The Internet of Things(IoT) Research Paper Competition 2018 and a roundtable discussion on IoT related policy issues.

Venue: Emerson Centre for Advanced Studies, Veermata Jijabai Technological Institute (VJTI).

Date: 27th February 2018.

“Imagine you are a cop. Your team is in hot pursuit of a convict who has been accused of mass shooting at a neighbourhood church which killed 26 people and wounded 20 other individuals. As your team’s vehicle follows the convict’s vehicle, the convict loses control of his vehicle and his vehicle flips into a ditch. You stop your vehicle and your team rushes towards the convict’s vehicle to save the convict. Unfortunately, the convict is found dead in his vehicle. As a part of cyber forensic investigation to determine the convict’s rationale to carry out mass shooting of school students, your team is supposed to investigate the convict’s mobile phone. Is it ethically right for your team to access a dead convict’s mobile phone as his consent can’t be sought?”

This scenario is inspired from mass shootings at a church in Sutherlands Springs in Texas in 2017. The scenario and corresponding question was raised by ISOC India Mumbai Chapter team to Master and Doctoral engineering students of VJTI. Though the students agreed that consent is critical to access any individual’s mobile records, they acknowledged the complexity of situation faced by police officials in procuring personal sensitive data of convicts.

In an era of ubiquitous Internet based technology, some Internet philosophers might opine that our devices are an extension of our biological anatomy. Thus, a smart phone is more than just a phone as no other piece of hardware captures quality and quantity of information that is held in your smartphone. In 2014, the United States Supreme Court used this observation of ‘technology as an extended mind’ to justify the decision that police must obtain a warrant before browsing our smart phones.

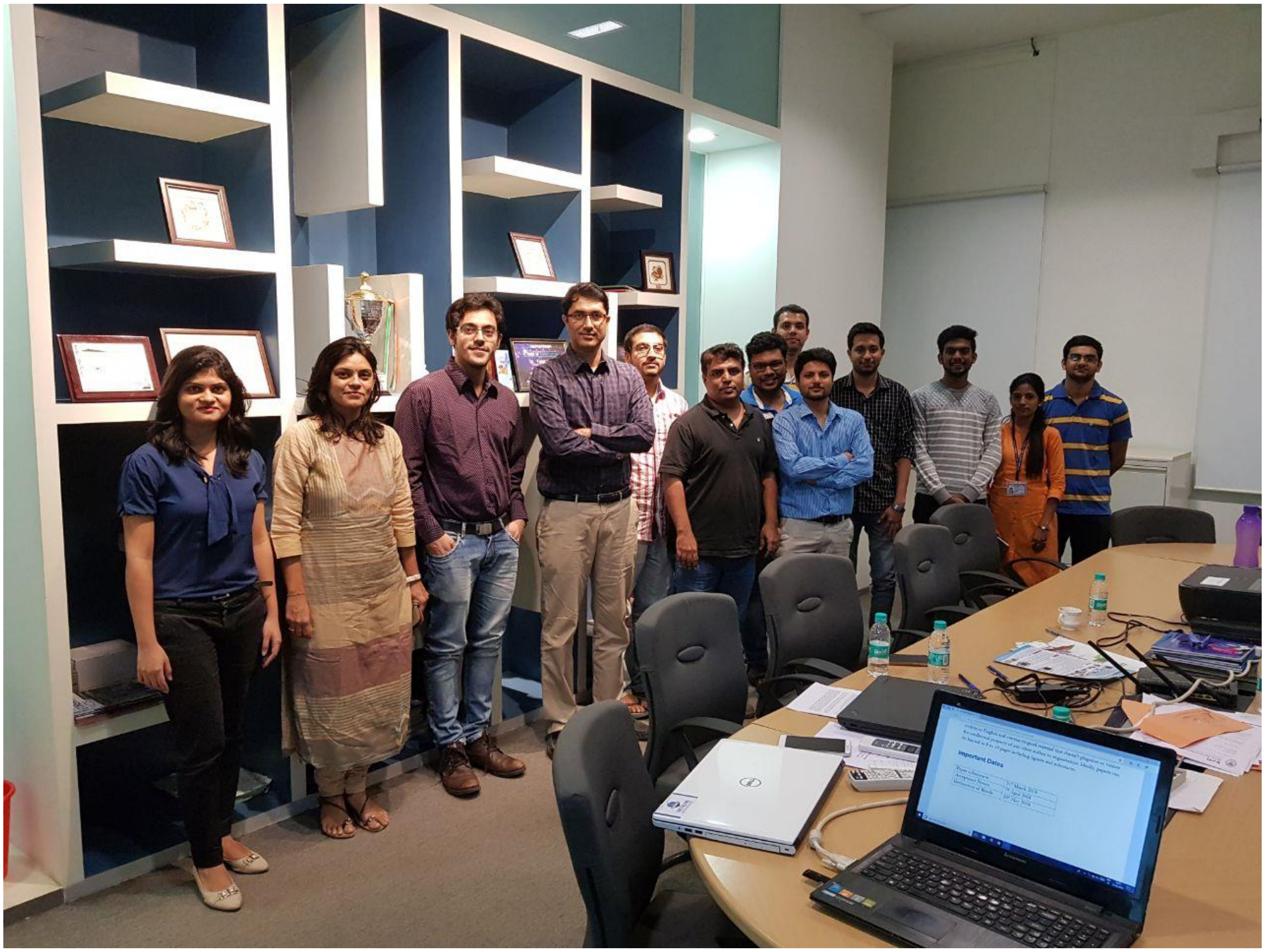
However, smart phones are just one piece of a wide variety of smart objects that are an extension of our cognitive capabilities. As other objects like thermostats, cars etc. turn smart leading to an ecosystem of *Internet of Things* (IoT) wherein they can interconnect with each other, important questions are raised about the legitimacy, privacy and security within the IoT ecosystem. Two of these questions were discussed at the roundtable. A summary of discussion on them is as follows:-

First, how can one control the proliferation of fake devices/users over the IoT ecosystem? Coming up with Open Standards for the same can be a solution to this problem. These open standards can contribute to definition of appropriate authentication mechanisms for identifying fake users/devices by resisting key space searching attacks, protecting authentication credentials, resisting authenticated DOS attacks, instantiating all devices before shipping and disabling unauthenticated devices by default. Restricting fake devices/users coupled with well-defined community driven communication standards will also contribute to overall efforts to combat fake news/protocol calls in the IoT ecosystem. Specifically, The Internet Engineering Task Force (IETF) document for 'Best Current Practices for Securing IoT device' released on July 3,2017 throws light on some of these measures.

Second, how can users influence the governance of IoT driven firms considering that they symbolise new forms of private governance? Most of the participants opined that user centricity should be a key principle that has to be adopted by these IoT driven firms wherein users will have the right and control over their data. Similar to social media platforms like Facebook, safe harbour provisions should protect IoT firms from undesirable activities of their devices/users. In certain cases of critical importance like Smart City projects wherein the impact of IoT ecosystem has the potential to extend to the masses, these firms can be structured on the principles of public benefit corporations.

Apart from this discussion, students were introduced to the ISOC India Mumbai Chapter and the work done by Internet Society for developing open standards for IoT. They were also informed about the IoT Research Paper Competition 2018 organised by Internet Society India Mumbai Chapter and encouraged to participate.

Some photos from the event:-



Prof.(Dr).Kazi, VJTI students and ISOC India Mumbai team volunteers participated in the roundtable discussion. Prof.(Dr). Kazi, Dr. Iqbal and Mr. Sanchit Pathak played a key role in organising the session.