Form 4: Results and Conclusion

1. Team No: 13

2. Project Title: Integrated Electronic Health Records (EHR) Platform: Enhancing Patient-Centric Healthcare Management

3. Experiment Environment:

Visual Studio Code: We used the Visual Studio code to execute our project as a whole. The Visual Studio code's environment was suitable for the React application to run efficiently with the integration of the backend using Python and Flask.

4. a Experiment 1:

We choose 3DES as the encryption algorithm for our experiment. Triple DES (3DES), also known as Triple Data Encryption Algorithm (TDEA), is a symmetric key block cipher designed to enhance the security of the original Data Encryption Standard (DES). In 3DES, the DES algorithm is applied three times consecutively in a process known as Encrypt, Decrypt, Encrypt (EDE). It operates on fixed-size blocks of 64 bits and offers three keying options: 2TDEA (Double DES), which employs two different keys for encryption, decryption, and encryption; and 3TDES(Triple DES), which utilizes three different keys for the three passes. The key size options include 56, 112, or 168 bits, achieved by using three 56-bit DES keys.

Findings:

While 3DES has been widely used for its increased security over the original DES, its usage has diminished with the advent of more modern and efficient symmetric key algorithms, such as AES. Despite its enhanced security, 3DES is relatively slow compared to contemporary encryption algorithms and it has a fixed block size of 64 bits, prompts consideration of newer options for applications requiring robust security measures.

4. b Experiment 2:

The Advanced Encryption Standard (AES) is a widely adopted symmetric key algorithm that operates on fixed-size blocks of 128 bits. It supports key sizes of 128, 192, and 256 bits, with the number of rounds varying accordingly (10 rounds for 128-bit keys, 12 for 192, and 14 for 256). Employing a Substitution-Permutation Network (SPN) structure, AES incorporates key expansion to generate unique round keys and utilizes operations such as byte substitution, shift rows, mix columns, and add round key in each round.

Findings:

The algorithm employs principles of diffusion and confusion for enhanced security, ensuring that changes in one bit of the plaintext have a widespread impact on the ciphertext, and the relationship between the key and ciphertext is intricate. AES is considered highly secure and is extensively used for encrypting data in various applications, including securing internet communications and protecting sensitive information.

5. Parameter comparison table

Parameter	Previous methods	Proposed method
Security	PDFM(Privacy-free Data Fusion and Mining)	AES Algorithm for file encryption
Data Searching Platform	Hybrid ontology but does not have a platform.	We have created a data searching platform and made ease access to data.
Storage	Blockchain but it is expensive and cannot manage multiple databases.	SQLite

6. Final Conclusion Statements

We've developed a platform that ensures both patients and hospitals can securely access medical histories and records. Our top priority is safeguarding data through advanced encryption algorithms, guaranteeing that information remains inaccessible without proper authorization. This means peace of mind for patients and healthcare providers alike, knowing that sensitive information is protected at every step. With our platform, users can confidently navigate their medical journeys, trusting in the security measures put in place to uphold confidentiality and privacy.

Signature Supervisor:
Mr. Madar Bandu