White Paper : Avarana IoT System

Contact : info@agneyas.com

Avarana IoT System

Tailor-made IoT Solution for your Business

Internet of Things (IoT) technology in the context of business systems is the use of sensors and actuators in the value chain of the business processes, collect data and process it along with other information to unlock economic value. IoT plays a critical role in the **digital transformation** of businesses, which is essentially the use of this data collected from sensors and application of Analytics, Machine Learning (ML) and Artificial Intelligence (AI) techniques to automate and optimize the business processes, enhance customer experience or create new business models altogether.

Figure 1 shows the key components of a IoT system.

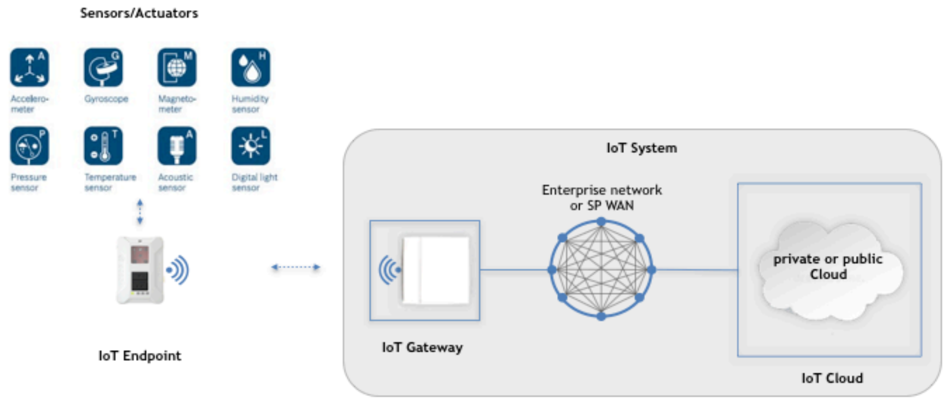

Figure 1. Components of an IoT System

IoT Endpoint: Sensors and actuators attached to a controller together form the IoT endpoints. IoT endpoints have minimal compute capability and some from of wireless connectivity to the nearest gateways or to the cloud directly. They are responsible for reading signals from the attached sensors, process and send it to the gateways as well as receive control instructions from the gateway and converting them into appropriate signals on the attached actuators.

IoT gateways aggregate many such IoT endpoints and provide secure connectivity to the backend IoT cloud (described below). In addition, they provide compute power close to these IoT endpoints capable of edge services and data transformation/ingestion into the data pipeline towards the IoT cloud.

IoT Cloud is the backbone of IoT system and provides modern cloud capabilities such as elastic compute, orchestration, scalability, resiliency and load balancing infrastructure for the service workloads (micro-services) as well as applications . Its also the central repository for the data pipeline and provides for event processing and data storage for both real time and offline applications. In addition, a monitoring and control infrastructure resides in the IoT cloud to collect and process relevant system data for the system.

Other main components of IoT system include a **connectivity** infrastructure to reliably and securely connect the gateways to the IoT cloud, a **manageability** solution that includes User interfaces (UI) and Application program interfaces (API) to configure and manage various system components and a **security** framework that ensures access control, authentication and protection for the data in motion and at rest.

So what are the pain points ? One can clearly see that, a typical IoT solution involves diverse software and system components which are provided by different players in the industry. While some of these components are still evolving, the main challenges of planning and implementing a IoT solution pointed to by different surveys are as follows :

Security & Privacy tops the list of many customer surveys and involves authentication of endpoints, securing data in transit through the data network and data at rest in the cloud repositories. Its important to have a consistent implementation of security policies across the different components. Isolation of IoT traffic and keeping it private will help in reducing the attack surface atleast during the initial implementation phases to protect existing network from vulnerabilities.

Implementation Complexity is another pain point to customer especially who are not technology savvy. As mentioned earlier, getting various components to work together in itself involves ***integration complexity***. ***Technology skills*** spanning endpoint devices, connectivity and all the way to cloud native applications involving AI/ML is another. As one can see there is no one solution can fit all the requirements. ***Customisation*** of the software components to suit the business needs becomes important.

Cost-benefit Analysis plays a critical role as well. While a few example use cases may look appealing, identifying proper use cases in the context of business, prioritising and funding them requires a careful cost-benefit analysis. In most cases, this would require both the solution domain and business domain experts to sit together and chart out the details. Business model of the offering often plays a role in making this viable to start with. Typical offering is a platform as a service (PaaS) or Software as a service (SaaS) where a standard set of services is offered as software solution running on the cloud and is charged based on tenure and/or usage. While there may be support for initial solution development using the existing software stack and functions, there is little or no engagement and support for identifying and customising platform components for business specific needs.

What is our solution ? Avarana IoT System is an offering from Agneyas Labs, that addresses all of the pain points mentioned above and provides an ***ultra-secure*** and ***tailor-made*** IoT solution using fully ***customisable*** open source components and a standard programming environment. We also engage with customers through the development phase all the way till they are fully comfortable operating the system on their own. The system is licensed based on the usage and the entire intellectual property (IP) rights of the developed solution would lie with the customer.

How does Avarana IoT system work ? Avarana IoT consists of a gateway component (Avarana Gateway or AVAG) and a cloud component (Avarana Server or AVAS) as shown in the figure 2. One or more IoT endpoints are connected to a IoT Gateway and multiple such IoT Gateways are connected to the Avarana IoT Cloud using secured tunnels.

Avarana IoT Gateway: The Avarana IoT system as whole is designed in such a way that Avarana IoT Gateway works as an extension of Avarana IoT Cloud and the entire IoT system can be managed as one unit. This has several advantages.

In addition to manageability as one unit, the cloud internal network is extended all the way to the IoT endpoints. This works as a strong security mechanism as the entire system addresses remain private. In addition, Avarana IoT Gateway authenticates each device on receiving connection request and installs security ACL to allow the device to access only the

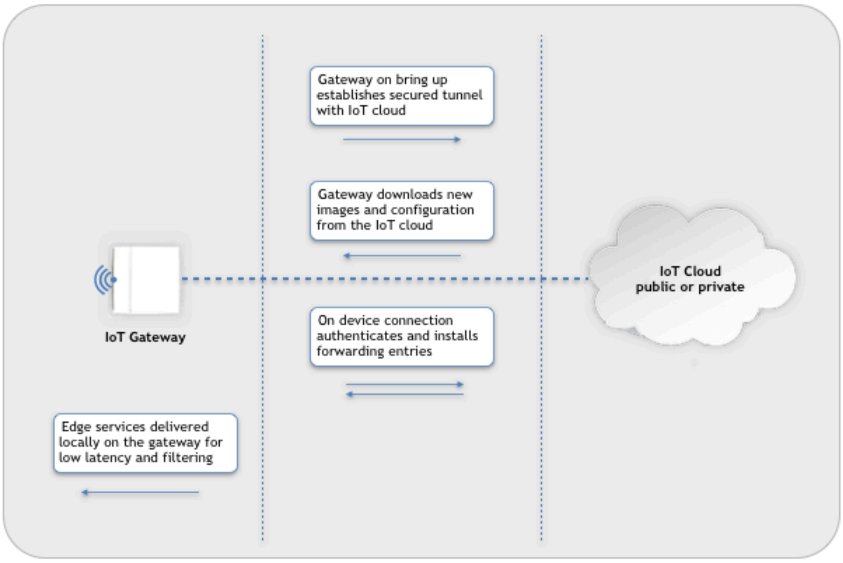
Gateway on bring up establishes secured tunnel with IoT cloud
Gateway downloads new images and configuration from the IoT cloud
IoT Gateway
IoT Cloud public or private
On device connection authenticates and installs forwarding entries
Edge services delivered locally on the gateway for low latency and filtering

Figure 2. Functions of Avarana IoT Gateway

authorised services. Service mapping is also simplified as the endpoints are in the same networking domain.

Avarana IoT gateway also supports deploying Edge Service on the gateway computing system. This can provide low-latency compute services to the endpoints. This can also be used to reduce or contain overall traffic towards the cloud simplifying cloud services. For instance, a protocol translator implemented as part of the edge service frees cloud processing from supporting multiple protocols. A filtering policy installed in the gateway, for instance, can drop insignificant traffic going towards cloud.

Avarana IoT Cloud has all the ingredients of a modern cloud including distributed and elastic compute, distributed event processing and a reliable and distributed storage as shown in figure 3.

Avarana IoT cloud follows a micro-services based architecture and uses Docker® containers and Kubernetes® container orchestrator to create an agile, elastic, efficient and highly available compute infrastructure. A distributed stream processing engine based on Kafka® is the central hub for all the data coming from IoT endpoints, gateways or elsewhere in the system. A distributed storage infrastructure shared among the Kubernetes cluster nodes stores data reliably and efficiently for system and application purposes. Applications

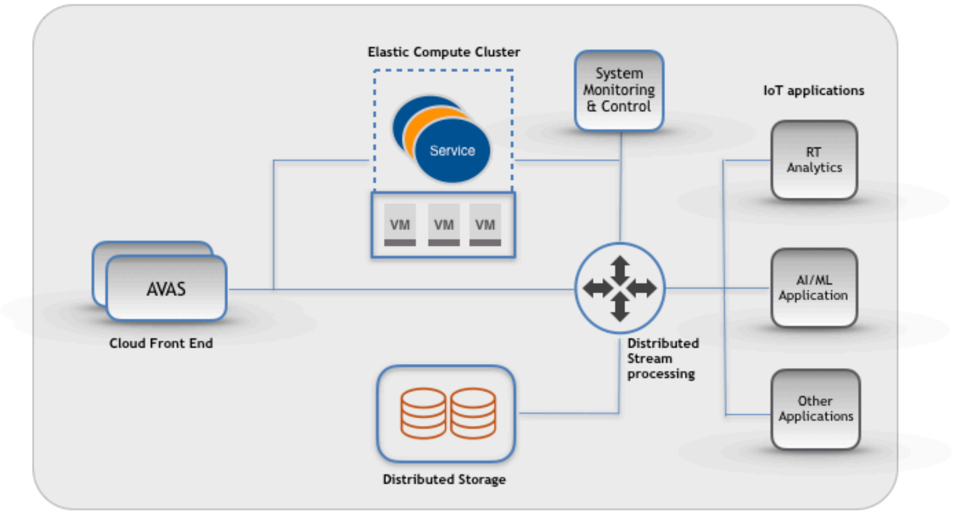

Figure 3. Avarana IoT Cloud

tap into the data stream coming from device partitions in the Kafka and use it for deriving useful information and in turn control the IoT endpoints or any other business assets.

Avarana deployment workflow is designed to simplify deployment and management of IoT services and applications.

A **Service** in Avarana IoT system is a program, packaged in a container, that receives and processes data from a IoT endpoint. A significant aspect of Services is that they can be deployed either on the IoT cloud or on the gateway system. The objective here is to develop services as functions or programs which are specific to endpoints. So, closer they are to the endpoints lower the latency of accessing their service. Services can be created from a program or a function (function as a service) using one click deployment as shown in the figure 4. Services can also be created from a docker images.

When deployed with program or function as input, the deployment workflow automates the entire process of building the program/function using the appropriate language libraries and OS environment into a docker image and inserts that into Kubernetes cluster. The programming environment assumes no knowledge of docker or Kubernetes cluster and our goal is to make it as simple as writing client-server programs on a unix server.

Services works with the data stream from the endpoints on the one hand and as such can provide a low-latency request-response service compared to going to the cloud. They can also publish the transformed data to the Kafka stream engine in the cloud making the data stream available to the applications. Typical use of services include protocol translation, data transformation and data ingestion into the Kafka pipeline.

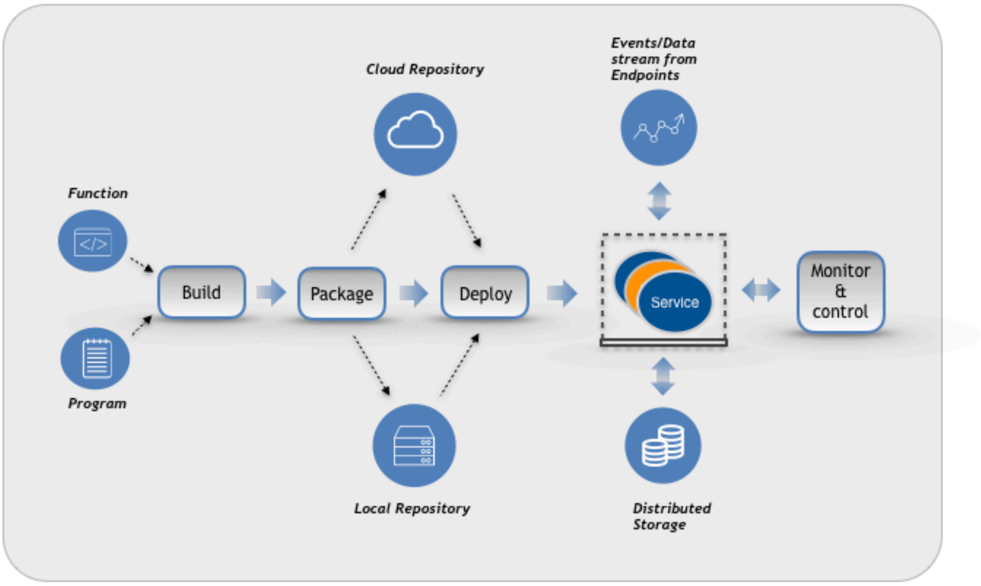

Figure 4. Avarana Deployment Workflow

Applications in the Avarana IoT cloud are programs that work with the data stream from Kafka, make sense of it and applies domain specific knowledge and arrive at a set of actions to be performed on the endpoints or other system components. While Avarana services typically work with a single type of endpoint, Avarana applications can tap into multiple endpoint data streams from Kafka apply other information such as AI/ML database to solve a domain specific problems. For instance, data from a motion detector sensor and a camera feed could be used along with location information to decide if there is a security threat in the building.

Figure 5 shows how the **Avarana Data Pipeline** uniquely combines the power of **services** and **applications** to build comprehensive end to end IoT solutions.

While there are a few built-in services and applications to solve some common needs, users can develop new services and applications in their own familiar programming environments and deploy them in Avarana IoT system with a click of a button or a single command.

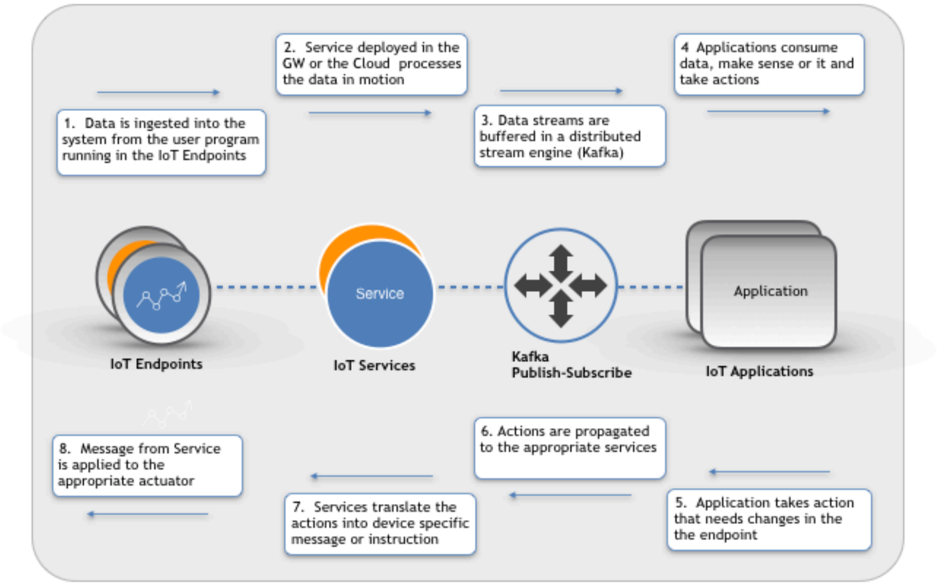
1. Data is ingested into the system from the user program running in the IoT Endpoints
2. Service deployed in the GW or the Cloud processes the data in motion
3. Data streams are buffered in a distributed stream engine (Kafka)
4 Applications consume data, make sense or it and take actions
IoT Endpoints
Service
IoT Services
Kafka
Publish-Subscribe
Application
IoT Applications
8. Message from Service is applied to the appropriate actuator
7. Services translate the actions into device specific message or instruction
6. Actions are propagated to the appropriate services
5. Application takes action that needs changes in the the endpoint

Figure 5. Avarana IoT Data Pipeline

Use cases are key to demonstrate the capabilities of any IoT system. In the last few weeks we have been working on the following real-world problems and are making progress towards a successful deployment of solutions working along side the customers.

Use case 1 : Air Quality Monitoring & Data Access Platform Ever increasing air pollution in major cities in India is a health hazard for people living in those areas. A reliable approach to collecting and analysing the data from various points in the city is essential in finding a solution to this menace. Until recently, the sensor equipment to measure all the major parameters used to be bit expensive (upwards of USD 20K per analyser for each parameter). However, recent advances in so called smart sensors which are available at much cheaper price (in the range of USD 2K-3K). Though their accuracy is not up to the mark compared with the analysers, it can be addressed using modern modelling techniques (Machine Learning algorithms) to a great extent.

These smart sensors are especially relevant in smart cities context and their use is likely to increase rapidly in the coming years due to new smart cities initiatives world over. A scalable platform for connecting 1000's of these smart sensors and providing a modern, scalable cloud based platform is a compelling requirement to achieve this. We are working with partner companies to build one such platform using Avarana framework and other computing and visualisation tools.

Use case 2 : Fraud Detection at the Bank ATMs. Finance sector is one of the most dynamic sectors in any national economy. India, for instance, has been witnessing tremendous growth in rural finance and banking industry. This resulted in proliferation of bank ATMs and associated fraud. Banks are spending tons of money to procure systems that can detect these frauds early enough to prevent them from happening. While most of the solutions are focused on analytical techniques, off late, some AI systems are coming to the fore that make use of video clips from the ATM centres and process them in real-time to predict any fraud occurrence using the behavioural patterns of the user of ATM and correlating that with other information that is involved in the transaction. The challenge here for cloud based solutions is to stream the video and do real-time analytics. Avarana IoT system with its edge processing capability can be deployed to process the video in real-time at the gateway installed in the ATM centre and any suspicious activity alone can be reported to the cloud using compressed video stream where more elaborate checks could be employed.

www.agneyas.com