The Internet of Things has arrived and it’s going to introduce incredible opportunity over the next five years. And while smart things are exactly that, the IoT industry has a long way to go in terms of overall security. Many of today’s IoT devices are rushed to market with little consideration for basic security and privacy protections: “Insecurity by design.”

This puts you and everyone else at risk: from unwittingly being spied on or having your data compromised to being unable to lock your own home. You could even become part of a botnet that attacks the Internet. Your insecure webcam – along with millions of others – could be used to attack the power grid of an entire country.

From dental sensors that can monitor what a person eats to kitty litters that can track a cat’s every movement, it can be difficult to sort fact from fiction when it comes to the Internet of Things. Can you tell which is real and which is not?

The potential applications of IoT are vast and varied, and its impact is already being felt across a wide range of industries, including manufacturing, transportation, healthcare, and agriculture. As the number of internet-connected devices continues to grow, IoT is likely to play an increasingly important role in shaping our world. Transforming the way that we live, work, and interact with each other.

In an enterprise context, IoT devices are used to monitor a wide range of parameters such as temperature, humidity, air quality, energy consumption, and machine performance. This data can be analyzed in real time to identify patterns, trends, and anomalies that can help businesses optimize their operations and improve their bottom line.