Using Analytics and Half-Space Trees for Real-Time Threat Detection

In times of rapid digital evolution, I will present you today how you can prepare your business with an IoT cyber security use case for the threats of tomorrow. There is no doubt that IoT will be a critical success factor for many companies. Internet of Things (IoT) services and implementations are growing drastically and steadily to reach again an all-time of available sophisticated analytics, service deployments, and IoT applications:

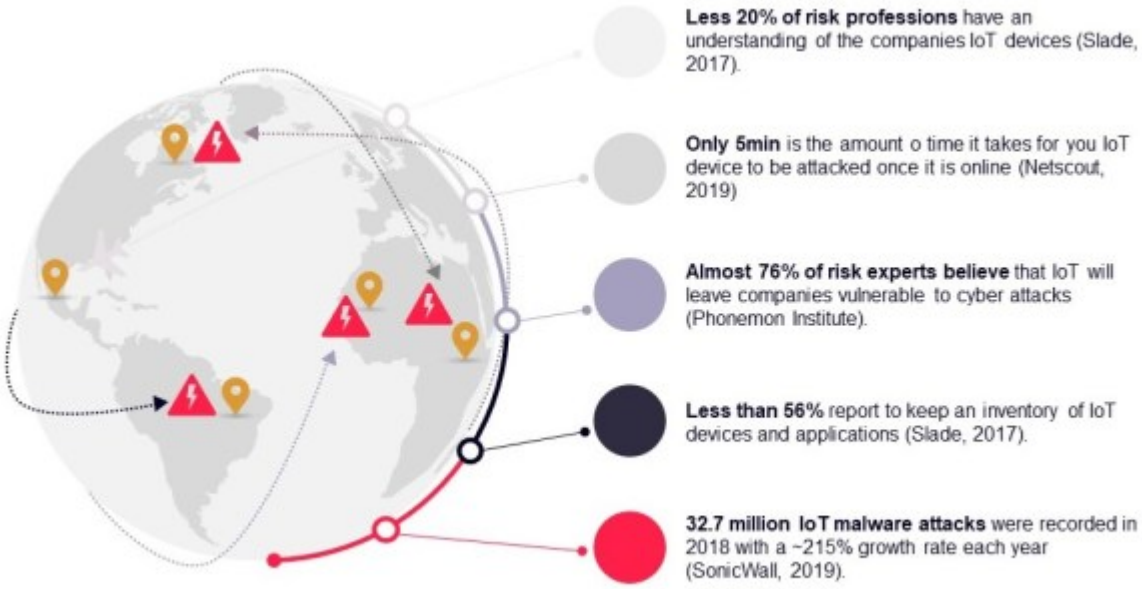
- Fortune Business Insights anticipates the IoT devices markets to reach **$1.1 trillion by 2026** (Fortune Business Insights, 2019).
- Gartner reports that there are **14.2 billion connected IoT devices** in use in 2019 already (Gartner, 2018).
- According to a Forbes Insights survey, **58% of financial executives** report having well-developed IoT initiatives (Forbes, 2018).
- **Already 80%** of the organizations report that they are achieving **better results with the IoT initiatives** than initially estimated according to Gartner (Gartner, 2018).

The pace of global IoT growth is tremendous, but it leaves a critical and very important key vulnerability unanswered: how safe and reliable are the IoT applications? What is the IoT cyber security use case? How do we make sure that all IoT applications fulfill their functions as expected? Within an IoT-system, if a small part performs differently than expected or has been hacked, it can have devastating consequences for the whole system.

Table of Contents

The Problem: Lacking real-time monitoring puts all your IoT-initiatives

at danger



IoT cyber security threats

Lack of security systems to monitor your IoT applications leaves your organization exposed to substantial financial and reputational risks, where a small failure within the system can lead to the whole system reacting in unexpected ways. Among classical cyber security problems like intrusion in the system and denial-of-service (DoS) attacks, there are also simple internal failures of the system that occur unexpectedly like software bugs and hardware failures.

In conclusion, lack of security means that you cannot ensure performance as well as reliability of your IoT applications and that you also miss out on an opportunity to learn from the past by applying analytics to your IoT environment. This keeps your IoT-initiatives at high risk and will keep them from unleashing the full potential.

The IoT Cyber Security Use Case: >99% detection rate with half-space tree algorithms

Two researchers from Berlin, Witzig & Gulenko, have investigated how real-time monitoring can be applied to the new emerging and challenging fields of Internet of Things applications and found a simple but powerful method for monitoring. In particular, they have

investigated how half-space tree algorithms can be used to implement such reliability checks and detect abnormal behavior in the context of IoT in real-time so that preventive measures can be applied. Their research reveals an interesting IoT and cyber security use case.

In their study, they test their approach on a real-world IoT-example and achieve impressive results using the unsupervised method: **the detection rate of dangerous behaviors was as high as 99,4% with a less than 3% false alarms.**

The Solution: Real-time abnormality detection with minimal resources

In computer science and machine learning, half-space tree learning is an algorithm that computes a decision tree form pre-existing data to classify certain events in the IoT-environment as “normal” or “abnormal”. There are three key challenges imposed by IoT applications that this algorithm overcomes:

1. **Patterns of interactions of the devices change constantly:** This means that the decision trees have to be constantly adapted and a new tree has to be computed sometimes within a fraction of time.
2. **The detection of abnormal activities has to occur quickly to prevent further consequences in time:** This means that the decision trees are relatively simple, can use real-time data and label IoT behaviors within seconds.
3. **An IoT-gateway offers only minimal resources for computation:** That implies that the algorithm has to be able to achieve good results with minimal computations.

The half-space tree learning algorithm overcomes these three key challenges in the area of IoT cyber security better than other machine learning algorithms such as random forest, neuronal networks or k-means clustering. Therefore, it provides a simple and implementable IoT cyber security use case using modern analytics capabilities.

Conclusion: A novel approach to ensure security in the business context

The approach presented by the two researchers Witzig & Gulenko represents a new way of approaching and tackling security and compliance monitoring problems within the business sphere, which other IoT cyber security use cases cannot provide. It differs from classical monitoring approaches in 4 ways, which contribute to the advantages of the approach:

1) **Unsupervised learning approach instead of a supervised learning approach**

Classical detection approaches follow a supervised learning approach, which uses already labeled data to train the machine learning models first. However, this has several disadvantages in IoT. First, enough labeled data is usually not available to companies. Second, once a model is trained, it cannot adapt to the changing interaction patterns of IoT devices in real-time quickly. The half-space tree algorithm is an unsupervised approach that overcomes these hurdles by giving the application flexibility.

2) Component-level monitoring instead of system-level monitoring

The half-space tree algorithm is implemented for each IoT-device individually, meaning that the computation burden is spread across all IoT-devices and the trees can be tailored to the individual IoT device. Compared to system-level monitoring, where there is a central monitoring instance surveilling the interaction of devices, the component-level approach makes the detection faster, accurate and easier to scale. While a system-level center reaches it is computational limits fast, a component-level approach can scale up and scale down with your amount of IoT devices without problems.

3) Accountability instead of black-box predictions

Half-space trees are simple algorithms that can be very easily interpreted and understood. Even for simple business clerks, it is easy to understand how abnormal behaviors are detected. While classical machine learning approaches lose the “explainability” of their predictions, half-space trees can be easily understood and investigated. This increases user acceptance enables you to learn from the trees and always provides you with accountability.

4) Generalizability

While other machine learning algorithms are very context-specific, need labeled training data and can sometimes only work with quantitative variables, half-space trees can perfectly work with quantitative and categorical variables without preexisting data. This makes it applicable to many more scenarios.

Referenes

Forbes (2018). How IoT Is Impacting 7 Key Industries Today. Retrieved from https://www.forbes.com/sites/insights-inteliot/2018/08/24/how-iot-is-impacting-7-key-industries-today/#6c72130f1a84.

Fortune Business Insights (2019). Internet of Things (IoT) Market Size, Share and Industry

Analysis By Platform (Device Management, Application Management, Network Management), By Software & Services (Software Solution, Services), By End-Use Industry (BFSI, Retail Governments, Healthcare, Others) And Regional Forecast, 2019 – 2026. Retrieved from https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.

Gartner (2018). Early adopters of IoT are working through the challenges of implementation to deliver compelling business value. Retrieved from https://www.gartner.com/smarterwithgartner/lessons-from-iot-early-adopters/.

Gartner (2018). Gartner Identifies Top 10 Strategic IoT Technologies and Trends. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

Gulenko, A., Schmidt, F. (2019). Unsupervised Anomaly Alerting for IoT-Gateway Monitoring using Adaptive Thresholds and Half-Space Trees.

Netscout (2019.) NETSCOUT Threat Intelligence Report: Dawn of the terrorbit Era. Retrieved from https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf.

Phonemon Institute (2019). Third Party IoT Risk: Companies don’t know what they don’t know. Retrieved from https://sharedassessments.org/2019-iotstudy/.

SonicWall (2019). SonicWall 2019 Mid-Year Threat Report show worldwide malware decrease of 20%, rise in ransomware-as-a-service, IoT attacks and cryptojacking. Retrieved from https://www.sonicwall.com/news/sonicwall-2019-mid-year-threat-report/.

Slade, R. (2017). The Internet of Things (IoT): A New Era of Third-Party Risk. Retrieved from https://sharedassessments.org/the-internet-of-things/.

Share this:

- Click to share on LinkedIn (Opens in new window)
- Click to share on Twitter (Opens in new window)
- Click to share on WhatsApp (Opens in new window)