IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 6, Ser. II (Nov - Dec 2019), PP 42-46
www.iosrjournals.org

IoT Devices Communication Need of Listener for IoT Device Communication

Indrajeet

Abstract
The emergence of IoT *– the networked connection of people, process, data and things – is expected to significantly grow the number of connected devices worldwide, from billions of units we have today, to tens of billions of units expected to be deployed in the coming years as stated by several analysts:*
• IDC1 states that "By 2018, cloud, mobile, and IoT services providers will own/operate 30% of IT assets in edge locations and micro data centers".
*• Prediction is that "By 2020, IoT technology will be in 95% of electronics for new product designs,while**development of listener** needs to be sorted".*
• Forrester recently ranked the Internet of Things the number 1 tech trend from 2018 to 2020.

Date of Submission: 24-12-2019 Date of Acceptance: 07-01-2020

I. Introduction - Security Challenge

There are still plenty of security challenges to be addressed while the market is continuing to massively adopt IoT technologies. IoT Security remains the major concern when deploying IoT solutions. As per prediction by 2022 half of all listener development budgets for IoT will go to fault remediation, recalls and safety failures, rather than on protection. Innovation around IoT security is key to enabling safe and effective IoT adoption. Moreover, the increase of compute capabilities outside of the cloud will bring increased complexity to the "edge": this complexity is by its nature less controlled and more exposed to security threats. There are plenty of entities providing IoT Security services and solutions but there are none covering the overall landscape, especially considering it is such a massive ecosystem with new threats emerging on a daily basis.

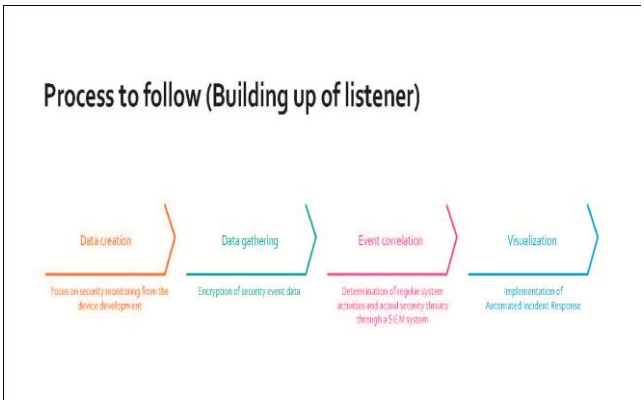
Standardization, centralized orchestration and end-to-end management are core drivers, together with an IoT Security framework that converges security controls from Things, or Edge, up to the backend platforms and all communications in between. Therefore, it is important to obtain a proper understanding of the various categories of IoT Security pain points' in existence today, and what security controls we can put in place to mitigate them.

We first need to define what a "thing" is in terms of IoT.

"Things" in the Internet of Things as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environments. So this gives us a very broad definition of what could be considered a "thing" ranging from temperature sensors to smart plugs to cameras to medical devices up to industrial robots and automobiles (or even discrete parts of these things).

II. Focus On Listener

We need to look at IoT Security &**development of Listener** from both an architectural point of view, as well as from a risk based perspective, in order to concentrate our efforts on those things that are at a higher risk of compromising sensitive data. It is the case with audio/video devices located within meeting rooms or data centres for example and less for those which may be highly vulnerable but would only be capable of leaking the temperature of a part of a building or informing that your toast has burned.



In a world where we have IoT networks everywhere, as in the trucks which transport our merchandise, the machines in a factory which are monitored and controlled and even the household appliances and lights which are IoT enabled, we realize that all of this communication with the IoT has to be controlled somehow(Listener will play an important role). This is where IoT Gateways come into place and concept of Edge Security becomes a major consideration.

Edge communications

IoT Listener will play a major role in the IoT landscape going forward. The reason for their importance is due to the way in which IoT Listener are converging the world of IoT with the traditional infrastructure space, whether this be on premise or in the cloud. Since the large amount of data which are expected to be produced by the IoT sensors, the IoT Listener will also play the role of a data controller, and in this case it should offer the following services:

• Data collection • Data aggregation • Data filtering • Data processing • Data real-time analytics • Data real-time decisions and actions

- IoT Listeners will evolve as well and all the services above might be distributed among different entities in the IoT network, sometimes embedded in Things hence enabling full Machine to Machine communications.
- Security by design and in depth, since much of the data which will be processed could be classed as confidential or could contain sensitive personal information. Encryption techniques are the most suitable to address such requirement.
- Containers which run on different hardware depending on the application, from automotive, to industrial, to power grid measurement systems and residential home control, these gateways need to be upgradable and maintainable with the least possible interaction. Therefore, specifying well defined data providers, **listeners**, actors and interfaces is essential for allowing automated cloud updates and controls. Of course, the software which is loaded onto each device must be hashed, signed and verified ensuring that changes will not be possible via an unauthorized source

IoT Listeners will take a major part in the future infrastructure and applying security in all the layers is essential.

IoT Asset management

Asset management has been a challenge for everyone, even when we are moving towards greater degrees of virtualization. Frequently, every management tool deployed in an environment presents a different number of assets under it, be it an antivirus solution or Vulnerability scanners.

The approach for IoT asset management would ideally be based on the individual device reporting itself to the Asset management tool and every other solution should be integrated with that tool. Several existing well-known message exchange protocols like Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Constrained Application Protocol (CoAP) can be used for asset management of IoT devices.

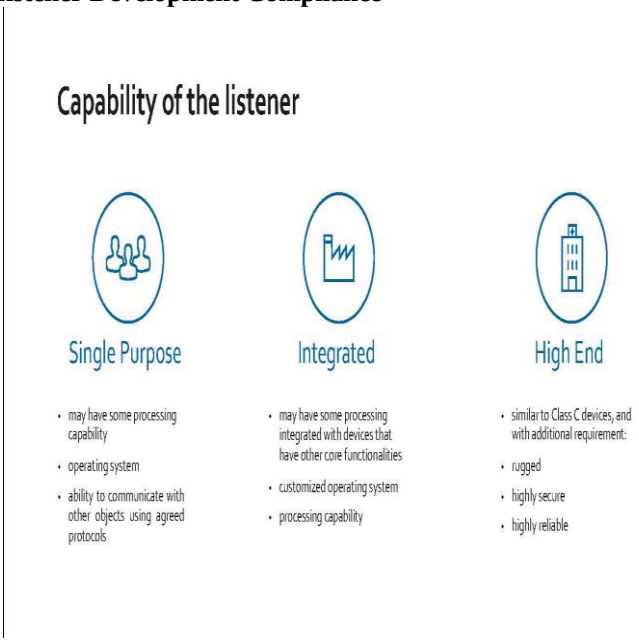
An Exchange protocol should be chosen bearing in mind that they use less data as the potential traffic generated will be enormous.

Another approach is the use of Distributed Ledger Technology in order to identify a device as it reports itself into a management tool. This approach creates new opportunities in managing identities as a homogeneous group, and opens a range of possibilities in the of asset management for IoT.

Devices such as sensors, and individual smart devices, may be feeding their data to a central server, or a monitoring device which may be keeping track of those sensors and individual smart devices. In such cases we can get the data on those devices from that central server or monitoring device.

To address the issue of the additional complexities, and potentially huge data volumes, inherent in IoT devices some new approaches will most likely be required. To this end, we can find interesting solutions like an extended module for Listener development which links their real time and IoT specific information with CMDB functionality.

Vision regarding IoT Listener Development Compliance



In order to effectively manage IoT cyber security compliance, the processes of compliance shall focus on the following domains

1. Business processes
2. Devices and aggregation points such as related gateways/hubs that provide generic part of the connectivity for IoT devices
3. Networking including wired (whether LAN or power supply), and radio connections using short-range, LPWAN and cellular
4. Cloud and server elements as specific to IoT.

Listener principles

Regarding IoT Listener compliance, these basic principles can be considered

: • Everything is connected to everything
• Basic controls still hold as true
• Utilize existing frameworks/guidelines
• Be aware of credential theft techniques, For the certified systems adherent to ISAE 3402, there should be a portfolio of emerging recommendations for IoT forthcoming.

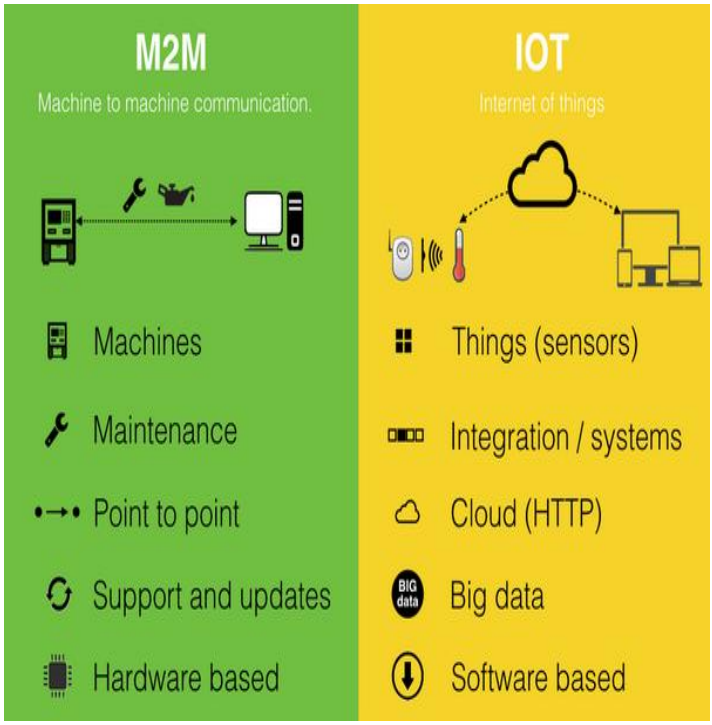
Key Features of Listener

Low Mobility: M2M Devicesdo not move, move infrequently, or move only within a certain region
Time Controlled: Send or receive data only at certain pre-defined periods
Time Tolerant: Data transfer can be delayed
Packet Switched: Network operator to provide packet switched service with or without an MSISDN
Online small Data Transmissions: MTC Devices frequently send or receive small amounts of data.
Monitoring: Not intend to prevent theft or vandalism but provide functionality to detect the events
Low Power Consumption: To improve the ability of the system to efficiently service M2M applications
Location Specific Trigger: Intending to trigger M2M device in a particular area e.g. wake up the device

III. Smart Utility Management

- In the new age of energy efficiency, automation will quickly become the new normal.
- As energy companies look for new ways to automate the metering process, M2M&IoT comes to the rescue, helping energy companies automatically gather energy consumption data, so they can accurately bill customers.

- Smart meters can track how much energy a household or business uses and automatically alert the energy company, which supplants sending out an employee to read the meter or requiring the customer to provide a reading.
- This is even more important as utilities move toward more dynamic pricing models, charging consumers more for energy usage during peak times.

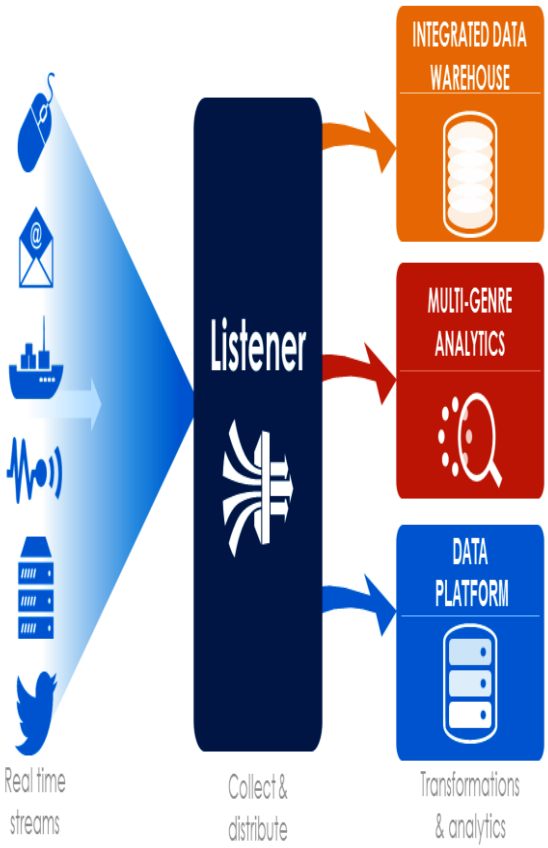


IV. Goals To Achieve

- As part of my goal to continuously challenge the status quo and democratize integration, my focus area will be Listeners, the service, to help out the untapped potential of IoT devices.
- The Listeners will enable devices the events of your IoT devices using the Built.io Flow platform.
- The developed listener will use in-memory sockets to listen to these protocol servers for events and fetch event responses.
- Once the Listener is developed, a dedicated in-memory socket will be created and it starts listening to the specified channel. After this, whenever an event occurs on the channel, the socket sends the event response data in the binary format—which makes it very lightweight and hence, ideal for the IoT devices—to the Built.io Flow server. The Built.io Flow server then uses this data to trigger the workflow.
- It will be simple, fast, secure, and most importantly, requires only a few seconds of time.

Feature of Listener to be designed for Device Communication

- Ensures fast and secure data delivery
- Sends real-time notifications
- Requires minimum user intervention
- No maintenance overhead.



V. Conclusion

- The pace of market adaption is accelerating because the increase in market demand and number of users increasing day by day and more advanced system will be needed in future, by increasing users there will be need to control the traffic which can be eliminate by using M2M along with IoT.
- IoT applications connecting developers and customers the market demand of these products may lead into hybrid products with the combination of two or more technologies together.
- Internet is a big and important media and backbone for communication among devices or things, there are billions of machine and in future those machines will communicate with each other using internet so that the life of human will become more comfortable.
- To achieve good scalability and cope with the upcoming challenges raised by pace of market we need M2M with IoT.

Acknowledgments

This White Paper has been prepared by project team in with a major contribution from the project leader Fraunhofer AISEC.
The project team met four times –and held a number of online conference calls. The project team includes:
Project Manager Dr. Claudia Eckert, Fraunhofer AISEC
Project Partner Dr. Kazuhiko Tsutsumi, Mitsubishi Electric, MSB Member
Mr. Mark Crawford
Krista Grothoff, Fraunhofer AISEC
Mr. Peter Lanctot, IEC, MSB Secretary

Indrajeet. " IoT Devices Communication Need of Listener for IoT Device Communication." IOSR Journal of Computer Engineering (IOSR-JCE) 21.6 (2019): 42-46.