SUSTAINABLE DEVELOPMENT GOALS

16. PEACE, JUSTICE AND STRONG INSTITUTIONS

Back to main

Academic Freedom Policy

- Ensure that all faculty, students, and staff can freely engage in research, discussions, and debates on peace, justice, and institutional integrity without fear of censorship or backlash.
- Promote an inclusive atmosphere where a range of perspectives, particularly those from marginalized or underrepresented groups, are acknowledged and appreciated in scholarly discussions on subjects linked to SDG 16.
- Provide resources and protection for research on critical issues like corruption, human rights, peace-building, and social justice, even when findings may challenge powerful interests.
- Encourage ethical practices in research and discourse, ensuring academic work contributes constructively to peace and justice without compromising truth or transparency.
- Protect the academic community from undue political, corporate, or government entities that could threaten independence and integrity in research and teaching.
- Establish transparent and fair processes for handling conflicts related to academic freedom, ensuring impartiality in cases of disputes or challenges to freedom of expression.
- Promote international partnerships and knowledge-sharing on peace, justice, and institutional resilience, supporting SDG 16 on a global scale.
- Lead by example with transparent governance, demonstrating the values of accountability, justice, and ethical decision-making within the institution.
- Educate academics on peace, justice, and strong institutions. Integrate SDG 16 goals into curriculum to promote responsible and informed action.

Policy History

Policy created on	25-04-2019
Policy reviewed on	06-06-2022

Student Projects Contributing in SDG-16

S.No	Name of the Project	Abstract
1	Secure cloud data storage with integer based encryption and efficient space utilization	The increasing reliance on cloud-based data storage necessitates robust solutions to address security vulnerabilities associated with traditional encryption methods. This work addressed the critical problem of potential unauthorized access and decryption of sensitive data stored in the cloud by introducing a novel approach to secure cloud data storage. The proposed system utilized integer-based encryption, adding an additional layer of security by converting input data into integers before encryption. Implemented in MATLAB with a user-friendly graphical interface, the system not only enhanced security but also optimizes storage space through the efficient representation of data as integers. The dual-layered encryption strategy ensured that even in the event of a security breach, compromised data remains encrypted, safeguarding sensitive information. The work contributed to advancing the discourse on secure cloud data storage by presenting a comprehensive solution that aligns with the evolving needs of information management systems in a cloud-centric environment
2	Design and Detection of HT using side channel analysis	Power analysis techniques have emerged as a promising method for detecting hardware Trojans within integrated circuits (ICs). This proposed work explores the application of power analysis in hardware Trojan detection, focusing on the use of power monitors to identify abnormal power consumption patterns associated with Trojan activation. By analyzing the power signatures of ICs during operation, power analysis can uncover subtle deviations indicative of Trojan presence, activation, or malicious behavior. This work begins by providing an overview of hardware Trojans and their potential threats to IC and PCB security, highlighting the need for robust detection methods. It delves into the principles of power analysis, explaining how variations in power consumption can reveal insights into IC behavior and functionality. Specifically, this experiment examines the use of power monitors, which are

		specialized hardware components capable of accurately measuring power consumption in real-time. Next, this work discussed various power analysis techniques employed in hardware Trojan detection, including static power analysis, dynamic power analysis, and differential power analysis. It explored how these techniques leverage power signatures to identify anomalies associated with Trojan insertion, activation triggers, and malicious payloads. Furthermore, this work presented case studies and experimental results demonstrating the effectiveness of power analysis in detecting hardware Trojans across different IC designs and scenarios. This work discusses challenges and limitations associated with power analysis, such as noise, calibration, and sensitivity to Trojan variations, and propose strategies to address these issues.
3	Fake news detection: An ensemble approach	This is a review report on the research performed and a project built in the field of Information Technology to develop a system for Detecting Fake news to prevent the spread of misinformation that happens through various fake news sites, online media, social media, etc. In this project we made use of some existing solutions for fake news detection like using classical approach, ensemble methods, natural language processing, sentiment analysis, and aimed to improve the accuracy of the existing models. The implementation part of the project gave us an idea of how the system works in real world scenarios, its possible use cases and the changes that can be improved or implemented that can enhance the working and utility of the machine learning model. Furthermore, the paper contains a deep analysis about the project architecture along with some important observations made by the authors of the project. These observations were used to achieve better optimization of the proposed system. The machine learning models used in this system were trained on a WELFake dataset which contained over 70,000+ news articles(a mixture of fake and real news). There have been several models and techniques proposed in the past which used the classical machine learning models like Logistic Regression, SVM, Decision Trees, Random Forest, deep learning models like CNN, BERT, and Ensemble Techniques were used in the past as well. The maximum accuracy achieved using those models was around 96.11% but we propose a system that has achieved an accuracy of

		97% This report is a detailed discussion of how we achieved a higher accuracy, what techniques were used and some samples screenshots of how it might get implemented in the real-world.
4	Democracy direct: A Digital poll revolution	The project Digital Poll is a web portal for developing a Voting System for schools and colleges. The project makes the election in digitalized form. Digital Poll is aimed at developing a voting system in online mode. The main objective of developing the system is for voting purpose which saves lot of time in counting process. It makes the voting process fully digitalized. which is very fast and more efficient. Even though this application maintains the records of the students, candidate's records and voting records. Digital Poll can be used by any schools and colleges to make election digitalized. In 'Digital Poll' a voter can use his/her voting right online without any difficulty. Voters has to be registered first to vote the nominee. Registration is mainly done by the system administrator for security purpose.To successfully implement a college voting system, it is important to involve all stakeholders in the process, including students, faculty, administrators.
5	AI -Powered assistance simplifying sentiment analysis in digital discussions	In today's tech world, our project serves as a versatile assistant, integrated with smart devices like Google and Siri. It handles voice input and output for tasks such as medical advice, organization, notes, calculations, and searches. Using microphones, it accesses the web for information, employing Natural Language Processing for communication.
6	Decentralized identity management	Identity management is the process of setting and organizing the roles and access privileges of a user's identity. The current identity management system is centralized and is controlled by a single entity. Users' privacy concerns are not in their best interest. Users have very little to no control over their data. The centralized system becomes a single point of failure which is prone to attack that leads to users losing their data privacy if these centralized systems are breached. Therefore we propose a Block chain-based decentralized Identity Management System that makes use of self-sovereign identity, decentralized identifiers, and verifiable credentials. It also gives users the ability to choose from a very large number of identity providers instead of just a select few corporations. The main advantages of the proposed solution

		include the elimination of the need for a central authority for identity verification and identity data management, the reduction of time spent on identity verification, the ability to share data with permission, and the ability to verify the origin of the data while sharing.
7	People opinion analysis using valence aware dictionary and sentiment reasoner	People opinion analysis primarily focuses on the evaluation of feelings and viewpoints in written material. As opinion mining, sentiment analysis can be referred to. Sentiment analysis identifies and supports a person's feelings toward a specific material source. Huge amounts of sentiment data are present on social media in the form of tweets, blogs, status updates, postings, etc. The viewpoint of the majority can be expressed extremely effectively using sentiment analysis of this widely generated data. Due to slang, misspellings, and repeated characters, Twitter sentiment analysis is more difficult than wide sentiment analysis. We are aware that each tweet on Twitter can only be 140 characters long. Therefore, it is crucial to determine the exact sentiment behind each word. In our research, we provide a very precise model for the sentiment analysis of tweets in relation to the most recent reviews of upcoming Hollywood or Bollywood films. We are accurately identifying these tweets as Positive, negative to offer sentiment of each tweet with the aid of feature vector and classifiers like Support vector machine and Logistic Regression.
8	Secure and Efficient privacy preserving probable data possession	Cloud computing is an emergent paradigm to give dependable and versatile foundation empowering the clients to store their data and the information purchasers can access the data from cloud servers. This worldview decreases stockpiling and support cost of the information proprietor. At the meantime, the information proprietor loses the physical control and ownership of data which leads to many security dangers. Therefore, auditing service to check data integrity in the cloud is essential. This issue has become a challenge as the possession of data needs to be verified while maintaining the protection. To address these issues this work proposes a protected and effective security saving provable information ownership. Further, we stretch SEPDP to support different proprietors, data dynamics and clump verification. The most alluring e feature of this scheme is that the reviewer can verify the possession of data with low computational overhead.

9	Feature level fusion of the face and finger print biometrics	The aim of this paper is to study the fusion at feature extraction level for face and fingerprint biometrics. The proposed approach is based on the fusion of the two traits by extracting independent feature pointsets from the two modalities, and making the two pointsets compatible for concatenation. Moreover, to handle the 'problem of curse of dimensionality', the feature pointsets are properly reduced in dimension. Different feature reduction techniques are implemented, prior and after the feature pointsets fusion, and the results are duly recorded. The fused feature pointset for the database and the query face and fingerprint images are matched using techniques based on either the point pattern matching, or the Delaunay triangulation. Comparative experiments are conducted on chimeric and real databases, to assess the actual advantage of the fusion performed at the feature extraction level, in comparison to the matching score level.
10	SSPRIVACY -Enhanced security in message and file transferring using PHP timestamps and whispering technology	This paper presents an innovative approach to enhancing security in message transmission and file transfer over networks using PHP timestamps and whispering technology. In today's digital landscape, ensuring the confidentiality and integrity of data during transmission is paramount to safeguarding sensitive information from unauthorized access and tampering. Our proposed system leverages PHP timestamps to generate unique identifiers for messages and files, which are then encrypted using whispering technology to obscure their contents from potential eavesdroppers. The utilization of PHP timestamps ensures temporal validity and non-repudiation, while whispering technology provides robust encryption to protect data in transit. Through extensive experimentation and evaluation, we demonstrate the effectiveness and efficiency of our approach in mitigating security risks associated with message and file transfer, thereby bolstering the confidentiality, integrity, and authenticity of communications over networks. Our system offers a viable solution for organizations and individuals seeking to fortify their data transmission mechanisms against evolving cyber threats and vulnerabilities.
11	GLOBAL THREAT MONITORING WITH AZURE SENTINEL AND GEOMAPPING	Cybersecurity threats present substantial risks to organizations globally, necessitating advanced threat monitoring and response mechanisms. This paper introduces a novel approach to augmenting

		real-time threat monitoring capabilities by integrating Azure Sentinel, a cloud-native Security Information and Event Management (SIEM) solution, with GeoMapping technology. By harnessing Azure Sentinel's sophisticated threat detection and investigation capabilities alongside GeoMapping's spatial visualization features, our system offers security professionals comprehensive visibility into global threat landscapes. We discuss the architecture, implementation, and feasibility of our system, emphasizing its technical, economic, and operational viability. Additionally, we present the outcomes of system testing and evaluation, showcasing its efficacy in detecting and responding to cyber threats. This research contributes to the cybersecurity field by proposing an innovative solution for proactive threat defense and risk mitigation in digital environments.
12	Digital counter terrorism to detect the online proliferation of terrorist	Terrorism has proliferated exponentially in certain regions, necessitating urgent action to curb its impact on human lives and property. The widespread adoption of technology, particularly the internet, has facilitated the dissemination of terrorist propaganda through speeches and videos. Terrorist groups exploit online platforms to malign individuals, recruit followers, and incite criminal activities. To counter this threat effectively, the integration of web mining and data mining techniques is imperative. Web mining encompasses diverse text mining methodologies that enable the extraction of pertinent information from unstructured data sources. Text mining plays a crucial role in uncovering patterns, identifying keywords, and extracting significant insights from unstructured textual content. Both data mining and web mining algorithms are instrumental in analyzing structured datasets and extracting valuable information from the vast expanse of web content. However, the varying data structures of websites pose challenges for a singular algorithmic approach. Terrorist groups exploit the internet to spread propaganda and recruit followers through webpages. To counter this threat, web mining and data mining can be used to extract valuable information from vast amounts of web data. Text mining algorithms can then analyze this data to identify patterns and critical information. The internet has become a breeding ground for terrorist activities, used to propagate extremist ideologies and recruit followers. Terrorist organizations

		leverage web pages to spread hate speech and propaganda, urging viewers to join their cause. To combat this threat, web mining and data mining techniques can be employed to extract relevant information from vast amounts of unstructured web data.
13	Distributed ledger technology - Embedded byzantine fault - tolerant web based electoral mechanism (Votechain)	Elections are crucial for modern democracies. However, many individuals do not view them as having a significant impact on democracy. Vote-rigging, hacking Electronic Voting Machines (EVMs), election manipulation and polling booth capturing are some of the issues responsible for the growing mistrust over the electoral process. Block chain is a technology that allows and opens up a possibility for developing a secure and reliable system. This study aims to contribute to the advancement of secure and reliable electoral systems, addressing challenges associated with trust, security, and transparency in traditional voting methods. The block chain is an emerging, decentralized and distributed technology. It eliminates the need of a third party to manage the access control in the process of election. A voting system that relies on block chain ensures both the security and integrity of votes, all while maintaining transparency throughout the process. This project contributes to the evolution of a new way of exercising a healthy democracy. This project focuses on implementing a web-based application that facilitates convenient and secure participation for remote voting through computer or a smartphone. We utilise Ethereum block chain network to implement the project along with Meta Mask wallet. To increase the efficiency of the system, we deploy a new and optimized version of the Byzantine Fault Tolerance (BFT) consensus algorithm called the Federated Byzantine Agreement (FBA). This helps the nodes to achieve consensus even in the face of faulty or malicious nodes. “Distributed Ledger Technology-Embedded Byzantine Fault Tolerant Web-Based Electoral Mechanism (VOTECHAIN)” offers a comprehensive system that is feasible.
14	Credit card fraud detection using Artificial Intelligence	Credit card fraud detection using ARTIFICIAL INTELLIGENCE Abstract: A credit card is issued by a bank or financial services company that allows cardholders to borrow funds with which to pay for goods and services with merchants that accept cards for payment. Nowadays as everything is made cyber so there is a chance of misuse of cards

		and the account holder can lose the money so it is vital that credit card companies are able to identify fraudulent credit card transactions so that customers are not charged for items that they did not purchase. This type of problems can be solved through data science by applying machine learning techniques. It deals with modelling of the dataset using machine learning with Credit Card Fraud Detection. In machine learning the main key is the data so modelling the past credit card transactions with the data of the ones that turned out to be fraud. The built model is then used to recognize whether a new transaction is fraudulent or not. The objective is to classify whether the fraud had happened or not. The first step involves analyzing and pre-processing data and then applying machine learning algorithm on the credit card dataset and find the parameters of the algorithm and calculate their performance metrics.
15	Development of lost kid recognition system using multiclass SVM and CNN	This paper tells a pair of novel use of deep learning methodology which is employed for identifying the reported missing children from the images of multiple youngsters available, with the assistance of face recognition. the ultimate public can upload their images of suspicious children into an everyday portal with landmarks and remarks. The photo are automatically compared with the registered photos of the missing child from the repository. Cataloging of the input child photo is performed and photo with best match are designated from the database of missing children. For this, a deep learning model is trained to properly identify the missing child from the missing child image database provided, using the facial image uploaded by the final word public. The Convolutional Neural Network (CNN), is incredibly effective deep learning technique for image based applications is adopted here for face recognition. Face descriptors are extracted from the images employing a pre-trained CNN model VGG-Face deep architecture. Compared with normal deep learning applications, our algorithm uses convolution network only as a high level feature extractor and thus the kid recognition is completed by the trained SVM classifier. Choosing the foremost effective performing CNN model for face recognition, VGG-Face and proper training of it finally ends up during a very deep learning model invariant to noise, contrast, image pose and also the age of the children and earlier methods in face

		recognition based missing child identification.
16	Truth Track: Harnessing RNNs and NLP for news verification with chatbot support	Research delved into the pervasive issue of fake news and limited information literacy through a novel AI system. The system, which utilized Natural Language Processing (NLP) techniques and Recurrent Neural Networks (RNNs), offered the following key functionalities. An RNN model, trained on a comprehensive dataset of labelled real and fake news articles, was used to analyse news content using NLP. The likelihood of an article being fake news was then predicted by the model. Additionally, legitimate news was categorized into relevant categories (politics, sports, business) using NLP techniques like topic modelling. To address user queries arising from news content, an NLP-powered chatbot was integrated into the project. User questions were understood, and the most relevant and reliable information was provided by the chatbot, leveraging machine learning. The news analysis performed by the first component was drawn upon by the chatbot, guiding users towards trustworthy sources and offering explanations to combat potential biases. The primary objective of the AI system was to empower users to become more discerning consumers of information. Users could readily identify fake news and gained a deeper understanding of legitimate news content. Information literacy was further enhanced by the chatbot, which provided context and facilitated user queries.
17	A Multi-modal approach for Deepfake detection system using LSTM and MLP in CNN	In the rapidly advancing landscape of machine learning, the detection of deepfake videos has become an imperative challenge. The proposed introduces a novel approach everaging the synergies of Dense Net v2, LSTM, and MLP architectures in a multi-modal system for enhanced deepfake detection. In an extensive review of existing work in deepfake detection, identifying key parameters and methodologies. The project model integrates the strengths of Long Short-Term Memory (LSTM) networks and Multi-Layer Perceptron (MLP) classifiers with the feature extraction capabilities of Dense Net v2, creating a robust and efficient framework. The training process involves optimizing key parameters to ensure model accuracy, and discuss the tools employed for data preprocessing and model evaluation. In experimental results, it present a comprehensive performance analysis using precision-recall curves, confusion matrix heatmaps,

		F1 score comparison bar charts, and accuracy box plots. The proposed multi-modal approach demonstrates superior detection capabilities compared to existing models, showcasing its potential for real-world applications. The study contributes not only to the field of deepfake detection but also to the broader discourse on the intersection of machine learning and video analysis.
18	Performance enhancement of video surveillance in fortifying banking security through darknet analysis	This research delves into the fusion of the YOLO v5 (You Only Look Once) object detection framework with the Darknet architecture to create an advanced Intelligent Video Image Processing and Monitoring Control System tailored explicitly for enhancing security in the banking sector. Leveraging the real-time object detection capabilities of YOLO v5, the system enables efficient monitoring and surveillance across various areas within bank premises. Darknet, functioning as a neural network framework, serves as the foundational structure for implementing and optimizing YOLO v5 within the proposed system. This integration ensures robust real-time performance, allowing for seamless monitoring and control mechanisms throughout banking environments. By utilizing Darknet's capabilities, the system can effectively handle the complexities of processing video feeds in real-time, enhancing overall security measures within banking facilities. The primary objective of the proposed system is to bolster security measures within banking environments by providing instantaneous and accurate alerts for potential security threats or anomalous activities Through the amalgamation of YOLO v5 and Darknet, the system aims to offer comprehensive surveillance capabilities, enabling banking institutions to proactively identify and respond to security incidents promptly. This innovative approach to video image processing and monitoring control holds promise for significantly enhancing security protocols within the banking sector.
19	Authentication access control for vehicle ignition system using RF and Fingerprint technology	Fingerprint identification is one of the most popular and reliable personal biometric identification methods. The proposed system consists of a smart card capable of storing the fingerprint of particular person. While issuing the license, the specific person’s fingerprint is to be stored in the card. Vehicles such as cars should have a card reader capable of reading the particular

		license. The same automobile should have the facility of fingerprint reader device .A person, who wishes to drive the vehicle, should insert the smartcard in the vehicle and then swipe his/her finger. If the fingerprint matches with the fingerprint stored in the smart card then it goes for alcohol detection and seatbelt checking. After passing all authentications, the vehicle will be ignited. The vehicle will not be ignited, if any one of the authentications fails and will not proceed the next step. This increases the security of vehicles and also ensures safe driving by preventing accidents. The prototype of the ignition system is used by the Master controller (Cortex M3 based Micro controller) is implemented along with the vehicle prototype is developed and the results are attached. Biometric authentication is an emerging technology that has found its application in various domains. One of the domains that have recently gained attention is vehicle ignition. This technology is used to prevent unauthorized access to the vehicle and ensure that only the authorized driver can start the vehicle. The biometric authentication system typically uses a combination of physiological and behavioural traits to identify the driver, such as facial recognition, fingerprint scanning, recognition, voice recognition, and gait analysis. This paper aims to provide an overview of the biometric authentication system for vehicle ignition, including the advantages, disadvantages, and challenges of implementing such a system. The paper also discusses the different biometric modalities that can be used for authentication, the algorithms used for recognition, and the security aspects of the system. The results show that biometric authentication for vehicle ignition has the potential to increase the security of the vehicle and prevent theft. However, there are still some technical and social challenges that need to be addressed before this technology can be widely adopted.
20	Border defense mechanism classification using Deep Learning techniques	The Advancements in deep learning are set to transform border defense, leveraging attention mechanisms and meta-learning to enhance threat detection accuracy. Integrating diverse sensor types, including aerial imagery, satellite data, social media analytics, and IoT devices, offers a comprehensive surveillance approach. This multi-modal data fusion enables nuanced threat assessments, improving situational awareness.

		Real- time processing, facilitated by edge computing solutions, ensures swift responses to potential threats by handling high-volume streaming data efficiently. Despite technological strides, ethical considerations remain paramount. Transparency, fairness, and privacy protection are imperative in border security applications. Implementing accountable decision-making processes and privacy-preserving techniques in data processing pipelines is essential. Engaging stakeholders ensures societal concerns are addressed, balancing security needs with individual rights. Ultimately, the future of border defense classification holds promise for more accurate, efficient, and responsible systems. By prioritizing ethical principles alongside technological innovation, borders and sensitive areas can be safeguarded effectively while upholding fundamental rights and values.

Events to raise awareness for SDG-16

Raise awareness about Sustainable Development Goal 16 (SDG 16) – "Peace, Justice, and Strong Institutions" – and mobilize individuals and organizations to take actionable steps towards promoting peaceful, inclusive societies.

1. On the **187th birth anniversary of Sri Ramakrishna Paramahamsa**, a **Power Talk** was conducted at **CIT Campus** exclusively for the **2nd-year students**, centered on the inspiring theme: **"Discover the Power Within You."** The event aimed to honor the timeless teachings of Sri Ramakrishna, focusing on the importance of self-discovery and inner strength in navigating life's challenges. It encouraged students to realize their potential and build a strong foundation for personal and professional growth.

Back to main