SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Volume: 5 | Issue: 12 | December 2020 - Peer Reviewed Journal

ORGAN-IZE: A PROXY RE-ENCRYPTION BASED ORGAN DONATION SYSTEM

Poojan Patel

Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune-412115, India

Kalyani Kadam

Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune-412115, India

Rahul Joshi

Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune-412115, India

ABSTRACT

Building an organ donation system that satisfies the privacy, confidentiality, and security requirements of healthcare records and private data of donors have always been a challenge in the digital world. Cryptographic technology is an exciting technological advancement in information technology. NuCypher's Proxy Re-Encryption (PRE) Scheme is a distributed and decentralized cryptologic network providing intuitive, accessible, and extensible interfaces as well as runtime for private data management as well as access control dynamically. This paper outlines the Umbral Proxy Re-Encryption scheme, as used by NuCypher KMS. Umbral is a threshold proxy re-encryption scheme following a Key Encapsulation Mechanism (KEM) approach. This paper aims to evaluate the application of NuCypher's Proxy Re-Encryption Scheme to implement the privacy, security, and confidentiality aspects of organ donation systems. The paper elucidates the requirement of securing the healthcare records and private data security and confidentiality in organ donation and identifies the legal and technological limitations of existing healthcare systems and how proposed solutions help to overcome such limitations. The paper also focuses on evaluating the current healthcare system working and its limitations regarding the security and confidentiality of healthcare records with some facts and understanding. The paper briefly emphasis on securing the organ donor's medical records using data encryption until his/her demise and then delegate access to concerned authorities using NuCypher's PRE (Proxy Re-Encryption) network.

KEYWORDS: *Digitization, Privacy, Security, Confidentiality, Proxy Re-Encryption, Cryptography, Data Encryption, Public-key Cryptography, etc.*

I. INTRODUCTION

Healthcare organizations are designing future ways towards accepting complete digitization within the enterprise. Digitization throughout the care trade has helped suppliers of healthcare services to make a sturdy as well as important foundation by specializing in the patient's or customer's desires. The future of digitalization in health-care appears encouraging because the patients tend to be softer in victimization services that are digital for advanced and delicate problems equivalent to health-care as well as drugs. It's a transparent manifestation for payers as well as suppliers to accept the future of digitization in health-care by accepting yet another digital wave.

The non-medical organizations are going to have with success adopted entirely digitalization by providing products that are digital and are also processed through and up to date channels as well as gaining their effectiveness and potency by investment in advanced analytics. Digitization within tending business has reworked means of the patients and suppliers perform as well as commune to each other; as a result of that, creating treatment services available to everybody through guaranteeing broad accessibility.

A. Digitalization in Health-care Industry

Digitization which is authorized by Health Information Technology (HIT) has completely changed the perception of individuals towards health-care, modified the approach of end users, as well as the subject of medical and health services. Adopting digitalization, within the aid trade has remodeled the link between doctors and patients, authorizing folks to participate in the activity of family as well as personal health management. From the aid service supplier's attitude, to form price, it's important to understand what the patient wants and therefore the encompassing myths about them, as well as apprehending the market landscape. Aid or Medical organizations will support intelligent market solutions like client analytics as well as massive information analytics to spot patient's wants. What is more, aid organizations should determine their client division as well as position the services accordingly in order to fulfill the calculable patient wants as well as commands. In order to adopt success in health-care, the only way is to achieve unjust insights and as a result of that, other services are added in order to keep attention of patients as well as drive price

II. CURRENT SCENARIO OF ORGAN DONATION IN HEALTHCARE INDUSTRY

In the current scenario of organ donation in the healthcare industry, especially in countries like-India, they are moving towards digitalization and the donor's health records collected electronically but the current system is not very efficient and well secured. The electronic patient records are depending on any centralized third party including the government and there is no way to track how data is used and by whom and for what purpose. The data is also not encrypted and due to that anyone can hack the system and get access to health records. There is also no proper space for consent for the usage of any particular data for any particular purpose in our current organ donation system. Security and confidentiality are mainly those points that are missing in the current system and which can affect the donor and also health organization in a very serious way. Hackers can do data breaches that can affect the donor private data confidentiality and loss of a huge amount of money.

Privacy, security, and confidentiality all are basic rights of every patient and these things give security to patients and help them to trust the healthcare system. One can easily lose trust if its privacy regarding their private data is sacrificed. On the other hand, health organizations are also affected by the loss of billions of data due to security issues of their system. By improving the security and taking care of personal data of every patient which is the right of every patient and at the same time consent of every patient regarding the sharing of their medical data is also an important part. It basically helps to take care of the rights of patients regarding their data. There are national frameworks made regarding the privacy and security of patient health records.

On the other hand, organ trafficking is one of the lesser discussed forms of human trafficking. Be that as it may, organ trafficking holds a basic spot with sorted out wrongdoing bunches because of popularity and moderately low paces of law authorization. Global Financial Integrity (GFI) accepts that almost 10 percent of the total organ transplants counting liver, heart, and lungs, is done by means of the assistance of organ trafficking. In any case, the most prominent organs which are exchanged illegally are kidneys, with the well known World Health Organization (WHO) assessing that about 10,000 kidneys are exchanged on the bootleg market overall yearly, or nearly more than 1 kidney consistently.

Looking into the background of the healthcare industry regarding the security and privacy issue, the main flaw in today's digital era is the security of data. The data is a new form of generating money and the hackers are always ready for that. There are many breaches done in the past which show losses of billions of dollars. Especially In a country like India where the digitalization is started and rapidly growing the security of personal data becoming a major problem and the patients even not aware about their rights on their healthcare data and companies also taking advantage of this kind of illiteracy and sell their personal data without their consent and hackers easily can give a big jolt to the Indian healthcare industry due to privacy and security issues. That's why it is important to make the healthcare system more secure and take care of the privacy of patient records.

The main aspects of an organ donation system should be to ensure:

- The *integrity of donor medical records* so data is exact, right, and reliable - the uprightness of data is basic to quality patient consideration, evaluation of administrations, research, and general wellbeing.
- The *accessibility of medical records to authorized people* who need the data for real medical purposes has prepared an approach to the information - if the medical data isn't promptly accessible to social insurance suppliers, the eventual benefits of patients might be essentially undermined.
- The *privacy of medical records* so donors and patients can be guaranteed that individual private data is only disclosed to authorized persons for authorized purposes at authorized times - recognizable information can be discharged distinctly with the educated assent regarding the patient or consumer.

III. ORGAN-ize's PROPOSED SOLUTION

A. Elevator Pitch

"To secure the organ donor's medical records using data encryption until his/her demise and then delegate access to concerned authorities using NuCypher's PRE (Proxy Re-Encryption) network."

B. General Overview

As discussed, the existing system of organ donation and its security and privacy issues have major flaws and are not a donor friendly system. It means it is not trustworthy to any donor because of the issue of privacy and confidentiality of their private data. The protection of patients and furthermore the security and privacy of their data is the most basic boundary to enter, once taking into consideration the selection of EHR(Electronic Health Records) inside the medical industry. The requirement of privacy of medical records of the patient can affect and play a crucial role in systems like organ donation. The delicate nature of the medical data contained inside the EHR while organ donation has incited the requirement for an increasingly secure framework which can help patients not to stress over their clinical records.

After understanding deeply the faults in the system, I build a prototype to secure organ donor's medical records using data encryption until his/her demise and then delegate access to concerned authorities using NuCypher's PRE (Proxy Re-Encryption) network and Shamir's Secret Sharing Scheme. Our proposed system is highly secured and clears the fault of privacy, consent, confidentiality issues of the current system. This system helps to keep medical records of patients secured with the help of proxy re-encryption.

This application helps organ donors to safely and anonymously store their medical records using data encryption technique, on a decentralized platform like IPFS until their demise and then delegate access of their private medical data, to their trustee/s as well as to the concerned authorities like Hospitals, which may perform organ transplant after certain verifications and with the use of public-key cryptography we are ensuring our donor's identity to completely safe. The project aims to build an organ donation system based on blockchain which helps to stop organ trafficking and also helps to keep medical records of patients secured with the help of proxy re-encryption.

C. Basic Scenario

Let's say, Alice wants to donate her organs after her demise. She collects all the necessary documents like Identity Proofs, Medical check-ups, Official Organ Donation documents, etc and encrypts the data using her private key P(A), and then encrypted data will be uploaded on IPFS storage. Using NuCypher's Policy Protocol, Alice will be able to write a policy statement granting access to all the medical data related to organ donation to a Medical Institution. Alice's Identity will always remain anonymous in the network.

Using Shamir's Secret Sharing Scheme, Alice will divide her private key P(A) into 2 sub-keys P(A1) and P(A2) and hand it over to her trustees, Bob and Carol. So that after Alice's death, Bob and Carol together can take charge of the medical documents and grant access for Alice's data to a Medical Institution so that all the procedures of organ transplant can be executed on time (before the body starts decomposing). And also Bob and Carol cannot individually access/tamper Alice's data using sub-keys. So Secret Sharing solves the problem of data tampering after Alice's death.Using Shamir's Secret Sharing Scheme, Alice will divide her private key P(A) into 2 sub-keys P(A1) and P(A2) and hand it over to her trustees, Bob and Carol. So that after Alice's death, Bob and Carol together can take charge of the medical documents and grant access for Alice's data to a Medical Institution so that all the procedures of organ transplant can be executed on time (before the body starts decomposing). And also Bob and Carol cannot individually access/tamper Alice's data using sub-keys. So Secret Sharing solves the problem of data tampering after Alice's death. The application focuses mainly on 4 major qualities:

- The anonymity of the organ donor should be maintained in the network.

- Privacy and Security of an organ donor's medical records.
- Confidentiality of an organ donor's private medical data.
- Keeping a track of unethical practices(organ trafficking) in the network.

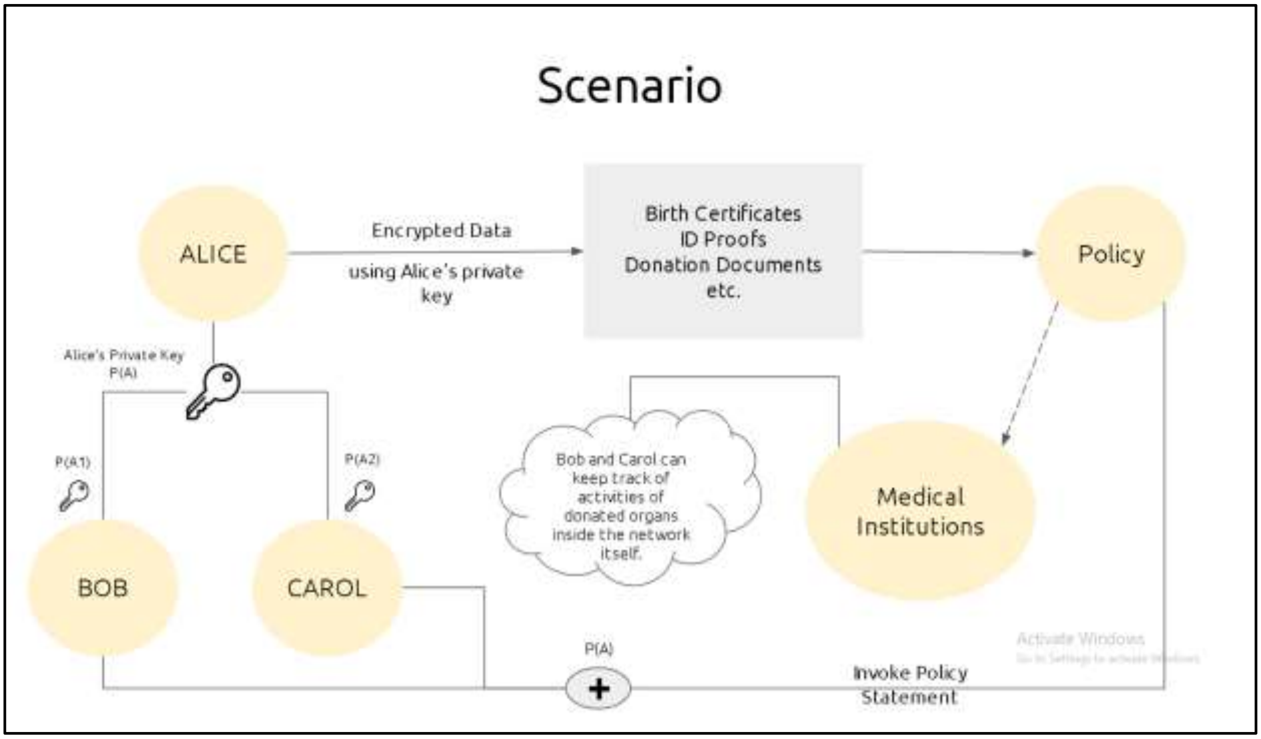

Figure 1: Basic structure explaining the complete scenario of the application

IV. NuCypher - A PROXY RE-ENCRYPTION NETWORK

"A decentralized cryptologic network offering accessible, intuitive, and extensible runtimes and interfaces for secrets management and dynamic access control."

A. Overview of PRE

NuCypher's Proxy re-encryption (PRE) Scheme is an alternate sort of public-key encryption (PKE) that permits an intermediary to change over ciphertexts starting with one public key then onto the next public key, without the intermediary(proxy) can learn or know any data about the first secret message; to do as such, the intermediary(proxy) ought to be in control of a re-encryption key that permits the underlying procedure. In this manner, it holds a spot for appointing unscrambling rights, opening up a lot increasingly potential applications that need to delegate permission to existing cypher text(encrypted data). [See Figure 2].

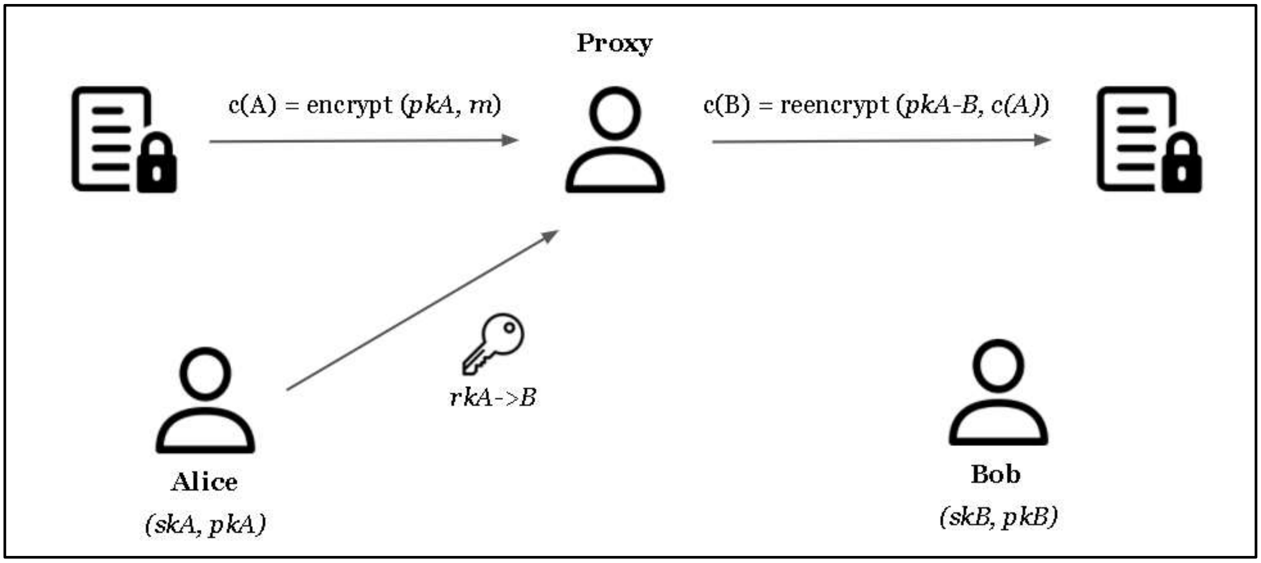

Figure 2: NuCypher Overview

B. Working of NuCypher Network

Umbral is nothing but NuCypher's threshold proxy re-encryption (PRE) scheme. Alice (the private data owner) can envoy decryption rights to Bob (the recipient/ the receiver) for any ciphertext intended for her, through a particular re-encryption process done by a set of semi trusted-minimized proxies. When a threshold of these semi-trusted proxies engage by performing re-encryption, Bob(the recipient/the receiver) could combine these independent re-encryptions and decrypt the original secret message sent by Alice, using his private key. [See Figure 3.]

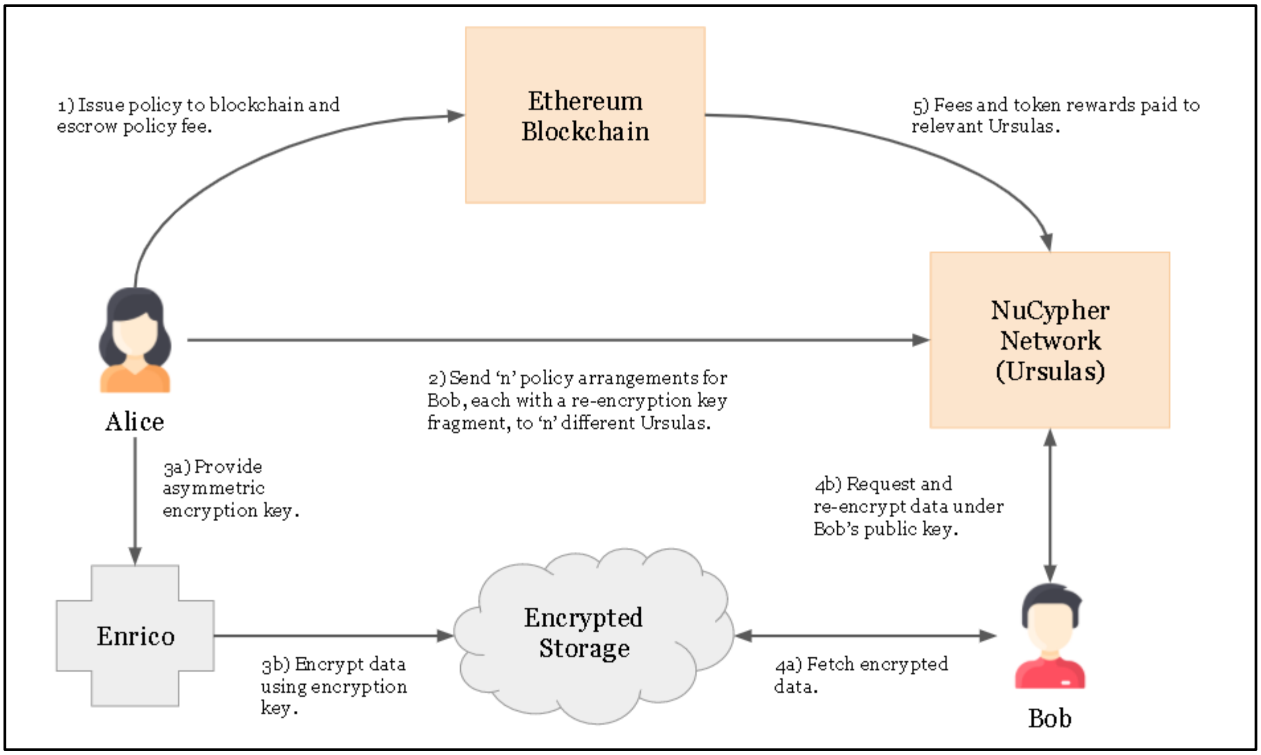
Ethereum Blockchain
1) Issue policy to blockchain and escrow policy fee.
5) Fees and token rewards paid to relevant Ursulas.
NuCypher Network (Ursulas)
Alice
2) Send 'n' policy arrangements for Bob, each with a re-encryption key fragment, to 'n' different Ursulas.
3a) Provide asymmetric encryption key.
4b) Request and re-encrypt data under Bob's public key.
Enrico
Encrypted Storage
3b) Encrypt data using encryption key.
4a) Fetch encrypted data.
Bob

Figure 3: Flow diagram of NuCypher Network

C. Features of NuCypher Network

NuCypher's Proxy Re-Encryption (PRE) Scheme is a distributed and decentralized cryptologic network providing intuitive, accessible, and extensible interfaces as well as runtime for private data management as well as access control dynamically.

- *Accessible* - The NuCypher Scheme works with no authorization and is restriction safe. There are no screens and completely nobody can utilize it.
- *Intuitive* - The NuCypher Scheme supports the classical cryptological account of Alice(the private data owner) and Bob(the recipient/ the receiver). This pervades the code-base and assists code engineers compose securely, abuse-safe code.
- *Extensible* - Presently, the system permits intermediary(proxy) re-encryption (PRE) however could be reached out to help support for some other well known cryptographic natives.

Access authorizations are transformed into the basic encryption, and access can exclusively be explicitly conceded by the secret owner itself by means of sharing policy. Subsequently, the secret owner has complete authority over their information. At no intention is the information decrypted nor will the secret keys be dictated by the NuCypher Scheme itself.

V. FUTURE SCOPE

The upcoming stage of our guide is to make a consortium of on-screen characters inspired by the arrangement portrayed here and to have pilot focuses to send the system and implement it at national or global scale. The main limitation of existing organ donation systems is privacy, lack of security, and confidentiality, and in the future to overcome such limitations cryptographic technologies like NuCypher's Proxy Re-Encryption Scheme, and also some other blockchain technologies, etc. will be an effective tool to deal with it. Our proposed solution is an example of how to overcome issues of security and privacy and how to bring transparency in the system. Currently, I am working on a prototype of the Organ-ize application, which will include Hyperledger Fabric Blockchain - A private and Permissioned Blockchain, along with NuCypher Network.

VI. CONCLUSION

The stakeholders of the health-care industry are operational within the technological period. Insurance suppliers place confidence in superannuated medical knowledge, clinics communicate inefficiently, and successively, patients receive inadequate service. As different industries adopt technologies to form practices a lot of economical care has been forgotten and effectively left within the mud. Medical records are one of the most important data of any person because it includes every private detail about that person and no one wants to share their private data with others without their consent and every patient wants a surety and reliability of healthcare organizations to keep their data secure. Security and Privacy are moral requirements of every patient. Organ-ize provides a straightforward, however effective cryptographic (Proxy Re-Encryption Scheme) based solution to mitigate the drawbacks of this broken system and build a care setting that supports patient-centered knowledge integrity and security. By utilizing the technology bestowed by Organ-ize, we will give higher record management for patients, quicker emergency response times, and improved security of sensitive medical data.

REFERENCES

1. *"Public Attitudes and Behavior Regarding Organ Donation"* - *https://jamanetwork.com/journals/jama/article-abstract/398795*
2. *"Knowledge regarding organ donation: Identifying and overcoming barriers to organ donation"* - *https://www.sciencedirect.com/science/article/abs/pii/027795369090174Q*
3. *"First prospective study on brain stem death and attitudes toward organ donation in India"* - *https://aasldpubs.onlinelibrary.wiley.com/doi/full/10.1002/lt.21912*
4. *"Current Status of Transplant Coordination and Organ Donation in India"* - *http://14.139.245.149:8080/jspui/bitstream/1/8263/1/Current%20status%20of%20transplant%20coordination.pdf*
5. *"Knowledge, attitude and behaviour of the general population towards organ donation: An Indian perspective"* - *http://www.nmji.in/article.asp?issn=0970-258X;year=2016;volume=29;issue=5;spage=257;epage=261;aulast=Vijayalakshmi*
6. *"Decentralised and Distributed System for Organ/Tissue Donation and Transplantation"* - *https://ieeexplore.ieee.org/abstract/document/9066225*
7. *"Using Blockchain Technology for The Organ Procurement and Transplant Network"* - *https://scholarworks.sjsu.edu/etdtheses/5065*
8. *"SECURE ORGAN TRANSPLANT INFORMATION SYSTEM"* - *http://casopisi.junis.ni.ac.rs/index.php/FUAutContRob/article/view/2554*
9. *"NuCypher KMS: Decentralized key management system"* - *https://arxiv.org/abs/1707.06140*

10. *"NuCypher: A proxy re-encryption network to empower privacy in decentralized systems" - https://static2.coinpaprika.com/storage/cdn/whitepapers/448411.pdf*
11. *"Cryptography for Pragmatic Distributed Trust and the Role of Blockchain" - https://hal.archives-ouvertes.fr/tel-01966109/document*
12. *"The Future of Healthcare: The Impact of Digitalization on Healthcare Services Performance" - https://link.springer.com/chapter/10.1007/978-3-319-99289-122*
13. *"The Future Impact of Healthcare Services Digitalization on Health Workforce: The Increasing Role of Medical Informatics." - \url{https://europepmc.org/article/med/27577470" The Future Impact of Healthcare Services Digitalization on Health Workforce: The Increasing Role of Medical Informatics." - https://europepmc.org/article/med/27577470*