COMPUTER NETWORKING

LIST OF PROJECTS

DIPLOMA IN COMPUTER NETWORKING

Project No	Title of the Project
CN1	AI BASED ASSISTANT FOR AUTONOMOUS ROBOTS
CN 2	EARLY WARNING SYSTEM TO DETECT SEWAGE BLOCKS & HAZARDOUS GASES USING IOT
CN 3	EARLY FLOOD WARNING SYSTEM FOR DISASTER MANAGEMENT
CN 4	SECURING IOT USING BLOCKCHAIN
CN 5	THIRD EYE – AI BASED AUGMENTED REALITY
CN 6	QUANTUM SECURE BLOCK-CHAIN SYSTEM USING POST-QUANTUM CRYPTOGRAPHY
CN 7	IOT BASED ATTENDANCE MONITORING SYSTEM

AI BASED ASSISTANT FOR AUTONOMOUS ROBOTS

GUIDE

Dr.S.Brindha

STUDENTS NAME

Mubashira Khatoon.M (19DC13)

Nimrukthi.S (19DC15)

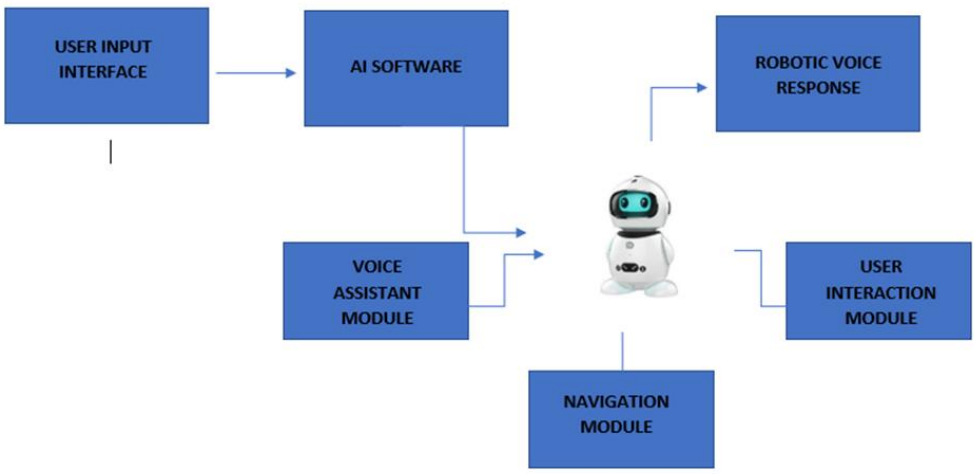
Rajasurya.E (19DC19)

Stenson.T (19DC25)

In this proposed system we aim to build an AI based assistant for autonomous robot. The AI based assistant will enable robots to respond to user questions related to the company in a human like manner which has the features including the voice assistance, navigation to the destination and understanding the expression and emotion.

Simpler autonomous robots rely on infrared or ultrasound sensors to help the robot "see" obstacles in their path. Higher-level robots such as autonomous vehicles use more complex sensors like cameras, radar and lidar (a detection system like radar, but using light from a laser). Combined with image-recognition software, these sensors allow the robot to precisely identify and categorize the objects they "see", and make real-time "decisions".

AI will be running in a server utilizing Application programming interface (API). An app will be created in android with speech to text and text to speech conversion capturing. When a speech is detected it will make request to AI model in the server and process the request and give back text. Then the Text-To-Speech Transaction Tracking System (TTS) engine will convert the text back to speech.



EARLY WARNING SYSTEM TO DETECT SEWAGE BLOCKS & HAZARDOUS GASES USING IOT

GUIDE

Ms.D.PRIYA

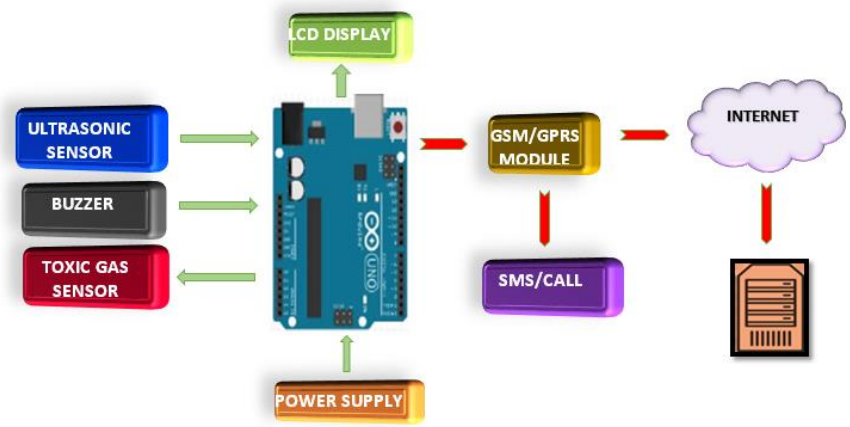
STUDENTS NAME

Brintha Shree S S	(19DC04)
Lakshmi Priya N	(19DC12)
Pavithran P	(19DC17)
Siranjeevi Srinivasan S	(19DC24)

Sewer flooding incidents are increasingly associated with the presence of blockages. Blockages are difficult to deal with as although there are locations where they are more likely to occur, they do occur intermittently. In order to manage sewer blockage pro-actively sewer managers need to be able to identify the location of blockages promptly. Drainage cleaning people are not aware of risk by sudden attack of poisonous gas since the gases are odorless, if exposed for long time which may cause serious health problems. Due to lack of Toxic gas leakage detection system, a number of dangerous accidents occurred during the last few last decades.

The main objective of the proposed system is to monitor the sewage blocks in sewer pipelines frequently and senses the hazardous gas using IoT. The proposed system identifies the blocks immediately after its occurrence using ultrasonic sensors and to alert the concerned maintenance in-charge at once using Wireless GSM module. Moreover, the entire system is taken care by a Centralized Monitoring System based on IoT Technology.

The proposed System consists of Arduino UNO Board, Power supply, LCD display, Ultrasonic Sensor, Toxic gas detector, Wireless GSM Module, Buzzer. Ultrasonic sensors are used to detect the blockage frequently in the sewage tunnel.Ultrasonic sensors detect objects regardless of the color, surface, or material (unless the material is very soft like wool, as it would absorb sound).Various Gas Sensors(MQ3, MQ6 etc.)are used to detect the toxic gases of water. The presence of sewage block and toxic gas related information from these sensors is received and processed in the Arduino UNO board and push notification is sent to the mobile in case of Blockage or Overflow. When these values reach a threshold value, then Arduino sends alert signal to the concerned department and it also sends location of the sewage vent using Wireless GSM and GPS module.



EARLY FLOOD WARNING SYSTEM FOR DISASTER MANAGEMENT

GUIDE

Ms.D.PRIYA

STUDENTS NAME

Gowtham S (19DC07)

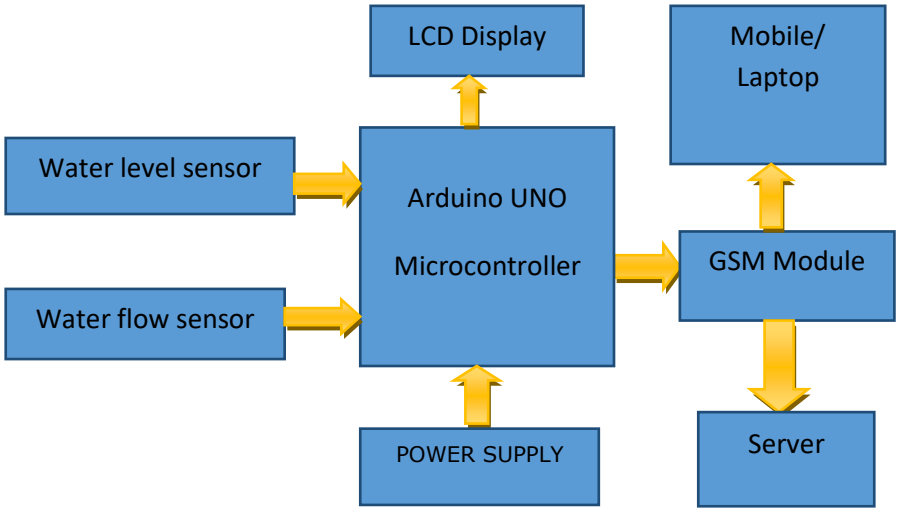
Kaliraj M (19DC09)

Karan Babu B (19DC10)

There are several types of natural disaster and one of the most vulnerable is Flood Disaster, which will have large consequences for individuals & Communities. Whenever, flooding happens, people living near the riverbank and downstream area are affected severely than others. They need to be alerted much earlier to have extra time to evacuate immediately. The main objective of the proposed system is to develop an early warning system to detect flood and send notifications to the authority so that they can evacuate people earlier and avoid loss of life and property.

This project is designed on the IoT based platform, where data from the sensor is collected at the Microcontroller and alert is generated and transmitted as SMS to Smartphone's. Our proposed system provides such information so that people can avoid false news. Also the proposed system makes use of voice call as it is helpful for people who do not know how to read the text message.

The main sensors used for our project are water level sensor and water flow sensor. Water level sensor is used to check whether the water reaches a certain level, and then it triggers the Arduino board to send the alerting messages. It consists of a circuit board, which can be programmed (referred to as a microcontroller) and a ready-made software called Arduino IDE (Integrated Development Environment), which is used to write and upload the computer code to the physical board. Then it is passed to GSM module for generating SMS aware of the residents, as a warning to take care and take precautions. If the water continues to rise and reaches the edge level, it's considered now as dangerous, an alert SMS once more sent to the resident and authorities. Water flow sensor is used to measure the flow level of the water. And then the details are displayed in LCD display continuously and a copy of the data is sent to server and to the user mobile or laptop as a notification.



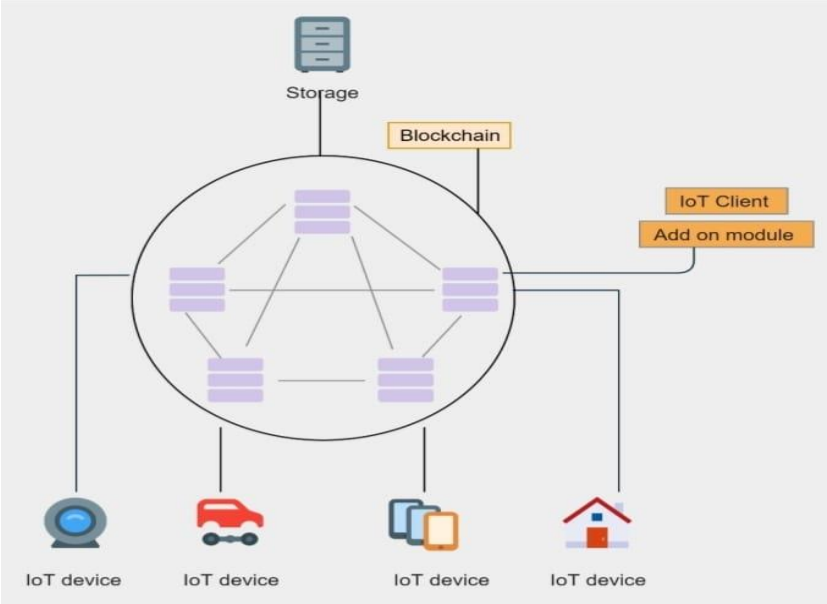
SECURING IOT USING BLOCKCHAIN

GUIDE	STUDENTS NAME	
MS.P.ABIRAMI	Aishwarya R	(19DC01)
	Ragavi N V	(19DC18)
	Shriehari A C	(19DC23)

The existing Blockchain-based IoT security solutions do not address the challenges- latency, applicability and resource-constraint. In direct wiretapping attacks, the attacker passively listens to network communications to gain access to private information, such as node identification numbers, routing updates, or application sensitive data. In sensor tampering attack manipulate the sensors to acquire data readings and sensor feed modification to modify the sensor feed and firmware during communications process.

In IoT devices ultrasonic sensor calculates the distance and collects the data, which can be manipulated. Which has a risk of privacy leakage and causes malicious traffic. The authentication system is based on single server architecture in which limitations are in terms of privacy, anonymity and integrity in direct wiretapping attack and DDoS attack.

Our proposed approach works in application and network layer using Hyperledger fabric Blockchain and add on hardware modules which offers a higher level of assurance, low level of assurance comparatively. A Blockchain-based status monitoring system is created for defending against unauthorized software updating in IoT devices. It can be solved using Blockchain based sensor data protection system (SDPS) and privacy aware data sharing using Blockchain VPN. It is filtered by SDN switch on the edge network which ensures synergy with the Blockchain environment and access from the Blockchain information about trustworthy resources and computers. A computer called validator is implemented which checks the IoT device validity using protocol of authentication.



THIRD EYE – AI BASED AUGMENTED REALITY

GUIDE

MS.T.P.KAMATCHI

STUDENTS NAME

Divith M J (19DC05)

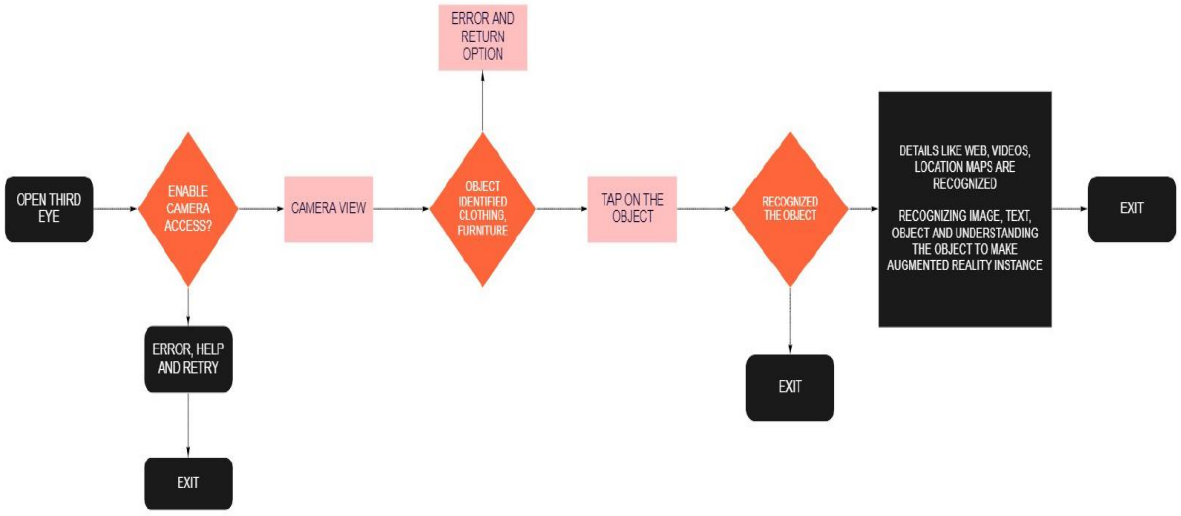
Mukil Aadhithian M S (19DC14)

Sanjay Kumar R (19DC21)

Augmented Reality starts with a camera-equipped device—such as a smartphone, a tablet, or smart glasses—loaded with AR software. When a user points the device and looks at an object, the software recognizes it through computer vision technology, which analyses the video stream. The device then downloads information about the object from the cloud, in much the same way that a web browser loads a page via a URL. A fundamental difference is that the AR information is presented in a 3-D "experience" superimposed on the object rather than in a 2-D page on a screen. As the user moves, the size and orientation of the AR display automatically adjust to the shifting context. New graphical or text information comes into view while other information passes out of view.

In industrial settings, users in different roles, such as a machine operator and a maintenance technician, can look at the same object but be presented with different AR experiences that are tailored to their needs. A 3-D digital model that resides in the cloud—the object's "digital twin"—serves as the bridge between the smart object and the AR. This model is created using computer-aided design and Android SDK (software development kit).

The twin then collects information from the product, business systems, and external sources to reflect the product's current reality. It is the vehicle through which the AR software accurately places and scales up-to-date information on the object.



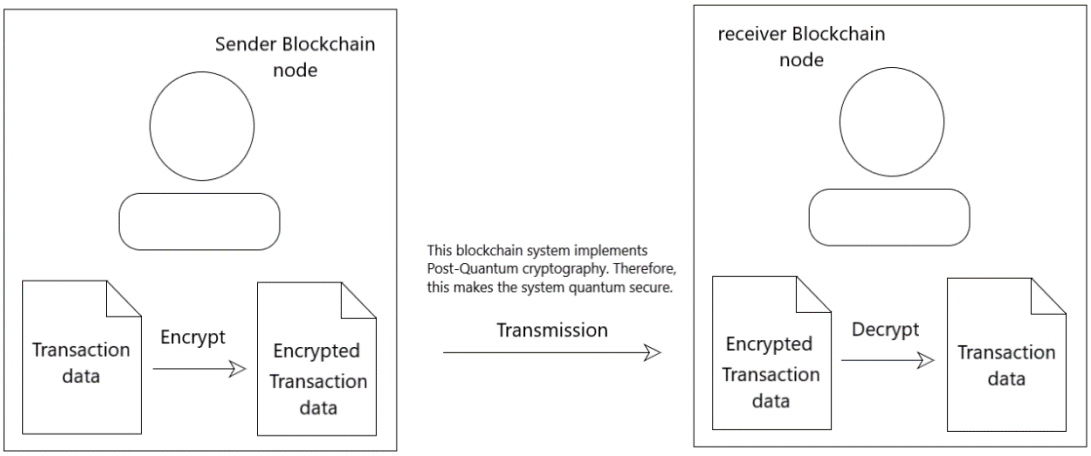
QUANTUM SECURE BLOCK-CHAIN SYSTEM USING POST-QUANTUM CRYPTOGRAPHY

GUIDE	STUDENTS NAME	
MS.T.P.KAMATCHI	Harshal Ram R V	(19DC08)
	Goutham Balaji P S	(19DC06)
	Karthikeyan T	(19DC11)

The objective of this project is to create a block-chain system that allows its nodes to perform quantum secure transactions and with quantum secure consensus (proof of work) mechanism. This is made possible by Post Quantum or quantum-resistant cryptography which is cost and time effect method to counter the quantum threats and it is implemented in a classical computer. Mathematical hardness of these cryptographic algorithm makes it secure against quantum attacks by quantum computers running Grover's and Shor's algorithms.

There are various types of PQC schemes which are safe against Shor's and Grover's algorithms. In this project lattice-based cryptography has been chosen to be implementing in the block-chain system because its most effective against the quantum threats, performs well when implemented in block-chain and its security properties based on worst-case assumptions. The name lattice based cryptography derived from fact that cryptography scheme in this area use the mathematical problems based on lattices. There are trapdoor functions quantum computers cannot crack, however. One such solution is to use a series of lattice operations instead of the traditional multiplication method. A lattice is a multidimensional mathematical group formed from a basis. The basis can be any set of linearly independent vectors whose components are whole integers.

This block-chain system implements lattice-based cryptography in both digital signature and consensus mechanism. This allows a node in the block-chain system to make quantum secure transaction with another node. This is possible by the implementation of lattice based digital signature scheme. To confirm these transactions a lattice-based consensus mechanism is implemented.



IOT BASED ATTENDANCE MONITORING SYSTEM

GUIDE	STUDENTS NAME	
Ms.P.ABIRAMI	Bala Ganesh A	(19DC03)
	Nishanth S	(19DC16)
	Vishnu Prasad N	(19DC26)

In the Fingerprint based existing attendance system, a portable fingerprint device need to be configured with the students fingerprint earlier. Later either during the lecture hours or before, the student needs to record the fingerprint on the configured device to ensure their attendance for the day. The problem with this approach is that during the lecture time it may distract the attention of the students.

Biometrics seem secure on the surface. After all, you're the only one with your ears, eyes, and fingerprint. But that doesn't necessarily make it more secure than passwords. A password is inherently private because you are the only one who knows it. Of course hackers can acquire it by brute force attacks or phishing, but generally, people can't Access it. On the other hand, biometrics are inherently public. Think about it: your ears, eyes, and face are exposed. You reveal your eyes whenever you look at things. With fingerprint recognition you leave fingerprints everywhere you go. With voice recognition, someone is recording your voice. Essentially, there's easy access to all these identifiers.

Our proposed system uses USB Camera which is connected to the raspberry pi camera slot. Live video stream of students is captured in the class with USB1 camera, Raspberry pi takes those images as input images and sends to the cloud server and we make use of face recognition service to compare the input images with the existing image which is already uploaded in the database. Matched images are detected and attendance is marked with date and time for students present in class in the local data base using MYSQL. Unmatched images are denied. This process is carried out for every period and students are given attendance accordingly. A unique RFID card is given to the faculty, when faculty enters the classroom and swipes the RFID card, the RFID sensor scans and sends the data to the database and displayed on OLED. We also, design a web application for the tracking of their attendance. Admin tracks the attendance of the students and faculty periodically or whenever required by the administration and finds the result. The result is displayed on the monitor screen and stores the validate images in the database. Student attendance will be monitored and if the student is absent for that class then the notification will send to the faculty and parents.