| Centrality Based SIoT Trust prediction systems using b-Layered Architectures |
| --- |

The Internet of Things (IoT) envisions a vast network of connected applications, spanning diverse domains and facilitating communication among heterogeneous objects to offer a spectrum of services. This ubiquity of connected devices sets the stage for a transformative paradigm within the IoT landscape known as the Social Internet of Things (SIoT). The integration of social and human activities into the IoT platform introduces novel dimensions, presenting SIoT as a burgeoning field.

In the SIoT framework, the working layer is structured into three distinct layers, each fulfilling unique functions and employing diverse technologies, data processing methodologies, and communication protocols. Artificial Intelligence (AI) plays a pivotal role in this landscape, enhancing the capabilities of SIoT systems to process and analyze data intelligently, leading to more informed decision-making.

The rapid expansion of SIoT is evident in real-time IoT applications, where AI is strategically implemented. Instances include user-intervened scenarios with IP-based phones, cameras, health equipment, televisions, and automobiles. In this project , implementation of SIoT and AI propels the evolution of smart and adaptive systems, fostering a dynamic and interconnected environment.

| Artificial Intelligence theft identification systems for Multi-source and Multi-powered Smart grid applications |
| --- |

Electricity theft is a global problem that negatively affects both utility companies and electricity users. It destabilizes the economic development of utility companies, causes electric hazards and impacts the high cost of energy for users. The development of smart grids plays an important role in electricity theft detection since they generate massive data that includes customer consumption data which, through deep learning techniques, can be utilized to detect electricity theft. This project introduces the theft detection method which uses comprehensive features in time and frequency domains in a deep neural network-based classification approach. We address dataset weaknesses such as missing data and class imbalance problems through data interpolation and synthetic data generation processes. We analyze and compare the contribution of features from both time and frequency domains, run experiments in combined and reduced feature space using principal component analysis and finally incorporate minimum redundancy maximum relevance scheme for validating the most important features. We improve the electricity theft detection performance by optimizing hyperparameters and we employ an adaptive moment estimation optimizer to carry out experiments using different values of key parameters to determine the optimal settings that achieve the best accuracy.

| Design and Development of Vehicular Attacks using Hybrid Deep Learning Architectures |
| --- |

Automotive cybersecurity is facing a critical issue as a result of the increased technological integration seen in contemporary cars and their vulnerability to cyberattacks. In this project, we use a hybrid deep learning architecture to suggest a new method for creating and developing vehicular attack detection systems. Conventional techniques for identifying vehicle cyberattacks frequently depend on rule-based or signature-based detection systems, which may find it difficult to adjust to changing attack tactics and take advantage of undiscovered weaknesses. In order to successfully capture the spatial and temporal patterns characteristic of vehicle attacks, our suggested solution combines the strengths of neural networks.Our hybrid design aims to improve attack detection robustness and accuracy by utilizing the sequential modeling capabilities. Our findings highlight the potential of hybrid deep learning architectures as a promising solution for safeguarding automotive systems against cyber threats, thereby ensuring the safety and security of vehicle occupants and road users.

| Bio-inspired Encryption and Decryption Schemes for the Edge –IoT based Agricultural Devices |
| --- |

Securing data transmission and communication in Internet of Things (IoT) devices deployed in agricultural environments is critical to safeguarding sensitive information and ensuring the integrity of agricultural operations. This project introduces novel bio-inspired encryption and decryption schemes tailored for edge-computing IoT devices utilized in agriculture. Drawing inspiration from biological systems, our approach aims to enhance the security and resilience of data communication channels while minimizing computational overhead and energy consumption.

The primary objective of this project is to develop efficient and robust encryption and decryption schemes that are well-suited for resource-constrained edge devices commonly used in agricultural settings. We explore algorithmic techniques, including symmetric key cryptography, asymmetric key cryptography, homomorphic encryption, and lightweight encryption protocols, to design bio-inspired schemes that leverage principles.

| Blockchain based intelligent and private preserving data transfer in IoT networks |
| --- |

The surge in Internet of Things (IoT) devices, here's a ton of data being generated and shared among them. But, keeping this data safe and private is tough. This project suggests a new way to securely send data between IoT devices using something called blockchain. Blockchain is like a super secure digital ledger. We're combining blockchain with smart ways to manage data to make sure it stays safe and private.

Our main goal is to create a strong system for sending data between IoT devices. We want to do this while keeping your personal info private. We're looking into using blockchain along with unique techniques and ways to keep data private.

| Multiple Message Presaving for the Identification of malwares using Artificial Intelligence |
| --- |

The identification and mitigation of malware threats pose significant challenges in today's interconnected digital landscape. Traditional malware detection techniques frequently depend on static signatures or behavioral analysis, which may not be able to keep up with the continuously changing threat ecosystem. We provide a new method in this project that uses artificial intelligence approaches to identify malware: Multiple Message Preserving for Malware Identification. Malware detection accuracy and efficiency are improved by MMPMI's integration of multiple message preservation techniques. Our approach attempts to capture several features of malware variants while reducing false positives by maintaining different facets of malware behavior, such as code structure, execution patterns, and system interactions. Through the use of advanced machine learning algorithms such as deep learning and ensemble methods, Our findings demonstrate MMPMI's promise as a reliable and flexible way to identify malware threats in real time, improving network and computer system security.

| Mutual Authentication Systems for the Edge –Based IoT devices |
| --- |

"Mutual Authentication Systems for the Edge-Based IoT devices" discusses the development of authentication mechanisms tailored for edge-based Internet of Things (IoT) devices. These systems are designed to ensure secure communication between devices and their respective networks, addressing the unique challenges posed by edge computing environments. This likely highlights the importance of mutual authentication, where both the device and the network verify each other's identity, enhancing overall security. Additionally, it may touch upon the implementation of encryption and decryption techniques to safeguard sensitive data transmitted between devices and the network. It provides insight into the significance of robust authentication mechanisms in securing IoT ecosystems at the edge. This ensures that data transmitted between the sites is encrypted and can only be decrypted by the intended recipient, providing confidentiality and integrity for the page.

| AI based Battery Management Systems connected in an IoT environment |
| --- |

The AI-based battery management system likely outlines the integration of artificial intelligence (AI) techniques to optimize the performance and longevity of batteries across various applications. It discusses the challenges associated with traditional battery management systems, such as limited accuracy in predicting battery health and optimizing charging/discharging cycles. The abstract would likely highlight how AI algorithms, such as deep learning, are employed to analyze battery behavior, predict degradation patterns, and dynamically adjust charging parameters in real-time. Furthermore, it may emphasize the benefits of such a system, including extended battery lifespan, improved energy efficiency, and enhanced safety. Overall, this project would provide insight into the innovative approach of leveraging AI for efficient battery management, contributing to advancements in sustainable energy usage and electronic device performance.