**CONCLUSION**

In this paper, we presented a proxy-invisible condition-hiding proxy re-encryption scheme which supports keyword search that can be applied to securing data sharing and delegation in e-healthcare systems. With our new system, a doctor, Alice (delegator), may construct a conditional authorization for a doctor, Bob (delegatee), by specifying a re-encryption key. With the re-encryption key, the cloud server can perform ciphertext transformation so that Bob is able to access the PHRs original encrypted under Alice's public key, thus enabling secure delegation. The cloud server can operate search over encrypted PHRs on behalf of the doctor without learning information about the keyword or the underlying condition. Specifically, we achieved the property of proxy-invisible in the system. We have also obtained the property of collusion-resistance in the system, where a delegator's (Alice) private key is still secure even a dishonest cloud server colludes with the delegatee (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.

Future Work:

Here are some possible future work directions:

* Scalability: The current implementation of the DSAS system is suitable for small-scale deployments. Future work can focus on improving the scalability of the system to support large-scale e-healthcare systems with a high volume of patients and medical records.
* Privacy Preservation: Although the DSAS system provides a high degree of privacy and security, there is still room for improvement. Future research can focus on developing more advanced privacy-preserving techniques to ensure that patient's personal healthcare records are protected even in the case of a breach or attack.
* Usability: While the DSAS system is efficient and practical, its usability can be improved. Future work can focus on developing a user-friendly interface for doctors and patients to access and manage the PHRs, making it easier to use and reducing the risk of human error.
* Interoperability: E-healthcare systems may involve multiple institutions and organizations, which may use different software and hardware. Future work can focus on ensuring interoperability between different e-healthcare systems and enabling seamless sharing of encrypted PHRs between different providers.
* Integration with Emerging Technologies: The DSAS system can be integrated with emerging technologies such as blockchain, AI, and IoT to enhance its functionality and security. For instance, blockchain can be used to create a decentralized, tamper-proof database for storing PHRs, while AI can be used for predictive analytics and personalized medicine.
* Adoption and Implementation: Finally, future work can focus on encouraging the adoption and implementation of the DSAS system in real-world e-healthcare systems. This can involve collaboration with healthcare providers, policymakers, and regulatory bodies to ensure that the system meets legal and ethical requirements and is compatible with existing healthcare systems.