National Security Planning Project

Introduction

There are many tourist spots & "must visit" places on the radar of our weekends. Even places nearby, sometimes become a paradise for people who are stressed out with their daily rituals. Since most of the people living in cities and towns are now connected to the internet all along the day, *Facebook*, *Twitter* & other social platforms are just a click away.

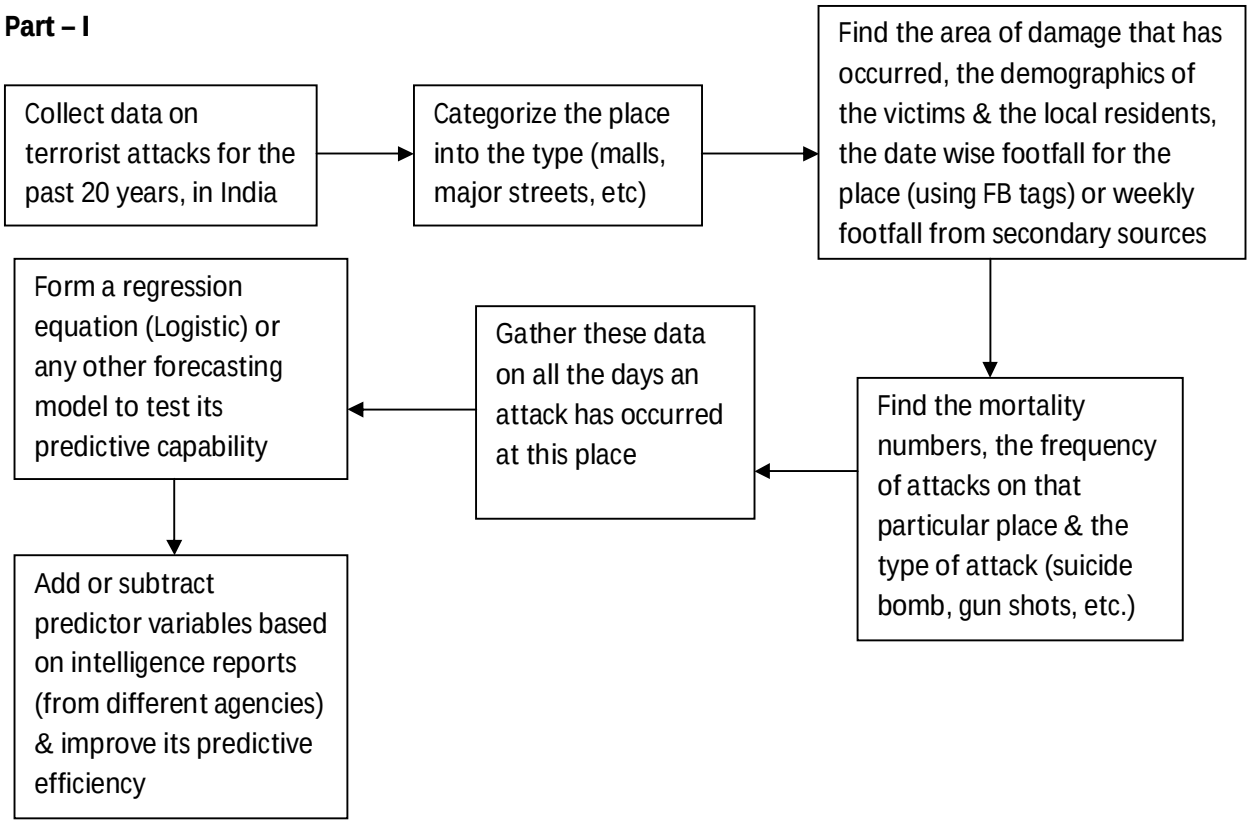
People visit many places & tag them on *Facebook* for their friends to see & talk about it. Those places which they tag are the ones where there is a huge influx of crowd from in and around areas, in most days of the week.

The history of terrorism has always been to attack and affect people's lives on a large scale. The threats to our country, including the recent *Waga* border attack, are sending a clear indication of India becoming the next target for various anti-social outfits. Such being the scenario, the government & its allied special forces are under a great pressure to plan for maximum security at potential attack areas.

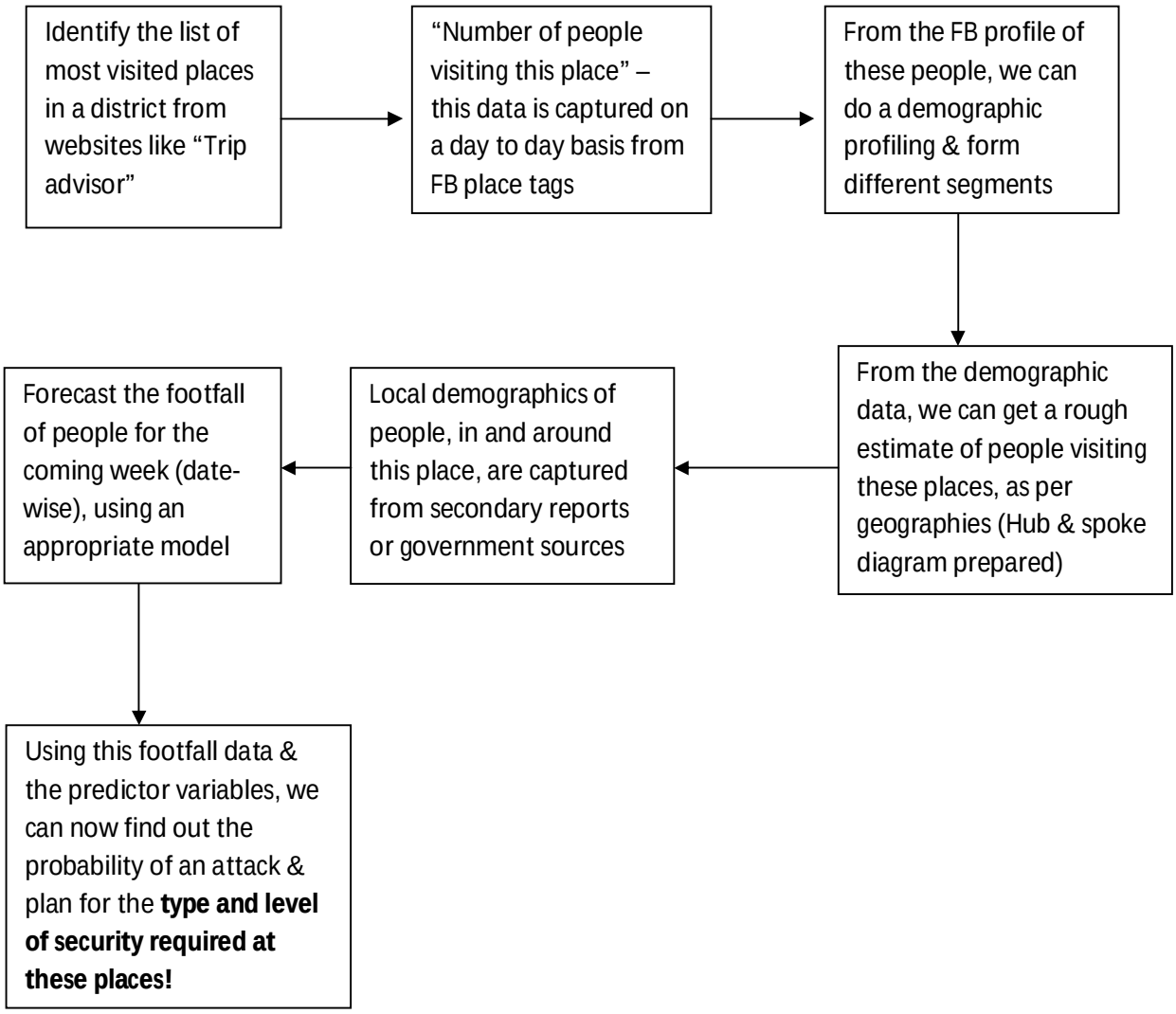
Our application, crunches the data available on ***Facebook*** and ***Twitter*** to see how tagged places can be the next target for terrorists & associates a probability for facing an attack in the next 2 months or a quarter, in these places. This helps the government to plan for an appropriate level of security at all such places, according to the level of attack risk. This data is primarily being extracted with the government's permission and help, as it may sometimes give rise to user privacy issues when done on a private level.

Methodology (Flowchart)

Part – I



Part – II



The basic logic behind the application is that, **we do not know why the terrorist choose a particular attack location, so we are trying to find that out**, using the vast amounts of data we have, in order **to safeguard similar places**.

This model, when used on a continuous basis by the government, security planning will be much more easy and efficient. However, a dedicated team has to be continuously working on improving the model efficiency & testing the authenticity of the data captured.

Let's prevent the attack before it happens!