DOCTOPRO –A Secure Authenticator Key System
MASTER OF COMPUTER APPLICATION

Presented By:
Student name : OM GUPTA
Roll No : 10071022048
Registration No : 221000512114

DOCTOPRO

Guided By:

Mr. Sanchayan Bhaumik

MAULANA ABUL KALAM AZAD
UNIVERSITY OF TECHNOLOGY,
WEST BENGAL
Utech

Department of Computer Application.
Maulana Abul Kalam Azad University Technology, West Bengal, India

Motivation

In the rapidly evolving landscape of healthcare, the adoption of a secure web-based authentication system for medical data is a game-changer. This technological advancement offers healthcare providers a flexible and efficient means of accessing and managing patient information while maintaining the highest standards of security. With this system in place, healthcare professionals can securely log in from anywhere with internet access, ensuring timely and accurate patient care. Leveraging state-of-the-art encryption, user verification methods, and stringent access controls, this web-based authentication system fortifies the confidentiality and integrity of sensitive medical data. It empowers healthcare institutions to streamline their operations, enhance collaboration, and embrace the digital transformation, all while upholding the trust and security of the healthcare ecosystem

In the ever-evolving realm of healthcare, the adoption of a robust and secure web-based authentication system for medical data stands as a pivotal advancement. This innovative technology promises to revolutionize the way healthcare providers interact with patient information, ensuring both accessibility and top-tier security. The intrinsic motivation behind the implementation of such a system is rooted in several key factors:

1. **Accessibility and Flexibility**: With this web-based authentication system, healthcare professionals gain unprecedented access to critical patient data. Regardless of their physical location, as long as they have an internet connection, they can securely log in. This level of accessibility ensures that no matter the circumstances, patients can receive timely and accurate care, even in emergency situations.

2. **Data Security**: The cornerstone of this authentication system is its unwavering commitment to data security. By deploying state-of-the-art encryption techniques, stringent user verification methods, and meticulous access controls, the system erects an impenetrable fortress around sensitive medical data. The result is a healthcare landscape where patient confidentiality and data integrity are non-negotiable.

3. **Trust and Integrity**: Maintaining trust and integrity within the healthcare sector is not negotiable. Patients and their families must have complete confidence in the security of their medical data. The implementation of this secure web-based authentication system serves to reinforce that trust. It sends a clear message that healthcare providers are committed to safeguarding patient information, no matter where it is accessed or shared.

4. **Necessity for the Future**: As the healthcare industry continues to evolve, the need for a secure web-based authentication system becomes increasingly critical. The interconnected nature of modern healthcare demands a digital infrastructure that is not just convenient but a necessity for patient safety and quality care delivery.

Why we need this System ?

The motivation behind the adoption of a secure web-based authentication system for medical data extends far beyond mere convenience. It embodies a commitment to patient care, data security, operational efficiency, collaboration, trust, and the future of healthcare. It represents a pivotal step forward in ensuring the highest standards of care while preserving the sanctity of sensitive medical information.

Literature Review

Journal Name:-Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics

Publication:- 2019

Moral/Gist Of The Journal

This article delves into the integration of modern technology within the field of medical science, with a specific focus on Telecare Medicine Information Systems (TMIS). In this context, the protection of patient-related information is of paramount importance. The article explores the introduction of authentication protocols designed to enhance the security of patient data within TMIS.
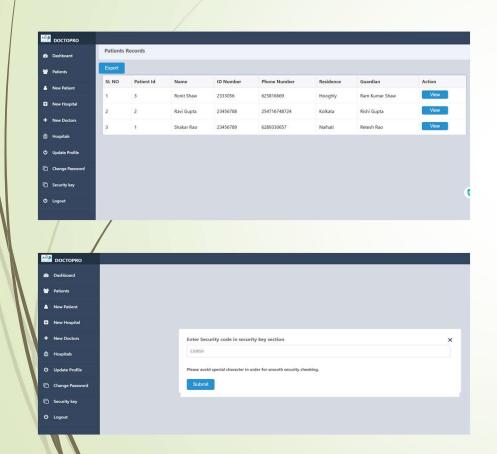
Proposed Method

Certainly, elaborate on the use of Public Key Infrastructure (PKI) in a secure authenticator key system, particularly in the context of managing digital profile credential to ensure secure communication and data protection.
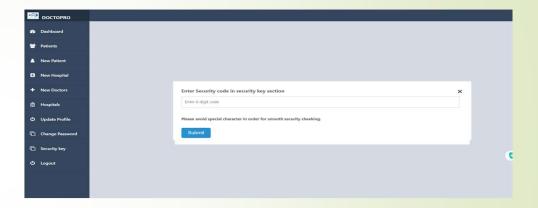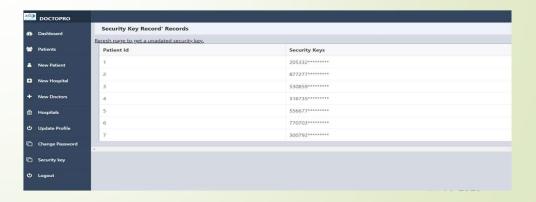
Encryption Keys:

PKI also manages encryption keys used for secure communication. The primary types of keys involved are:
- **Public Key**: As mentioned earlier, the public key is included in the digital certificate and can be used for encrypting data that only the certificate holder can decrypt using their private key.

- **Private Key**: The private key is kept confidential and is never shared. It is used for decrypting data that has been encrypted with the corresponding public key. In the context of secure communication, this private key is essential for decoding incoming encrypted data.

In summary, Public Key Infrastructure (PKI) forms the backbone of secure communication and data protection in the context of an authenticator key system. It accomplishes this by managing digital certificates and encryption keys, which provide identity verification, confidentiality, data integrity, and strong security against various threats.
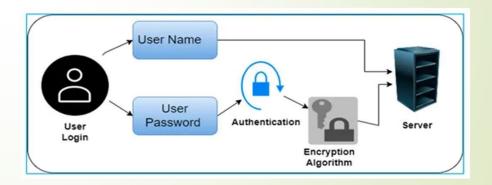
Interface View

LOGIN INTERFACE

Secure Md5 Encryption at login

MD5 (Message Digest Algorithm 5) is a cryptographic hash function that was widely used in the past but is now considered insecure for most security applications due to several vulnerabilities. MD5 generates a fixed-length, 128-bit hash value from input data of arbitrary length.
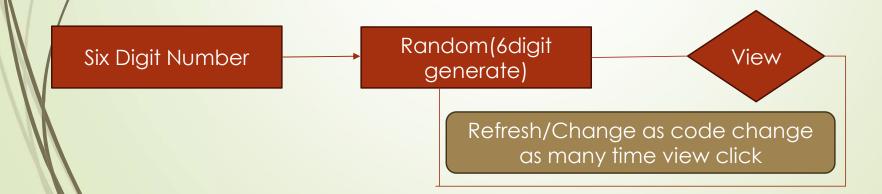

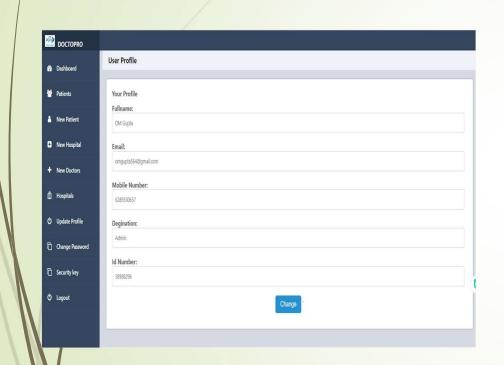17-10-2023

Generation of secure Code For Patient Cheek

Generating a secure code for patient check using a random function is a common requirement in healthcare and other fields. To create a secure code, you can use a combination of cryptographic principles and randomization. Below is a step-by-step algorithm to generate a secure patient check code:

1. Choose a character set: Decide on the character set you want to use for the code. Typically, this includes uppercase letters, lowercase letters, and digits. You can also include special characters for added security.

2. Determine the code length: Define the desired length of the patient check code. Longer codes are generally more secure.

3. Generate a cryptographically secure random code:

    1. Use a cryptographic library or a secure random number generator, depending on your programming language.

    2. Generate random characters from the chosen character set.

    3. Ensure that characters are selected with uniform randomness.

Six Digit Number → Random(6digit generate) → View

Refresh/Change as code change as many time view click

17-10-2023

Admin Interface

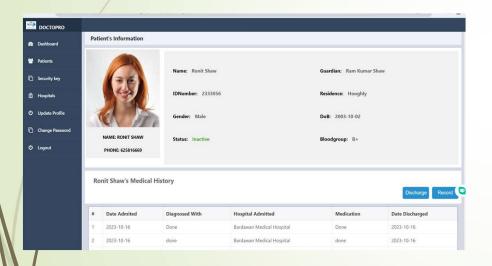# Doctor Interface

Function Of Doctor and Responsibility:-

1. To view a patient by secure key method to view the medical history.
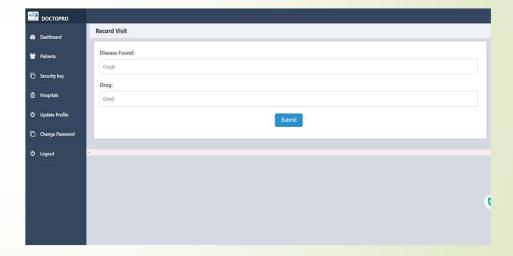
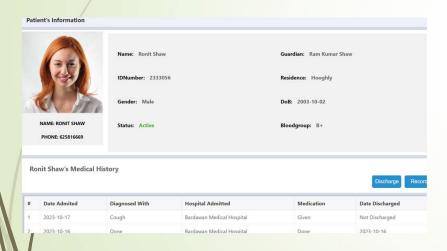2. To Records the symptoms(active) and discharge it automatically

Experimental Results

Admin Result View

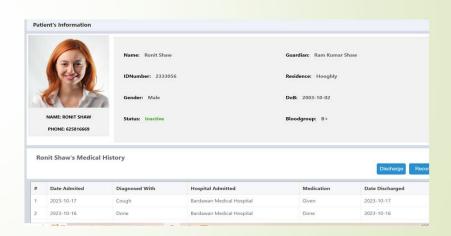**After Update Academic Record is active**

After Discharge it is inactive

Output Of Experiments

The experiment will give a clarity that both admin and doctor can view the patients medical history, record, detail and change the active status ,update medicine and feedback by the mean of a random security key that seems to change at the time of the view patients bar will be click and security code for the respective patients id's is update need to refresh the security key option by random function .

Reset password page

A "Reset Password" page is important for several reasons, as it serves critical functions in ensuring the security and usability of online accounts and systems:

1. **Security:**

   1. **Password Updates:** Passwords can become compromised or leaked over time due to data breaches or other security incidents. Allowing users to change their passwords enables them to react quickly to protect their accounts.

   2. **Prevent Unauthorized Access:** Regular password changes can help prevent unauthorized access to accounts, especially when users suspect that someone else may have learned their password.

2. **User Control:** Giving users the ability to change their passwords empowers them to take control of their own account security. This is especially important for maintaining trust and providing a sense of ownership over their accounts.

RESET PASSWORD

omgupta564@gmail.com

Reset

Change Password

Change Your Password

Email:
omgupta564@gmail.com

Current Password:
....

New Password:
...

Confirm Password:
...

Change

Summarize

Regarding Reset Password link Inbox ×

omgupta564@gmail.com
to me ▾

Password Updated Successfully.

Reply   Forward   Reply with AI

17-10-2023