FLOOD MONITORING AND EARLY WARNING

# PHASE-2

**INNOVATION**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **ARTIFICIAL INTELLIGENCE APPLICATION TO DETECT FLOOD:**

## As climate change is increasing the frequency and intensity of climate and weather hazards, improving detection and monitoring of flood events is a priority. Being weather independent and high resolution, Sentinel 1 (S1) radar satellite imagery data has become the go-to data source to detect flood events accurately. However, current methods are either based on fixed thresholds to differentiate water from land or train Artificial Intelligence (AI) models based on only S1 data, despite the availability of many other relevant data sources publicly. These models also lack comprehensive validations on out-of-sample data and deployment at scale. In this study, we investigated whether adding extra input layers could increase the performance of AI models in detecting floods fromS1 data. We also provide performance across a range of 11historical events, with results ranging between 0.93 and 0.97accuracy, 0.53 and 0.81 IoU, and 0.68 and 0.89 F1 scores. Finally, we show the infrastructure we developed to deploy ourAI models at scale to satisfy a range of use cases and user requests.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **SOME INNOVATION THROUGHT IN MY PROJECT ARE:**

Flood monitoring and early warning systems have indeed become important tools for addressing flood-related issues. Innovation in this field can help improve the effectiveness of such systems. Some innovations in our project include

**Remote Sensing Technologies:** Leveraging satellite imagery, drones, and other remote sensing technologies to monitor weather patterns, water levels, and potential flood risks in real-time.

**Data Analytics:** Utilizing advanced data analytics, machine learning, and AI algorithms to process and analyze vast amounts of data quickly, improving flood prediction accuracy.

**Mobile Apps and Alerts:** Developing user-friendly mobile apps and alert systems that provide timely information to residents, allowing them to take preventive actions.

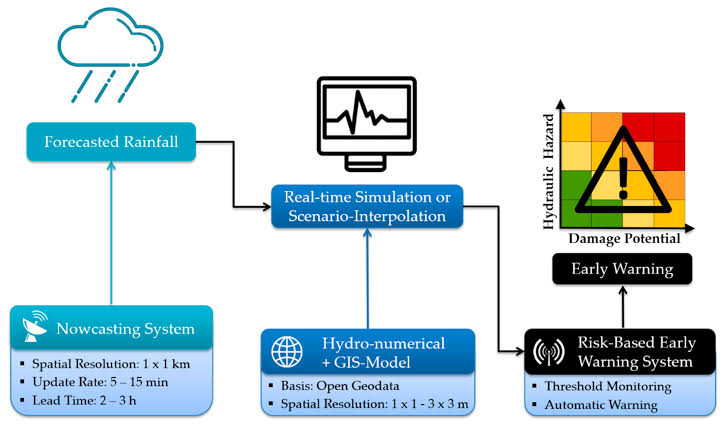
**IOT Sensor Network**: Create a network of IoT sensors strategically placed in flood-prone areas. These sensors can monitor water levels, rainfall, and soil moisture in real-time.

**Machine Learning Algorithms:** Implement machine learning algorithms to analyze the data collected from sensors. These algorithms can predict potential flood events based on historical data and weather forecasts.

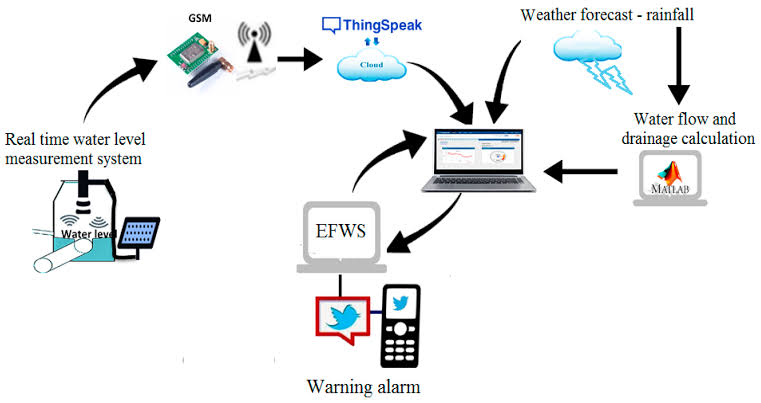
**Mobile App Integration**: Develop a user-friendly mobile app that allows residents to receive real-time flood alerts and updates. Include features like evacuation routes, emergency contacts, and flood safety tips.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

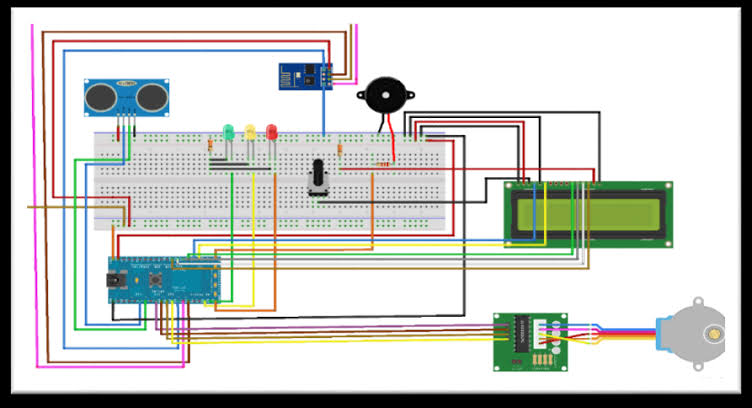
## **BLOCK DIAGRAM FOR FLOOD MONITORING AND EARLY WARNING:**



## **WORKING PRINCIPLE DIAGRAM:**

****

## **CIRCUIT DIAGRAM FOR FLOOD MONITORING AND EARLY WARNING USING IOT:**



**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## How does flood protection work on QRadar Network Security (XGS) sensors?

**Flood Module**  
  
The Protocol Analysis Module (PAM) provides a flood module to detect, report, and block denial of service attacks and other aggregate network events. Flood module signatures are triggered by a large number of network frames associated with a single IP address (intruder or victim, depending on the signature) over some configured duration of time. These signatures share a common configuration interface, detection algorithm, and event reporting mechanism. Note that PAM has some additional flood signatures, such as SYNFlood, TCP connection floods, and DNS response floods, that are not part of the flood module and have differing implementations.  
  
  
**Detection**  
  
As PAM analyzes a frame that may contribute to a flood attack, it determines whether the number of similar frames processed within the configurable detection interval has reached the configurable threshold for the relevant signature. If a flood threshold defined in the flood module is reached, PAM reports an initial event and maintains an active flood entry. If flood intruder tracking is enabled (the default behavior) and the attack is distributed across multiple intruders, PAM will report a new event for each top intruder contributing to the flood. Otherwise, PAM will regularly report updates on the total number of flood frames detected during the most recent detection interval until the flood ends. These events are reported once per reporting interval, which is 60 seconds by default. Note that the report interval may differ from the signature's detection interval.  
  
  
**Protection**  
  
Flood protection may vary based on the type of event and the configured blocking response. If a quarantine response is assigned to the signature, each new event may create or update a new quarantine rule for the specified intruder. As new top intruders are reported, more rules are created, prioritizing those intruders producing the greatest volume of traffic, and thereby reducing the likelihood of false positives. Aside from dynamic blocking, the standard block response will close and temporarily block TCP connections for TCP-based floods, and will block all UDP frames for the following UDP-based floods:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Flood monitoring and early warning systems in IoT (Internet of Things) play a crucial role in problem solving related to flooding. These systems involve the use of sensors and data analysis to provide timely information and alerts. Here's how they work:

**Sensor Deployment:** IoT sensors are placed in flood-prone areas, near rivers, and in urban areas to monitor water levels, rainfall, and other relevant data.

**Data Collection:** These sensors continuously collect data on factors like water level, weather conditions, and soil moisture.

**Data Transmission:** The collected data is transmitted in real-time to a central server or cloud platform using wireless communication protocols, such as LoRa, NB-IoT, or Sigfox.

**Data Analysis:** Advanced analytics are applied to the collected data to identify patterns and anomalies. Machine learning algorithms can be used to predict potential flooding events.

**Early Warning:** When a potential flood event is detected, automated alerts are generated. These alerts can be sent to authorities, emergency services, and the public through various communication channels like SMS, mobile apps, and sirens.

**Decision Support:** Decision-makers can use the real-time and predictive data to make informed decisions about evacuations, resource allocation, and flood mitigation strategies.

## Benefits of IoT flood monitoring and early warning systems include:

**Timely Alerts:** IoT systems can provide early warnings, giving people more time to prepare and evacuate if necessary.

**Data Accuracy:** Continuous monitoring ensures accurate data collection, which is vital for making informed decisions.

**Cost Efficiency:** These systems can reduce the cost of disaster response and recovery by minimizing damage and casualties.

**Remote Monitoring:** Authorities can monitor flood-prone areas remotely, reducing the need for physical presence in dangerous conditions.

**Historical Data:** IoT systems can also provide historical data that can be used for long-term flood risk assessment and infrastructure planning.

Overall, IoT flood monitoring and early warning systems are a powerful tool for addressing the challenges of flooding and improving disaster resilience.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**