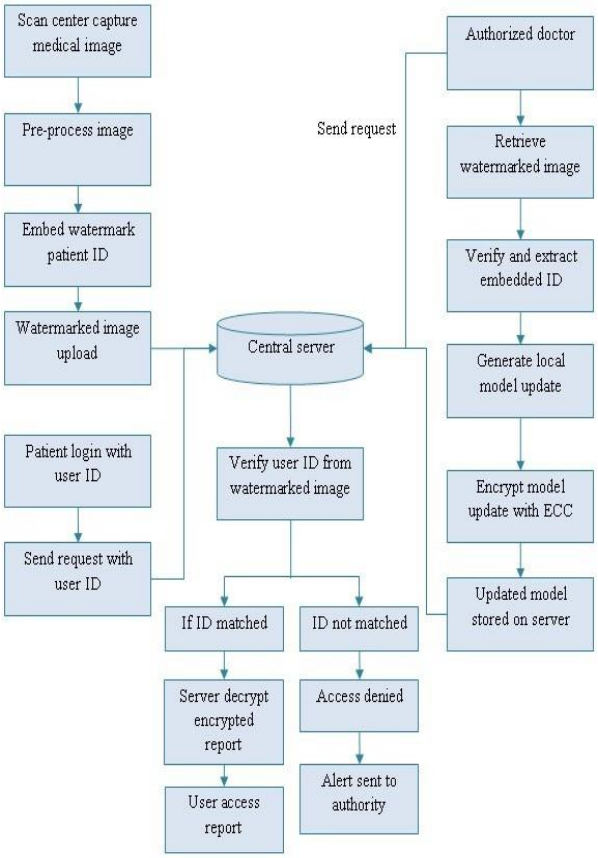
Patient-controlled access is enforced through cross-verification of login credentials against the watermark, and any mismatched or unauthorized access attempts trigger alerts to authorities, ensuring full auditability and data security.

Doctors perform local model training using decrypted images on their devices, and only model updates are shared with the central server.

The system stores encrypted diagnosis reports and maintains audit logs of access attempts, providing a secure and privacy-preserving platform for medical image management.

The proposed system offers a robust framework for secure, efficient, and compliant medical image sharing and disease diagnosis.

2.1 System Architecture



3.1 Data Processing & Preprocessing To ensure accurate results, the framework incorporates:

- **Data Collection:** Acquires medical images (CT, MRI, X-ray, ultrasound) along with patient metadata from scan centers.
- **Image Preprocessing:** Performs normalization, resizing, and format standardization to preserve diagnostic quality.
- **Identity Processing:** Generates hashed patient IDs for secure watermark embedding.
- **Watermark Preparation:** Prepares images to ensure compatibility with robust and imperceptible watermarking algorithms.
- **Learning Readiness:** Prepares preprocessed images for local disease prediction in the federated learning environment.

3.2 Security and Disease Prediction Techniques

3.2.1 Watermark-Based Identity Verification:

A robust digital watermarking technique embeds the patient's unique identifier into medical images in an imperceptible and manipulation-resistant manner. The extracted watermark is verified during access to authenticate patient identity and prevent unauthorized use.

3.2.2 Federated Learning with ECC Encryption:

Disease prediction models are trained locally on doctors' devices using federated learning. Raw images are not transmitted; only model updates are encrypted with ECC before aggregation, ensuring secure and privacy-preserving collaboration.

3.3 TOOLS AND LIBRARIES

The framework employs the following technologies:

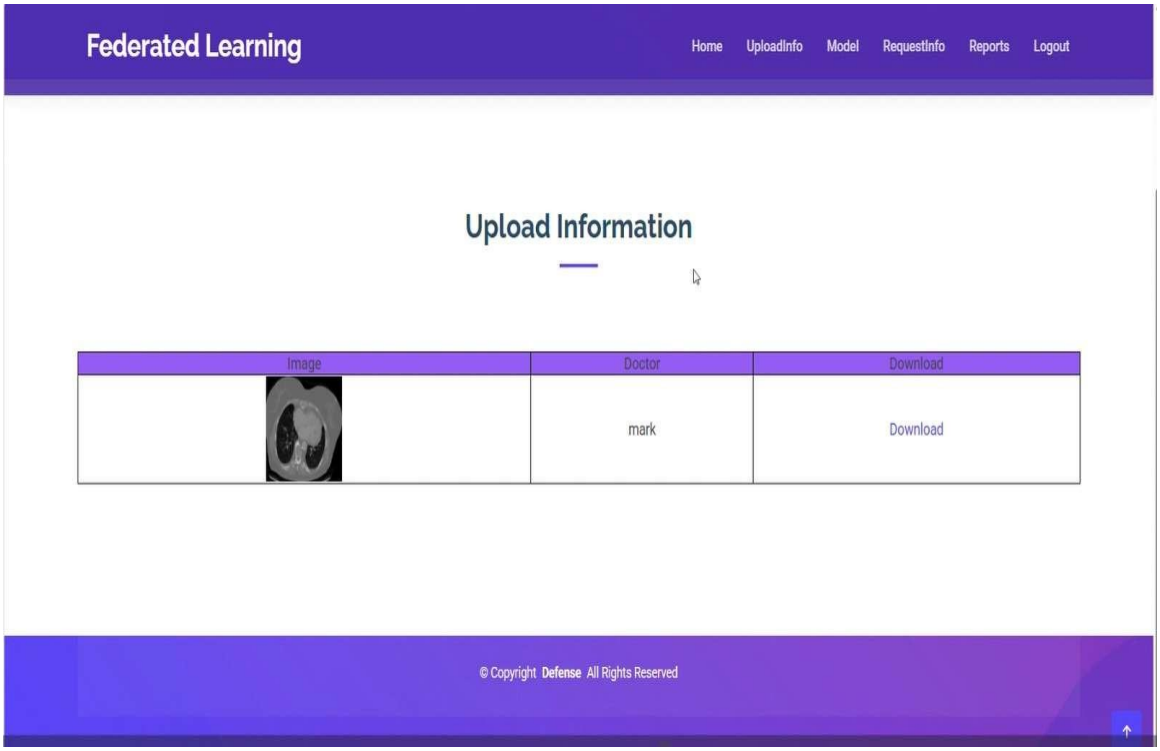
- **Python:** Handles image processing, watermarking, federated learning, and encryption.

- **TensorFlow/Keras:** Develops and trains disease prediction models.
- **Scikit-learn:** Performs data preprocessing, feature extraction, and model evaluation.
- **MySQL:** Stores encrypted medical images, reports, and logs.
- **ECC Libraries:** Encrypts model updates for secure aggregation.
- **PyCharm:** IDE for coding, debugging, and testing.

4. PROGRAM

```
from flask import Flask, request, send_file
from ecies.utils import generate_key
from ecies import encrypt, decrypt
import base64, os
app = Flask(__name__)
@app.route('/')
def home():
return "Federated Learning Secure Model"
@app.route('/upload', methods=['POST'])
def upload():
file = request.files['file']
file.save("model.bin")
key = generate_key()
pub, priv = key.public_key.format(True).hex(), key.to_hex()
data = base64.b64encode(open("model.bin", "rb").read())
enc = encrypt(pub, data)
open("enc.bin", "wb").write(enc)
return f"Uploaded & Encrypted<br>PrivateKey: {priv}"
@app.route('/download', methods=['POST'])
def download():
priv = request.form['key']
enc = open("enc.bin", "rb").read()
dec = decrypt(priv, enc)
open("dec.bin", "wb").write(base64.b64decode(dec))
return send_file("dec.bin", as_attachment=True)
if __name__ == '__main__':
app.run(debug=True)
```

5. RESULTS AND OUTPUT



SQL Injection Scan Results: Identifies vulnerable queries and assesses threat severity by analyzing database interactions.

- **XSS Scan Results:** Detects potential script injection and execution risks in web inputs and dynamic content.
- **Anomaly Detection Reports:** Flags abnormal access patterns and emerging attack behaviors in real time.
- **Remediation Recommendations:** Suggests targeted security measures such as input validation, parameterized queries, and output encoding.

6. CONCLUSION

The proposed system successfully addresses the critical challenges of privacy, security, and controlled access in medical image sharing and disease prediction. The integration of Elliptic Curve Cryptography (ECC) for encrypting model updates ensures that sensitive information within the predictive model remains secure during aggregation. Patients gain full control over access to their diagnosis reports, and any unauthorized attempts are automatically flagged and reported to authorities, enhancing auditability.

The approach reduces risks associated with data breaches, unauthorized access, and identity theft while enabling collaborative disease prediction across multiple healthcare providers.

REFERENCES

[1] Qayyum, Adnan, Junaid Qadir, Muhammad Bilal, and Ala Al-Fuqaha. "Secure and robust machine learning for healthcare: A survey." IEEE Reviews in Biomedical Engineering 14 (2020): 156-180.

[2] Masood, Fawad, Maha Driss, WadiiBoulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan. "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations." Wireless Personal Communications 127, no. 2 (2022): 1405-1432.

[3] Hasan, Mohammad Kamrul, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.

[4] Kamal, Sara T., Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. "A new image encryption algorithm for grey and color medical images." IEEE Access 9 (2021): 37855-37865.

[5] Li, Xin, and Dongxiao Zhu. "Robust detection of adversarial attacks on medical images." In 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI), pp. 1154-1158. IEEE, 2020.

[6] Müller, Dominik, Iñaki Soto-Rey, and Frank Kramer. "Towards a guideline for evaluation metrics in medical image segmentation." BMC Research Notes 15.1 (2022): 210.

[7] Salehi, Ahmad Waleed, et al. "A study of CNN and transfer learning in medical imaging: Advantages, challenges, future scope." Sustainability 15.7 (2023): 5930.

[8] Gupta, Ishu, et al. "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions." IEEE Access 10 (2022): 71247-71277.

[9] Narayanan, Uma, Varghese Paul, and Shelbi Joseph. "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment." Journal of King Saud University-Computer and Information Sciences 34.6 (2022): 3121-3135.

[10] Singh, Ashutosh Kumar, and Deepika Saxena. "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment." Journal of Applied Security Research 17.3 (2022): 385-412