TO PROPOSE A MODEL FOR IDENTIFYING SECURITY THREATS ON IOT USING FOG COMPUTING

The swift growth in emerging technologies such as sensors, smart phones, 5G connection and virtual reality leads to innovative applications such as connected industries, smart city, smart energy, smart agriculture etc. IoT has evolved due to the convergence of these multiple technologies. The traditional fields of embedded systems, wireless sensor, control systems, automation as well as real-time analytics, machine learning, commodity sensors etc contribute to enabling the Internet of Things.

As the technology grows the cyber attacks and data breaches were also targets on IoTs. The prospect of interconnectivity among IoT devices makes them vulnerable. It is clearly evident that there are a huge number of vulnerabilities for IoT devices[3]. According to [2], many organizations are exposed to greatest challenges in monitoring network based threats, prominently in the following sectors; government, energy, health care, banks and research centres.

Generally the IoT devices generate immense amount of data that flows through network is at possible risk for network attacks. Further existing tools and techniques are insufficient to detect innovative attacks triggered by cyber criminals due to volume, velocity, and variety of data. Existing mechanisms lack processing at large scales and bigdata analytics have been used to analyze and correlate security related data efficiently.

There are some solutions suggested by different authors. Most existing literature separately focus on deep learning, bigdata and IoT security. Many studies failed to consider the impact of volume, velocity veracity and variety of days generated by IoT devices. Hence inclusion of bigdata technology become mandatory to address the impact of V's.

But, there is a solution suggested by [1] to employ deep learning and big data technologies together to strengthen security of IoT devices. [1] have suggested a novel frame work for IoT security based on deep learning and bigdata technologies. Due to the limitation of storage in IoT devices leads to the storage of bigdata on cloud. The limitation of storage on cloud is the latency of data.

In this context I propose a model to analyze the existing threats happend in the past to suggest the vulnerabilities. To resolve the issue of latency, fog computing technologies can also be suggested.

REFERENCES

[1] M.A. Amanullah, R.A.A. Habeeb, F.H. Nasaruddin et al., Deep learning
and big data technologies for IoT security, Computer Communications (2020), doi:
https://doi.org/10.1016/j.comcom.2020.01.016.

[2] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, M. Imran, Real-time big
data processing for anomaly detection: A survey, International Journal of Information Management
45 (2019) 289–307.

[3] New trends in the world of IoT threats, accessed on May 10, 2019.
URL https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/