**Problem Statement**

“The case where an application lies about its intention for requesting a permission or intentionally violates the user's expectation of an applications behavior is not so well researched.” [ref: Jemal, Identifying cyber threats to mobile-IoT applications in edge computing paradigm]

* **Research Proposal**
  + Our research is to find a predictive malware detection technique based upon an interaction index between permissions used and invasions found

**Applications / Motivation**

* First Application
  + Research Area: Intrusion Detection
  + Applications: Smart City / Smart Home
  + Example: Someone tries to enter home / a gated community / a city when it wasn’t allowed to enter
* Second Application
  + Research Area: Malware Detection
  + Applications: Mobile Sensors IoT
  + Details: The malware has become an increasing problem for Mobile-Internet of Things applications in edge computing platform. Variants of malware can be identified once their general characteristics are known and overtly malicious behavior can be identified.
  + Example:

**Related Work**

* First Related Work
  + Author: Jemal
  + Title: Identifying cyber threats to mobile-IoT applications in edge computing paradigm
  + Details:

We particularly focus on a greater set of permissions which may be leveraged for other purposes, for example by using sensors to record user credentials or monitoring a user's movements. This research will attempt to identify such scenarios by employing behavioral analysis to determine when and how permissions are used.

They also perform static and dynamic analysis to predict the behavior of application logic yet to execute.

They have described various techniques of intrusion detection such as signature based, anomaly based, behavior based etc. Methods for implementing these techniques include neural networks, data mining etc

* Second Related Work
  + Author: Somya
  + Title: Methods and Techniques of Intrusion Detection: A Review