**Project Proposal**

- **Project title**: Securing IR communication from replay attacks

- **Team members**: Aisha Kothare and Namruth Reddy

- **Project outline:**

Infrared signals are widely used for communication between devices. It is primarily used in short-range distances, cost-effective, and small-scale data transmission use cases. Examples include remote-controlled smart devices, TVs, and more.

It is seen that most of these communications are susceptible to replay attacks, wherein data transmitted can be intercepted and replayed across to the receiver.

We aim to secure this communication so that replay attacks can be prevented

- **Tasks and Timeline**:

Week 1-2: Understanding IR communication and arranging the hardware.

Week 3-4: Building the transmitter and receiver using Arduino circuit

Week 5-6: Intercepting data and conducting replay attacks.

Week 7-8: Implementing security mechanisms to prevent such attacks.

Week 9-10: Analysis of security vs performance, usability, and cost

**- Motivation**

* Building our IR communication system using Arduino and other hardware.
* Understanding IR communication and specifically how it is susceptible to replay attacks.
* Implementing the security mechanisms to prevent these attacks and also understanding the effect of security on performance, usability, and cost.

**- Deliverables**

Three-part deliverables:

* Traditional IR communication system using Arduino
* Secure IR communication system to prevent replay attacks.
* Thorough Analysis of security vs performance, usability, and cost

- **References**

* [IR Communication using Arduino UNO](https://www.electronicwings.com/arduino/ir-communication-using-arduino-uno)
* [High secure infrared communication application | IEEE Conference Publication](https://ieeexplore.ieee.org/document/5929690)
* Previous year’s project