TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

INTERNET OF THINGS (IoT)

HOW CXOs CAN ENSURE DATA SECURITY IN THE IoT

#Areyoucybersecure

Follow us: @tataadvanced

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

The speed at which we are advancing towards digital transformation is phenomenal. Thousands of IoT devices are hitting the market every day. ***By the end of 2025, there will be more than 75 billion (approximately) Internet of Things (IoT) connected devices worldwide.***

There is no doubt that IoT has generated new opportunities for businesses to deliver significant outcomes, improve the efficiency of products and services, serve customers in a better way, and create new revenue streams. This rising technology possesses tremendous potential to make things even more intelligent and efficient. But while IoT devices are becoming crucial in keeping up with the rapidly evolving market, the business leaders are heedful of the security implications of this novel technology.

With the scale of connected devices, the volume of data and complexity of cybersecurity is also growing over time. For instance, IBM suggests that a smart car can produce approximately 25 GB of data every hour. There is a plethora of such devices that generate heaps of data every single second. Such a sheer quantity of information being produced is unparalleled in computing history. What bothers CIOs and all business stakeholders is how to store the giant blocks of data and ensure the privacy of the stored information.

Gartner's report on IoT & Datacenter says that the main contributing factor behind the increasing demand for more storage capacity is the impact of IoT on storage infrastructure. The research director at Gartner, Fabrizio Biscotti, said that the need for real-time processing of huge volumes of IoT data will increase with time, producing new security and analytics challenges for the datacenters.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

C-Suite executives need to proactively develop new strategies, keeping data storage and security in focus, to deal with the massive IoT data storm. The vice-president at Gartner, Andy Rowsell-Jones also said that CIOs need to evolve their roles alongside the growth of digital businesses and disruptive innovations.

Some of the aspects that could be considered to tackle this threatening data avalanche include:

Decide how you want to store the data

This is the first phase in which you receive data from multiple IoT devices, in both structured and unstructured formats. Now, it's time to decide how to store that data, whether you want to write it to a disk, store on cloud or set up an online instance to process the data.

Classify and categorize the data

Not necessary that each block of data you receive every hour from different devices is worth keeping. It could be possible that the data you're not interested in today might be an insight for tomorrow. So, keeping both things in mind, you need to develop an effective classification system that can group the data immediately as highly important, moderately important or less important. The system must be capable to review your classifications and stay in line with your expectations.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Decide how long you want to keep the data

Once you are done with categorizing the data, the next question that comes to your mind is how long you should retain the data. At some point, you need to make strategies to fix how much old data you want to keep, and what volume of data you would like to archive or move to cloud. You can also define when will you summarize data, it might be at the end of the year or after 5-10 years. This practice will help you keep a track of what you've kept in your data bucket and how valuable it is.

Establishing security protocols

CIOs and all business leaders must develop the skills and competency to overcome the emerging challenges of IoT ecosystems. They should establish security protocols to ensure data authentication and collaborate with manufacturing companies to embed security improvements in smart devices. Such steps will help businesses to thwart malicious activities and will result in safe and secure IoT solutions.

While there are huge benefits of using Internet-connected devices, IoT has its share of risks. There is no doubt that IoT technology makes our life more convenient and hassle-free, but one cannot isolate the possible risks. Businesses must take proactive safety measures to prevent cyberattacks based on this rapidly evolving technology.