1. Cryptography

a. A *Identity based cryptography*

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address.

A trusted third party, called the private key generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding **master private key** (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for the identity ID.

iTLS: Lightweight Transport-Layer Security Protocol for IoT With Minimal Latency and Perfect Forward Secrecy

b. *Attribute based encryption :*

Attribute-based encryption is a generalisation of public-key encryption which enables fine grained access control of encrypted data using authorisation policies. The secret key of a user and the ciphertext are dependent upon attributes (e.g. their email address, the country in which they live, or the kind of subscription they have). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext

CP ABE paper

CP ABE tool kit

c. Cloud Security - Access Control
https://www.sciencedirect.com/science/article/pii/S2772918423000036

d. Data Anonymization:
https://link.springer.com/article/10.1007/s40745-024-00557-w

e.Security and Privacy issues in Healthcare
https://dl.acm.org/doi/abs/10.1145/3571156

f Cloud computing - AWS platform security challenges and adding third party security algorithms for securing servers

Involves understanding the AWS architectures, hosting third party security protocols for securing remote server to assist secure healthcare project.

2. Secure Mobile computing

a. Host card emulation (Near field communication) - Android mobile application developtiong with NFC and HCE for smart access and applications.

A. **D. Sethia, D. Gupta, H. Saran,** "Smart HealthRecord Management with Secure NFC-enabled Mobile Devices", Elsevier Journal of Smart Health,Nov 2018, doi: 10.1016/j.smhl.2018.11.001, Peer reviewed since 2017

B. **Divyashikha Sethia, Daya Gupta and Huzur Saran**," NFC Secure Element-based Mutual Authentication and Attestation for IoT access", IEEE Transaction on Consumer Electronics", (vol 64 no 4), 2018 **(*SCI indexed*)** (Cryptography)

b. NFC based secure access
https://ieeexplore.ieee.org/abstract/document/10106459

3. *AI-based estimation for Mental work load with physiological.signals federated learning approach*

a Stress and Anxiety
b. STress and Reels
ci. ASMR emotion recognition
Id Federated LEaring with physiological signals

4. *Smart agriculture soil nutrient prediction using spectral data using machine learning*

A. Shagun, **Divyashikha Sethia**, "A Critical Systematic Review on Spectral-Based Soil Nutrient Prediction using Machine Learning", Springer Environmental Monitoring and Assessment Journal, Impact Factor 2.9., June 2024. (SCIE)

B. Sourav Seal, **Divyashikha Sethia**, "Soil Moisture Prediction Using Deep Learning on Hyperspectral Data", accepted in 2nd Workshop on SMART AGRICULTURE FOR THE ENVIRONMENTAL EMERGENCY (SmartAgr) ACM AI/ML conference Oct 2023

C. Shagun jain, **Divyashikha Sethia**, "A hybrid approach for soil nutrient estimation using multispectral data for Begium and Luxembourg.", Oct 2023, IEEE First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)

5. Early detection of Dementia using AI/ ML and risk factors

Dementia is considered one of the greatest global health and social care challenges in the 21st century. Fortunately, dementia can be delayed or possibly prevented by changes in lifestyle as dictated through known modifiable risk factors. These risk factors include low education, hypertension, obesity, hearing loss, depression, diabetes, physical inactivity, smoking, and social isolation. Other risk factors are nonmodifiable and include aging and genetics. The main goal of this study is to demonstrate how machine learning methods can help predict dementia based on an individual's modifiable risk factors profile.

Work will involve familiarisation on publically available datasets and then close with with neurologist from IHBHAS.

Reference paper is here