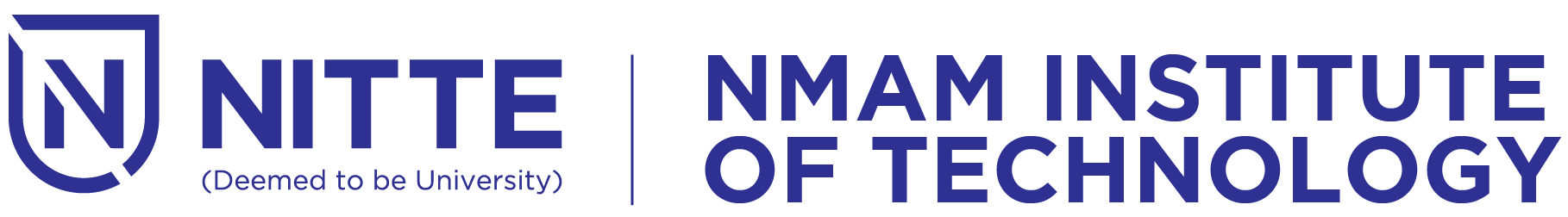
****

**SECURED HOMOMORPHIC AUTHENTICATED ENCRYPTION FOR HEALTHCARE APPLICATIONS**

Submitted By

**SWAPNIL SHARMA 4NM21EC161**

**UDITAPARNA SARMAH 4NM21EC173**

**VINEETH M D 4NM21EC183**

**VIKAS RAI K 4NM22EC421**

**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**

**N.M.A.M. INSTITUTE OF TECHNOLOGY, NITTE - 574110**

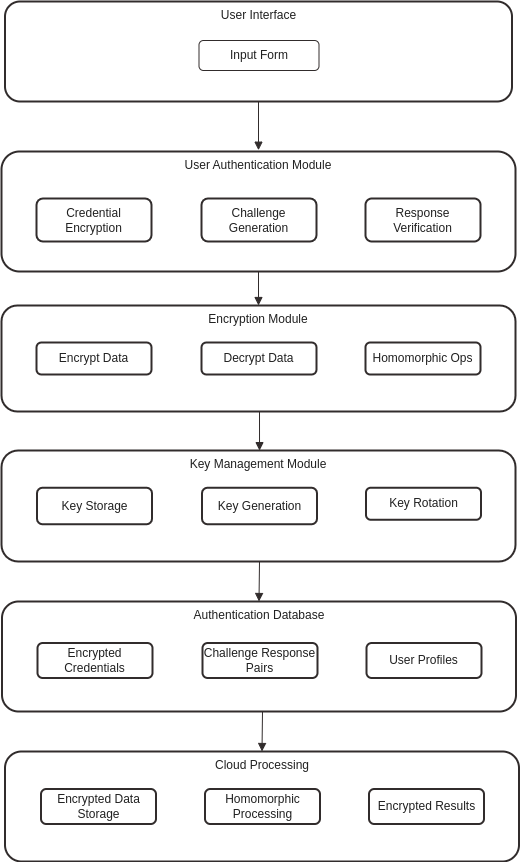
**2023 – 2024**

**INTRODUCTION**

Secure communication and data processing are essential requirements for applications such as healthcare, feedback systems, and voting, where privacy and authenticity are paramount. Traditional cryptographic algorithms necessitate data decryption before processing, which can compromise privacy when third parties are involved. Homomorphic Encryption (HE) offers a solution by allowing encrypted data to be processed without decryption, preserving privacy and enhancing the energy efficiency of networks by avoiding multiple decryption operations. However, ensuring the authenticity of data requesters remains a challenge. This project aims to develop an authentication protocol over a Partial Homomorphic Encryption (PHE) system specifically for healthcare data. By processing patient data in its encrypted form in the cloud and verifying the authenticity of data requesters, the project ensures both the privacy of sensitive information and the authenticity of the data requester, thereby addressing critical security concerns in healthcare applications.

**METHODOLOGY**

Developing a secure authentication protocol over Partial Homomorphic Encryption (PHE) for healthcare data involves several structured phases. Initially, a thorough requirement analysis is conducted to understand the specific needs for secure data communication and processing within healthcare, involving stakeholder meetings and documentation of privacy and authentication requirements. Following this, a comprehensive literature review is performed to study existing HE schemes and their applications, focusing on identifying suitable PHE schemes like Paillier and understanding zero-knowledge proofs. The design phase involves creating detailed architectural diagrams, specifying data flows, and defining encryption and authentication protocols. Implementation includes developing the system's user interface, authentication module, encryption and decryption processes, key management, and integration with the cloud processing system. Rigorous testing and security analysis are conducted to ensure robustness, followed by iterative refinement based on feedback to ensure the system effectively preserves data privacy and ensures the authenticity of data requesters.

**BLOCK DIAGRAM** 

**REFERENCES**

1. Gentry, C. (2009). "A Fully Homomorphic Encryption Scheme." <https://crypto.stanford.edu/craig/craig-thesis.pdf>
2. Paillier, P. (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." <https://link.springer.com/content/pdf/10.1007/3-540-48910-X_16.pdf>
3. <https://link.springer.com/article/10.1007/s40747-022-00756-z>
4. <https://www.researchgate.net/publication/360370944_A_systematic_review_of_homomorphic_encryption_and_its_contributions_in_healthcare_industry>