A Framework for Privacy-Preserving Detection of Sickle Blood Cells Using Deep Learning and Cryptographic Techniques

Kholoud Alotaibi, Naser El-Bathy
Computer Science and Engineering, Oakland University Rochester, MI, USA

***Abstract*—Sickle cell anemia is a hereditary disorder where abnormal hemoglobin causes red blood cells to become rigid and crescent-shaped, obstructing blood flow and leading to severe health complications. Early detection of these abnormal cells is essential for timely treatment and reducing disease progression. Traditional screening methods, though effective, are time-intensive and require skilled technicians, making them less suitable for large-scale implementation. This paper presents a conceptual framework that integrates transfer learning, cryptographic algorithms, and service-oriented architecture to provide a secure and efficient solution for sickle cell detection. The framework uses MobileNet, a lightweight deep learning model, enhanced with transfer learning to identify sickle cells from medical images while operating on hardware-constrained environments. Advanced Encryption Standards (AES) ensure sensitive patient data remains secure during transmission and storage, while a service-oriented architecture facilitates seamless interaction between system components. Although not yet implemented, the framework serves as a foundation for future empirical testing, addressing the need for accurate detection, data privacy, and system efficiency in healthcare applications.**

Keywords*—Sickle cells; deep learning; transfer learning; encryption; AES; SOA

I. Introduction

Sickle cell disease (SCD) is a genetic disorder that significantly impacts the shape and function of red blood cells. Under normal conditions, red blood cells are round and flexible, allowing them to move smoothly through blood vessels but they become rigid and crescent-shaped due to defective hemoglobin, the protein responsible for carrying oxygen throughout the body, in individuals with sickle cell disease, [1, 2]. This abnormal shape causes the cells to get trapped in small blood vessels, blocking blood flow, which leads to a range of serious health complications such as pain, organ damage, and an increased risk of infections [3]. Early detection of sickle cells is very important because timely treatment can reduce these complications and greatly enhance the quality of life for those affected [4].

Even though early detection is important, traditional diagnostic methods are often complex and require highly skilled technicians, making them unsuitable for large-scale screening, particularly in low-resource settings [5]. These limitations slow down the ability to diagnose SCD sufficiently early to prevent severe health consequences. Moreover, depending on manual analysis in traditional diagnostics creates challenges in terms of speed and accessibility.

Recent advancements in artificial intelligence (AI), particularly in deep learning, have shown significant potential for automating medical image analysis with high accuracy [6]. These technologies offer faster and more efficient solutions, enabling early detection and scalable screening even in challenging settings. However, deploying AI in medical applications introduces unique challenges. For instance, ensuring patient data privacy is critical, given the sensitive nature of medical data and the strict regulations governing its use, such as HIPAA in the United States and GDPR in Europe [7]. Additionally, many deep learning models require substantial computational resources for training and inference, which limits their feasibility in environments with constrained hardware resources [8].

This paper proposes a novel framework that combines deep learning, cryptographic algorithms, and service-oriented architecture (SOA) to address these challenges. The framework uses MobileNet, a lightweight deep learning model optimized for efficient operation on hardware-constrained systems, to detect sickle cells in blood smear images. Transfer learning is employed to achieve high detection accuracy without requiring extensive computational resources. Advanced encryption techniques, such as AES, ensure patient data remains secure during transmission and storage, addressing critical privacy concerns. Furthermore, SOA enables seamless communication between system components, enhancing the system's scalability, modularity, and flexibility.

By integrating these components, the proposed framework offers a secure, efficient, and practical solution for sickle cell detection in diverse healthcare settings.

The remainder of this paper is organized as follows: Section II identifies the problem, and Section III reviews related work, focusing on previous efforts in using AI for sickle cell detection and employing cryptographic techniques to secure medical data. Section IV provides details on the proposed framework, explaining the roles of each component and how they are integrated. Section V illustrates the workflow of the system, showing how data is securely processed from start to finish. Section VI discusses the security and privacy considerations involved in the framework. Section VII outlines the feasibility and limitations of the approach, while Sections VIII and IX provide future directions and conclusions, respectively.

II. Problem Identification

A. Research Problem

Creating an automated detection system for sickle cells comes with several challenges, one of the most important being data privacy. Medical data is very sensitive and needs to be handled according to strict regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe [7]. Ensuring patient privacy is very important when using AI models which require large amounts of data for training and validation. Additionally, deploying deep learning models can require more computational resources, which is challenging in environments where advanced hardware is not easily available [8]. Therefore, there is a need for a solution that balances accuracy, privacy, and efficiency to provide a secure and practical way to detect sickle cells.

B. Research Questions

How to build a system that can correctly detect sickle cells, keep patient data private, and work well with limited hardware? How to create a solution that meets the increasing need for automated medical testing, follows important privacy rules like HIPAA and GDPR, and performs well without needing expensive hardware? These are the key challenges to solve in creating a reliable and easy-to-use system for sickle cell detection.

C. Objective

The study objective is to develop a secure and efficient framework for detecting sickle cells by integrating deep learning, cryptographic algorithms, and an SOA. This framework uses the capabilities of deep learning for analyzing medical images while ensuring that patient data remains protected through cryptographic methods. The use of SOA makes the framework modular, meaning that each component—such as encryption, model inference, and data communication—can be flexible, scalable, and easily integrated into existing healthcare systems.

D. Significance

The significance of this proposed framework is its novel integration of AI with secure computation techniques designed to address healthcare needs. The framework handles the critical issue of privacy-preserving AI in healthcare by combining deep learning for medical image analysis with cryptographic methods for secure data handling [9]. Furthermore, the use of SOA allows for flexibility and scalability, making the solution adaptable to different clinical environments. This combination of accurate detection, data security, and scalability represents a unique approach to addressing the challenges of sickle cell detection to provide accessible high-quality care while protecting patient data.

III. Related Work

A. Existing Deep Learning Solutions for Sickle Cell Detection

Deep learning has brought remarkable improvements to medical imaging, especially in automating the detection of diseases like SCD. Traditionally, diagnosing SCD requires visually examining blood smears under a microscope, which is not only time-consuming but also prone to human error. To overcome these challenges, researchers have turned to deep learning models, which make the process faster and more reliable.

Goswami and colleagues used deep neural networks like ResNet50 and GoogleNet to classify sickle cells from digital blood smear images. They also applied explainable AI techniques, such as Grad-CAM to make the predictions easier for healthcare professionals to understand. This added transparency makes the diagnostic process more trustworthy. ResNet50 was the best-performing model, achieving an accuracy of 94.9%, which shows great potential for real-world clinical use [11].

Kawuma and his team compared different deep-learning techniques for detecting SCD, such as VGG16, VGG19, and Inception V3, demonstrating that Inception V3 achieved the highest accuracy at 97.3%, followed by VGG19 at 97.0%. These results highlight the effectiveness of pre-trained models for accurately identifying sickle cells [10].

Karunasena and colleagues took a different approach, using a region-based convolutional neural network (R-CNN) to detect sickle cells. Their model achieved over 90% accuracy and was particularly useful in segmenting and classifying specific regions within an image. This level of precision is important when dealing with complex blood smear images where cells may be crowded or overlap [12].

Another review by Balde et al. focused on recent advances in using AI to detect SCD, highlighting image segmentation and feature extraction techniques. These methods, particularly CNN, have been successful in analyzing microscopic images, even when they contain overlapping cells. However, there are still challenges in improving the robustness of these segmentation techniques to accurately distinguish between normal and sickled cells, especially in more complex or densely populated images [13].

Regardless of these advancements, one key issue remains largely unaddressed, data privacy. Most studies have focused primarily on improving detection accuracy but have not paid enough attention to the sensitive nature of medical data. This gap provides an opportunity for future research to explore privacy-preserving techniques, such as encryption, to protect patient information while maintaining the diagnostic accuracy of deep learning solutions.

In summary, existing research shows significant progress in using deep learning for sickle cell detection but there is still a need for better handling of overlapping cells, and a stronger focus on data privacy to create a comprehensive solution that can be widely adopted.

B. Cryptographic Techniques in Medical Data Security

Securing medical data is important, especially when using AI and machine learning (ML) models, as these often require sensitive patient information for processing. Cryptographic techniques have been a core part of ensuring that this data remains safe throughout its lifecycle—whether during transmission, storage, or even analysis.

One interesting approach is the MASS framework which uses blockchain technology to securely share medical data collected from wearable IoT devices. In this system, health information is encrypted using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which means that only authorized individuals can access specific parts of the data. This method not only keeps the data private but also ensures it cannot be altered, thus MASS is particularly effective for protecting data from wearable medical devices [14].

Amaithi Rajan and colleagues developed a secure way to retrieve medical images from encrypted cloud storage using a combination of deep learning and encryption techniques, ensuring that the images are not only safely stored but also easily retrievable when needed. This method relies on symmetric encryption and searchable encryption, allowing users to search through encrypted data and retrieve relevant images without compromising security [15].

Ahmad Al Badawi and Mohd Faizal Bin Yusof took another interesting approach by using fully homomorphic encryption (FHE). This allows medical data to be processed without ever decrypting it, meaning patient information remains secure even during analysis. They used this method for privacy-preserving pathological assessments using support vector machines (SVMs). This approach provides both strong data protection and effective analysis, making it highly suitable for privacy-sensitive medical diagnostics [16].

A different system developed by Kusum Lata and her team focused on detecting brain tumors using deep learning while ensuring privacy through encryption. They used the AES-128 algorithm to encrypt medical images before storage or transmission to keep patient data secure, even during the diagnosis. This system is a good example of balancing the need for secure data handling with the advanced diagnostic capabilities that AI offers [17].

Lastly, Runze Wu and colleagues developed a privacy-preserving system that used Gaussian kernel-based support vector machines (SVMs) and a simpler cryptographic method known as additive secret sharing. This approach is less computationally intensive compared to more advanced methods like homomorphic encryption, making it better suited for real-time applications. It ensures that both the patient's data and the healthcare provider's model are kept private during the diagnostic process, all while maintaining efficiency [18].

Overall, these cryptographic approaches highlight the importance of keeping patient data secure while using the power of AI in healthcare. While robust encryption methods like homomorphic encryption offer high security, they can be quite demanding in terms of computation. Hence, lightweight cryptography and blockchain-based methods are becoming attractive alternatives because they balance effective security with practical resource use—especially important in healthcare, where computational power is often limited.

C. Service-Oriented Architectures in Healthcare

The SOA has become popular in healthcare because it allows systems to be broken down into smaller, independent services that work together efficiently. This approach makes healthcare technology more flexible and scalable—perfect for dealing with the complexities of modern medical institutions.

Petrenko and Boloban explain how SOA can handle the increasing volume of healthcare data and provide efficient treatment by coordinating different services. By splitting a large healthcare system into smaller, interacting services, SOA improves how data is processed and how medical resources are managed, ultimately leading to better patient care. A major advantage is that new services can be easily added to the system without causing disruptions, making SOA both scalable and adaptable [19].

Liviu Ilie and colleagues looked at how SOA could be used to create a framework that connects electronic health records with other healthcare services to boost interoperability—the ability of different systems to exchange and use information. Interoperability is important in healthcare, especially for large medical institutions that need to integrate multiple systems. SOA provides a framework that helps different services communicate effectively, improving both the quality and efficiency of healthcare. This approach makes the system more flexible, easier to upgrade, and less expensive to maintain [20].

Similarly, Petrenko and Tsymbaliuk developed a cloud-based healthcare platform called "Clinic in Cloud" that uses SOA to bring together wearable sensors, data management systems, and user interfaces. This platform allows doctors to monitor patients remotely in real time, making diagnosis and treatment more accessible. The SOA approach ensures that all these different components, sensors, databases, and communication tools, work smoothly together, enabling timely and effective patient care. The modular design also makes it easy to add new features as healthcare needs develop [21].

In summary, SOA provides a strong foundation for building healthcare systems that are flexible and scalable. By breaking down complex systems into smaller, independent services, SOA makes integration easier, data management more efficient, and services more adaptable. This is especially valuable in healthcare, where technology is continuously changing and systems need to keep up.

D. Summary of Related Work

The research on deep learning, cryptographic techniques, and SOA has greatly advanced healthcare technology but there are still areas for improvement.

Deep learning models like ResNet50 and Inception V3 have made diagnosing SCD faster and more reliable compared to traditional manual methods. However, data privacy has not been addressed, a major issue when dealing with sensitive health information.

Methods like FHE and blockchain frameworks have been used to keep patient data secure and while they are highly effective, they can be computationally heavy, limiting their practicality in real-time applications or environments with limited computing resources.

The SOA has been used to make healthcare systems more modular and scalable. SOA improves integration between different healthcare tools and makes it easier to expand systems

when needed by breaking down large systems into smaller, easier-to-manage services.

The proposed framework builds on these existing solutions by combining the strengths of each approach while addressing their limitations. By integrating lightweight deep learning with efficient cryptographic techniques like AES and an SOA-based design, the framework prioritizes patient data privacy, operational efficiency, and system scalability. Unlike current solutions, this approach places patient privacy at the forefront while ensuring adaptability to evolving healthcare needs.

IV. Proposed Framework

A. Overview of the Framework

The proposed framework aims to provide a secure and efficient way to detect sickle cells in medical images. It consists of three main components that work together to ensure accuracy, privacy, and flexibility:

- A deep learning model for detection
- A cryptographic module
- A service-oriented architecture (SOA)

A pre-trained deep learning model, MobileNet [23], was employed to identify sickle cells in blood smear images. This model correctly detects sickle cells using transfer learning without requiring significant computational power, making it ideal for setups with limited hardware. The preprocessing steps include resizing the input images and normalizing pixel values to ensure compatibility with the MobileNet architecture. Performance evaluation metrics, such as detection accuracy and inference latency, will be used during the empirical validation phase to measure the effectiveness of the model.

Advanced Encryption Standards (AES) were used to encrypt the medical images before analysis to protect sensitive patient information. This ensures that the data remains confidential during both transmission and storage, providing strong security to prevent unauthorized access. Although AES introduces some computational overhead, its efficiency makes it a practical choice for environments with limited resources, balancing security, and performance. Beyond encryption, the framework is designed to align with data protection regulations such as HIPAA and GDPR, ensuring secure and compliant handling of patient data throughout the system.

SOA connects all the components, allowing perfect communication between the cryptographic module, the deep learning model, and the other system parts. Each function—such as encryption, analysis, and reporting—is treated as an independent service, thus the system is modular and scalable so components can be updated or replaced without disrupting the rest of the system, making it easy to expand or adapt as needed.

Fig. 1 illustrates how these components interact to visualize the flow of the system. Additionally, Table I provides a detailed overview of each system component, outlining its function and purpose within the framework.

B. Components

1) Deep learning model for detection: MobileNet was the transfer learning model selected for detecting sickle cells as it is specifically designed for environments with limited resources, making it ideal for training on a CPU. It employs a technique called depthwise separable convolutions [25], reducing the number of parameters and computational complexity without sacrificing accuracy.

MobileNet V2 is highly effective for different medical imaging tasks. For example, it achieved accuracy rates as high as 94% when used for brain tumor classification after being pre-trained and fine-tuned on relevant datasets [22].

This suggests that MobileNet can also perform well for sickle cell detection tasks.

MobileNet has also been applied for breast cancer classification, delivering fast execution times even on devices with limited computational resources without compromising accuracy [23]. This makes it an ideal choice for scenarios where only a CPU is available for training and inference.

MobileNet has also been successfully integrated into ensemble models for detecting conditions like cardiomegaly, showing that it is robust and works well in combination with other models [24].

TABLE I. System Components Overview

Component	Function	Purpose
Data Input and Encryption	Uploads and encrypts medical images using AES	Protect patient data during transmission
Service-Oriented Architecture (SOA)	Connects system components and manages secure data flow	Ensures modularity and scalability
Deep Learning (MobileNet)	Analyzes medical images to detect sickle cells	Provides accurate detection of sickle cells
Data Storage/ Transmission	Encrypts and securely stores or sends results to the user	Maintains data privacy throughout the process

This flexibility demonstrates its capability to handle complex medical imaging challenges effectively.

Its lightweight architecture makes it ideal for training and deploying on a CPU, which fits the hardware limitations of the proposed framework. Unlike heavier models like ResNet or VGG, MobileNet requires far less computational power while still delivering strong performance [25]. Additionally, pre-trained weights can be used and fine-tuned on the sickle cell dataset, allowing for efficient training even without high-end hardware.

2) Cryptographic module: AES was chosen for its well-known efficiency and security when encrypting large datasets like medical images. AES supports different key lengths (e.g., 128-bit or 256-bit) and provides an excellent balance between speed and security, making it suitable for both storing and transmitting medical data securely [33].

AES has been successfully used in cloud-based medical data systems to secure sensitive patient information. It ensures that data remains protected during transmission and storage, which is important for maintaining privacy in healthcare settings [26].

In comparison studies, AES was faster than other encryption methods for both encrypting and decrypting data, making it a reliable option for handling medical images without slowing down performance [27].

AES is also effectively used in combination with techniques like watermarking [26] to guarantee both the security and integrity of medical images. This dual functionality shows the flexibility of AES in ensuring data remains protected while preserving image quality, which is essential in healthcare.

AES offers strong encryption to protect patient information, ensuring confidentiality during transmission and storage. It efficiently secures large medical datasets without slowing down the system, thus is ideal for healthcare settings where both security and efficiency are important [26].

3) Service-oriented architecture (SOA): In this framework, SOA plays a key role in enabling the different components—such as the cryptographic module, deep learning model, and data management processes—to communicate smoothly. Each function, like encryption, model analysis, and data sharing, operates as an independent service, making the system more flexible and scalable, allowing each part to be developed, updated, and managed separately.

- Benefits of Using SOA

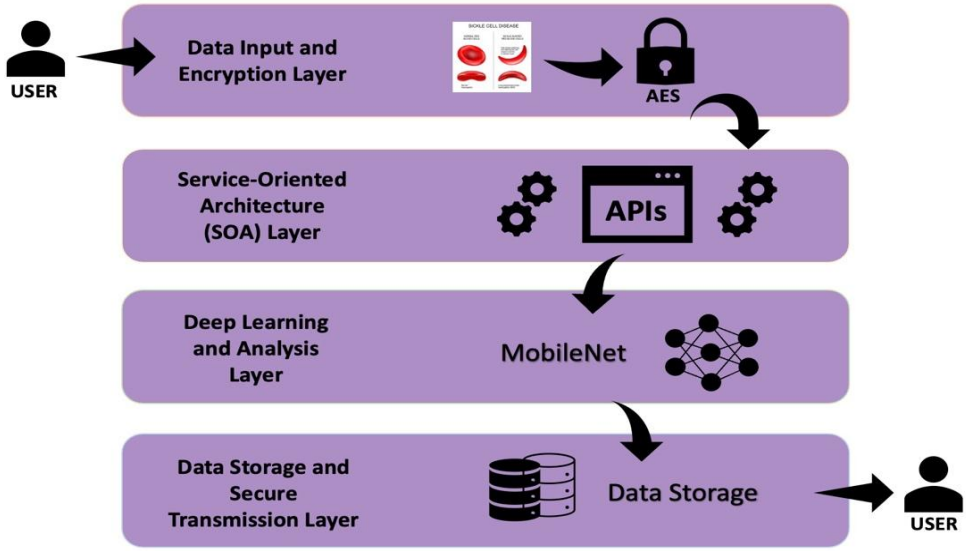

Fig. 1. High-level overview of the proposed framework showing the flow of data between components. Encrypted data is processed through the service-oriented architecture (SOA), analyzed by the Deep Learning Model (MobileNet), and securely transmitted and stored.

a) Modularity: SOA breaks down the system into smaller, reusable services so that each part, like data encryption, detection, or reporting, can be independently maintained. This modular approach makes it much easier to update or modify components without affecting the entire system. Essentially, the rest of the system can keep running smoothly if one part needs an upgrade [20, 28].

b) Interoperability: The framework includes different components such as cryptographic modules and AI models, and SOA makes sure they work well together. By using standardized protocols like SOAP and REST, SOA ensures that these services can easily communicate, even if they are built on different platforms or by different developers. This is important for smooth integration and effective communication between all system parts [28].

c) Scalability: Healthcare systems often need to handle growing amounts of data and SOA-based systems are inherently scalable, meaning new services can be added without disrupting the existing setup. This is particularly useful when integrating with cloud-based services or IoT devices for real-time monitoring, ensuring that the system can grow and adapt as needed [21].

- How SOA Enables Communication Between Modules:

SOA-based frameworks often use middleware and APIs to manage how different services interact. This not only helps standardize the flow of data but also supports plug-and-play integration, making it easy to add new components, such as an improved encryption method or an updated AI model, without causing disruptions to the rest of the system [28].

V. System Workflow

This section describes how data moves through each stage of the proposed framework, from the initial encryption of medical images to the secure return of prediction results. Each step is designed to ensure data privacy, accuracy, and efficiency.

The process starts by encrypting the medical images using AES [29] to ensure that sensitive patient data is protected from the beginning and remains confidential throughout transmission and processing.

Once encrypted, the data is securely transmitted to the deep learning service using an SOA. SOA allows the encrypted data to be passed easily between different services, making communication between the cryptographic module and the deep learning model smooth and secure [30]. This modular design ensures that the different system parts work together effectively without compromising sensitive information.

When the encrypted data reaches the deep learning model, it is first decrypted for analysis and then processed by the MobileNet [22] deep learning model to detect sickle cells in the medical images. This step generates predictions, helping identify any abnormalities in the blood smear images.

After the analysis is complete, the results are encrypted using AES to ensure privacy before they are sent back to the client. This step keeps the prediction results protected during transmission, maintaining the confidentiality of patient data at all times [30].

Fig. 2 illustrates the entire workflow, showing the interactions between each component:

1) Data encryption: Medical images are encrypted using AES for privacy.

2) Data transmission via SOA: Encrypted data is sent to the deep learning service.

3) Model inference: The deep learning model processes the data (after decryption) and generates predictions.

4) Result encryption and return: The analysis results are encrypted and returned securely to the client.

VI. Security and Privacy Analysis

The proposed framework includes different security and privacy protections to keep patient data safe and private. This section explains how privacy issues are managed, what security features are used, and how the framework balances being secure while still running efficiently.

A major concern with medical data is protecting patient privacy. The framework handles this by using AES encryption to secure medical images at every step. By locking the data before analysis and again when sending the results back, the system ensures that no one without permission can access sensitive patient information during transmission or storage. Using AES helps prevent data breaches that could compromise patient privacy in line with established privacy standards like HIPAA and GDPR which require strict protection for medical data to prevent unauthorized access [31].

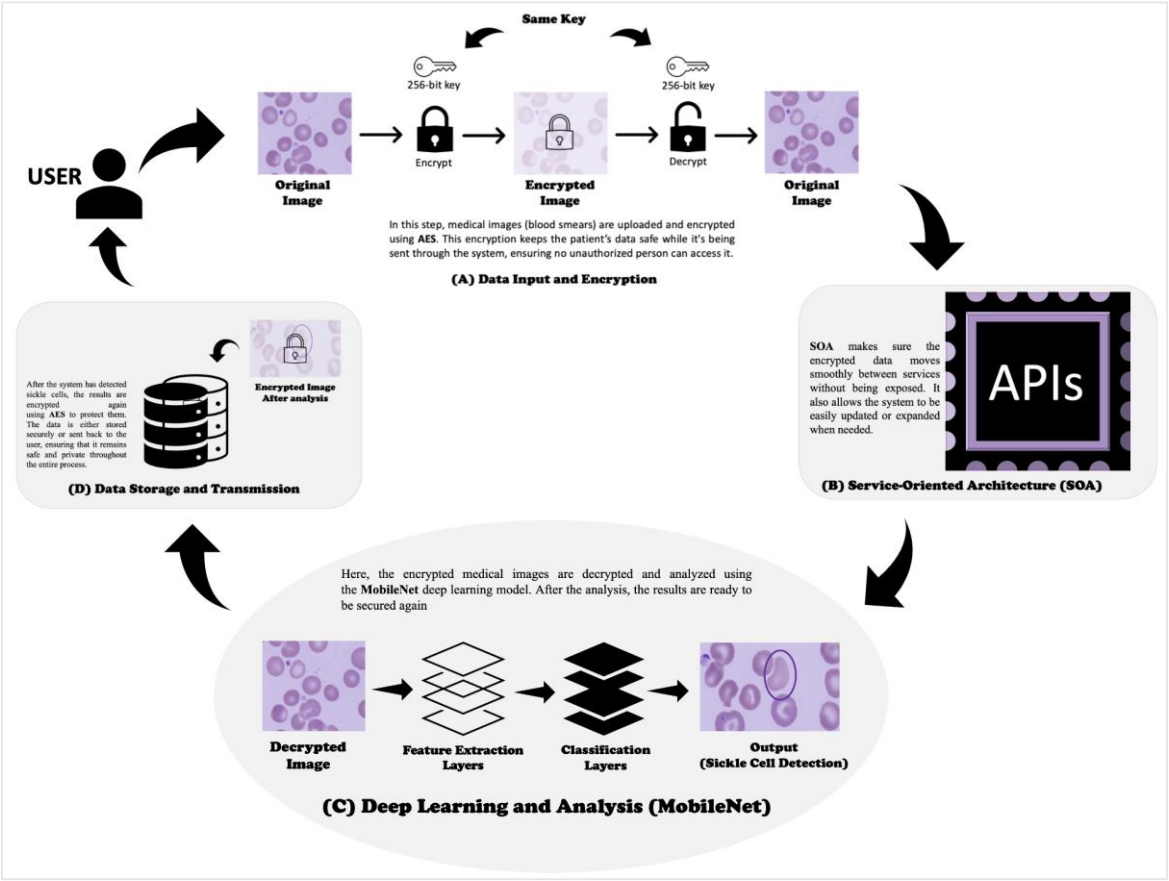

Fig. 2. System workflow diagram illustrating the flow of data within the proposed framework. The process begins with AES encryption of medical images, followed by secure transmission through SOA, analysis using the MobileNet model, and encryption of results before returning to the client. Each step ensures privacy, accuracy, and secure data handling.

The framework uses AES and other cryptographic algorithms to keep data secure and intact throughout the process. AES encrypts the data both when it is being sent and after analysis, providing:

- Confidentiality: AES keeps patient data private from the moment it is collected until the results are returned.
- Integrity: Encryption ensures that if anyone tries to tamper with the data during transmission, it becomes unreadable, keeping it accurate.

The framework also uses an SOA to safely transfer encrypted data between services, adding extra protection by reducing the risk of data exposure during transfers [30].

While security is very important, it is also necessary to consider how encryption affects system performance. AES encryption performs well at keeping data safe but can slow systems down, especially those with limited resources or using large amounts of data. Nonetheless, it is still more efficient than other options like RSA. AES finds a good middle ground between security and speed. It works well with large datasets, like medical images, because it provides strong protection without using too much computational power compared to heavier encryption methods [32].

1) Optimized workflow: Using the MobileNet model for analysis allows the framework to work efficiently, even on systems with just a CPU [23]. This helps lower the overall workload of both the encryption and the AI tasks, making the system both secure and practical for real-world healthcare use.

VII. Feasibility and Limitations

The framework is designed to work efficiently, even on systems with limited hardware like a standard CPU. This is possible through the use of MobileNet [24] with transfer learning. MobileNet is a lightweight deep learning model that reduces the computational workload by using fewer parameters compared to heavier models. By starting with a pre-trained model and only adjusting the final layers, the framework can achieve high accuracy without requiring advanced hardware, making it practical for environments with limited resources.

While the framework offers a balance between security and efficiency, a few challenges and limitations need to be addressed:

- Resource Limitations: Even though MobileNet is optimized for efficiency, using a CPU for processing may still be slower compared to a GPU, particularly when handling large datasets. This could limit the framework's scalability when analyzing a high volume of images.
- Balancing Privacy and Efficiency: There is a trade-off between ensuring data privacy and maintaining fast processing speeds. AES encryption provides strong data protection, but it adds steps to the workflow, which could slow down real-time performance.

This paper proposes a theoretical framework, and its implementation has not yet been carried out. While the framework integrates validated techniques such as MobileNet for deep learning, AES for encryption, and SOA for modularity, empirical testing will be conducted in future work. Metrics such as accuracy, latency, encryption strength, and scalability will be used to validate the framework's performance. The absence of implementation results reflects the current focus on the framework design, which serves as a foundation for future development and testing.

VIII. Future Work

The current goal is to design the framework and create a basic prototype to show how it works. In the future, the full system will be built, with all parts working together and tested in real-world situations. This full implementation will help identify practical limitations to improve the system's performance.

Once the system is fully built, a detailed evaluation of its performance will be performed, assessing the accuracy (how well it finds sickle cells) and speed (how long it takes to process each image) of the deep learning model, as well as the strength of the encryption (to keep patient data safe) and how efficiently the system runs (the encryption does not slow the system too much). The goal of this evaluation is to find the right balance between security, accuracy, and speed.

Another important future task is to determine how well the framework can handle larger datasets, like more medical images from different sources, to help understand how the system can be used in real-world healthcare, where securely and efficiently managing large amounts of data is essential.

IX. Conclusion

A. Summary

This paper presented a framework to help detect sickle cells in medical images securely and efficiently. The framework comprises three main parts: a deep learning model to identify sickle cells, a cryptographic module to protect patient data, and an SOA for efficient communication between all system parts. Together, these parts ensure that patient information stays safe during every step—from encryption to analysis and sending back the results.

B. Contribution

The main contribution of this work is creating a unique framework that combines deep learning and cryptographic techniques using an SOA-based structure. This design makes it possible to securely analyze medical images while maintaining patient confidentiality. Using MobileNet and transfer learning, the framework is also efficient for environments with limited hardware, making it useful in more healthcare settings.

C. Implications

This work is important for the future of secure AI in healthcare. This framework provides a way to develop AI solutions that not only work well but also protect patient privacy by combining strong encryption with deep learning in a scalable system. This approach can be applied to other types of medical imaging, improving diagnostics while keeping data safe—something that is becoming more important in today's digital healthcare world.

REFERENCES

[1] Ministry of Health Saudi Arabia, https://www.moh.gov.sa/en/Pages/Default.aspx.

[2] NIH National Heart, Lung, and Blood Institute https://www.nhlbi.nih.gov/health/sickle-cell-disease.

[3] Tanabe P, Spratling R, Smith D, Grissom P, Hulihan M. CE. (2019), Understanding the complications of sickle cell disease. Am J Nurs. 119(6):26-35. doi: 10.1097/01.NAJ.0000559779.40570.2c.

[4] Nationwide Children https://www.nationwidechildrens.org/family-resources-education/family-resources-library/early-diagnosis-key-to-dealing-with-sickle-cell-disease#:~:text=State%20laws%20require%20that%20babies,devastating%20complications%20of%20the%20disease.

[5] Dexter, D, McGann, PT (2022), saving lives through early diagnosis: the promise and role of point of care testing for sickle cell disease. Br J Haematol, 196: 63-69. https://doi.org/10.1111/bjh.17678.

[6] Bushra SN, Shobana, G (20121), Paediatric sickle cell detection using deep learning: A Review. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, pp. 177-183, doi: 10.1109/ICAIS50930.2021.9395756.

[7] Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal, 5(3), 528-543. https://doi.org/10.51594/csitrj.v5i3.859.

[8] Riccardo Miotto, Fei Wang, Shuang Wang, Xiaoqian Jiang, Joel T Dudley (2018), Deep learning for healthcare: review, opportunities and challenges, Briefings in Bioinformatics, 19(6): 1236–1246, https://doi.org/10.1093/bib/bbx044.

[9] Priyanka, Singh, A.K (2023), A survey of image encryption for healthcare applications. Evol. Intel.16, 801–818. https://doi.org/10.1007/s12065-021-00683-x.

[10] Kawuma Simon, Mabirizi Vicent, Kyarisiima Addah, David Bamutura, Barnabas Atwiine, Deborah Nanjebe, Adolf Oyesigye Mukama, (2023), Comparison of deep learning techniques in detection of sickle cell disease. Artificial Intelligence and Applications,

[11] Neelankit Gautam Goswami, Anushree Goswami, Niranjana Sampathila, Muralidhar G. Bairy, Krishnaraj Chadaga, Sushma Belurkar. (2024), Detection of sickle cell disease using deep neural networks and explainable artificial intelligence. Journal of Intelligent Systems,

[12] G.M.K.B. Karunasena, H.M.K.K.M.B. Herath, H.D.N.S. Priyankara, B.G.D.A. Madusanka, (2023), Sickle cell disease identification by using region with convolutional neural networks (R-CNN) and digital image processing, Sri Lankan Journal of Applied Sciences,

[13] Abdourahmane Balde, Avewe Bassene, Lamine Faty, Mamadou Soumboundou, Ousmane Sall, Youssou Faye, (2023), Recent artificial intelligence advances in detection and diagnosis of sickle cell disease: A review, 2023 IEEE International Conference on Big Data (BigData).

[14] L. Chen et al., MASS: A multi-attribute sketch secure data sharing scheme for IoT wearable medical devices based on blockchain, IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3468733.

[15] Amaithi Rajan, A., V, V., Raikwar, M. et al. (2024) SMedIR: secure medical image retrieval framework with ConvNeXt-based indexing and searchable encryption in the cloud. J Cloud Comp 13, 139. https://doi.org/10.1186/s13677-024-00702-z.

[16] Al-Badawi A, Faizal Bin Yusof M, (2024), Private pathological assessment via machine learning and homomorphic encryption. BioData Mining 17, 33 . https://doi.org/10.1186/s13040-024-00379-9.

[17] Lata K, Singh, P, Saini, S, Cenkeramaddi, LR, Deep learning-based brain tumor detection in privacy-preserving smart health care systems. IEEE Access, doi: 10.1109/ACCESS.2024.3456599.

[18] Wu R, Wang B, Zhao Z (2024), Privacy-preserving medical diagnosis system with Gaussian kernel-based support vector machine. Peer-to-Peer Netw. Appl.. https://doi.org/10.1007/s12083-024-01743-6.

[19] Petrenko, Anatolii/Boloban, Oleh (2023), Generalized information with examples on the possibility of using a service-oriented approach and artificial intelligence technologies in the industry of e-Health. Technology Audit and Production Reserves 4 (2/72), S. 10 - 17. https://journals.uran.ua/tarp/article/download/285935/280167/660189. doi:10.15587/2706-5448.2023.285935.

[20] Ilie L, Pop E, Caramihai SI, Moisescu MA, (2022), A SOA-based e-health services framework. E-Health and Bioengineering Conference (EHB), Iasi, Romania, 2022, pp. 1-4, doi: 10.1109/EHB55594.2022.9991608.

[21] Petrenko A, Tsymbaliuk R, (2024), A cloud-based platform ("Clinic in Cloud") as a significantly expanding the current capabilities of the Ukraine e-health system. EC Clinical and Medical Case Reports 7.9: 01-10.

[22] Arfan, TH, Hayaty M, Hadinegoro A (2021), Classification of brain tumours types based on MRI images using Mobilenet. 2nd International Conference on Innovative and Creative Information Technology (ICITech), Salatiga, Indonesia, 2021, pp. 69-73, doi: 10.1109/ICITech50181.2021.9590183.

[23] Ahmadi, Mahdie, Nader Karimi, and Shadrokh Samavi. "A lightweight deep learning pipeline with DRDA-Net and MobileNet for breast cancer classification." arXiv preprint arXiv:2403.11135 (2024).

[24] H. Atyam, S. C. Bachu, S. S. Kyatham and H. Satish, "Screening of Cardiomegaly using Ensemble Model of InceptionV3 and MobileNet," 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2024, pp. 1426-1431, doi: 10.1109/ICCSP60870.2024.10543609.

[25] Sarthak Joshi, Rachit Shah, Yashvi Chandola, Vivek Uniyal. "Classification of Brain MRI Images using End-to-End Trained AlexNet & End-to-End Pre-Trained MobileNet " International Journal of Research Publication and Reviews, Vol 5, no 7, pp 205-218 July 2024.

[26] Pendam T, Baig MM, Sonekar S, Sawwashere SS (2024), Enhancing security and privacy in cloud-based medical data systems using AES cryptography and digital envelopes. IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, pp. 1-8, doi: 10.1109/SCEECS61402.2024.10482070.

[27] Bowen Meng, Xiaochen Yuan, Qiyuan Zhang, Chan-Tong Lam, Guoheng Huang, (2024), Encryption-then-embedding-based hybrid data hiding scheme for medical images. Journal of King Saud University - Computer and Information Sciences, 36(1), 101932, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2024.101932.

[28] Giao J, Nazarenko AA, Luis-Ferreira F, Gonçalves D, Sarraipa JA (2022), Framework for service-oriented architecture (SOA)-based IoT application development. Processes 2022, 10, 1782. https://doi.org/10.3390/pr10091782.

[29] Aravind Kumar Kalusivalingam, (2020), Advanced encryption standards for genomic data: evaluating the effectiveness of AES and RSA, AJST 3(1).

[30] Vasilescu E, Mun, SK (2006), Service Oriented Architecture (SOA) implications for large scale distributed health care enterprises. 1st Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare, 2006. D2H2., Arlington, VA, USA, 2006, pp. 91-94, doi: 10.1109/DDHH.2006.1624805.

[31] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Ahmad Khan R (2020). Healthcare Data Breaches: Insights and Implications. Healthcare 8, 133. https://doi.org/10.3390/healthcare8020133

[32] Hafsa A, Malek J, Machhout M (2021), Performance trade-offs of hybrid cryptosystem for medical images encryption – decryption. 18th International Multi-Conference on Systems, Signals & Devices (SSD), Monastir, Tunisia, pp. 1221-1229, doi: 10.1109/SSD52085.2021.9429477.

[33] Bhavitha M, Rakshitha K, Rajagopal SM (2024), Performance evaluation of AES, DES, RSA, and Paillier Homomorphic for image security. 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-5, doi: 10.1109/I2CT61223.2024.10544282.