Internet of Things - Unit 2

· Network functions virtualization infrastructure (NFVI) is the totality of all hardware and software components that build the environment where VNFs are deployed. The NFV infrastructure can span several locations. The network providing connectivity between these locations is considered as part of the NFV infrastructure.

· Network functions virtualization management architectural framework (NFV-MANO Architectural Framework) is the collection of all functional blocks, data repositories used by these blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs.

Software defined networking (SDN) and Network Virtualization (NV):

· It is two of the most prominent technologies to serve as key enablers for the IoT networks of the near future. The main idea behind SDN is to separate the control plane (where the logical procedures supporting the networking protocols are executed and all the relevant decisions are taken) from the data plane (where the forwarding of packets on the most suitable interface towards the intended destination is executed).

· The main entity behind this separation is the controller, which communicates with the network applications through the so-called northbound interface and translates their requirements into appropriate network decisions. The controller also communicates with the network switches that forward packets according to the controller-installed rules. This way, SDN provides increased possibilities to smartly route traffic, for example to balance the load over the network or to exploit underutilized network resources in an optimal way, thereby alleviating the burden on the network by the data onslaught of IoT.

· The term network virtualization concerns a network that allows multiple service providers to form multiple separate and isolated virtual networks by sharing physical resources provided by one or more different physical network infrastructure providers.SDN (software defined networking) is another element that works in combination with NFV while creating IoT network infrastructure. NFV in combination with SDN enable network to utilize distributed intelligence capacity to analyze and manage traffic flows across the network. NFV enables SPs to assemble and provide cost effective and secure IoT networks along with ISV partners. The complexity part can be handled with effective implementation of NFV capabilities with IoT network.

Relevance of NFV in IoT System-NFV can play a crucial role in achieving the goal with IoT network combining both hardware and software network features in a single virtual network. NFV helps accelerate the deployment of new services, operations, and

maintenance of a network allowing high level of network optimization. It brings multiples benefits to service operators and service providers including ROI. The relevance of NFV lies with the promise of benefits across network architecture.

NFV to Enhance IoT Networking Capacity-NFV leverages couple of IT technologies to build flexible and agile IoT network such as virtualization, standard servers, and open software. It distributes intelligence throughout the IoT network enabling real time analytics and business intelligence. NFV creates menu for virtual network functions (VNFs) that includes gateways, mobile core, deep packet inspection (DPI), security, routing, and traffic management that helps delivering customized network services for IoT. Conversely IoT drives NFV opportunity for service providers too financially and technologically.

Data storage in IOT-The Internet of Things is creating an enormous amount of data. To manage, access, and make use of this data, digital storage becomes a critical factor. Data management is a broad concept referring to the architectures, practices, and procedures for proper management of the data lifecycle needs of a certain system. In the context of IoT, data management should act as a layer between the objects and devices generating the data and the applications accessing the data for analysis purposes and services. The devices themselves can be arranged into subsystems or subspaces with autonomous governance and internal hierarchical management. The functionality and data provided by these

subsystems is to be made available to the IoT network, depending on the level of privacy desired by the subsystem owners.

· IoT data has distinctive characteristics that make traditional relational-based database management an obsolete solution. A massive volume of heterogeneous, streaming and geographically-dispersed real-time data will be created by millions of diverse devices periodically sending observations about certain monitored phenomena or reporting the occurrence of certain or abnormal events of interest .

· Periodic observations are most demanding in terms of communication overhead and storage due to their streaming and continuous nature, while events present time-strain with end-to-end response times depending on the urgency of the response required for the event. Furthermore, there is metadata that describes “Things” in addition to the data that is generated by “Things”; object identification, location, processes and services provided are an example of such data. IoT data will statically reside in fixed- or flexible-schema databases and roam the network from dynamic and mobile objects to concentration storage points. This will continue until it reaches centralized data stores. Communication, storage and process will thus be defining factors in the design of data management solutions for IoT.

· A data management framework for IoT is presented that incorporates a layered, data-centric, and federated paradigm to join the independent IoT subsystems in an adaptable, flexible, and seamless data network. In this framework, the “Things” layer is

composed of all entities and subsystems that can generate data. Raw data, or simple aggregates, are then transported via a communications layer to data repositories. These data repositories are either owned by organizations or public, and they can be located at specialized servers or on the cloud. Organizations or individual users have access to these repositories via query and federation layers that process queries and analysis tasks, decide which repositories hold the needed data, and negotiate participation to acquire the data. In addition, real-time or context-aware queries are handled through the federation layer via

.

· a sources layer that seamlessly handles the discovery and engagement of data sources. The whole framework therefore allows a two-way publishing and querying of data. This allows the system to respond to the immediate data and processing requests of the end users and provides archival capabilities for later long-term analysis and exploration of value-added trends.

IOT Data Management-Traditional data management systems handle the storage, retrieval, and update of elementary data items, records and files. In the context of IoT, data management systems must summarize data online while providing storage, logging, and auditing facilities for offline analysis. This expands the concept of data management from offline storage, query processing, and transaction management operations into online-offline communication/storage dual operations. We first define the data lifecycle within the context of IoT and then outline the energy consumption profile for each of the phases in order to have a better understanding of IoT data management.

IOT Data Lifecycle-The lifecycle of data within an IoT system proceeds from data production to aggregation, transfer, optional filtering and preprocessing, and finally to storage and archiving. Querying and analysis are the end points that initiate (request) and consume data production, but data production can be set to be pushed to the IoT consuming services. Production, collection, aggregation, filtering, and some basic querying and preliminary processing functionalities are considered online, communication- intensive operations. Intensive preprocessing, long-term storage and archival and in-depth processing/analysis are considered offline storage-intensive operations.

is a known procedure in data mining called data cleaning. Schema integration does not imply brute- force fitting of all the data into a fixed relational (tables) schema, but rather a more abstract definition of a consistent way to access the data without having to customize access for each source's data format(s). Probabilities at different levels in the schema may be added at this phase to IoT data items in order to handle uncertainty that may be present in data or to deal with the lack of trust that may exist in data sources.

· **Storage/Update—Archiving:** This phase handles the efficient storage and organization of data as well as the continuous update of data with new information as it becomes available. Archiving refers to the offline long-term storage of data that is not immediately needed for the system's ongoing operations. The core of centralized storage is the deployment of storage structures that adapt to the various data types and the frequency of data capture. Relational database management systems are a popular choice that involves the organization of data into a table schema with predefined interrelationships and metadata for efficient retrieval at later stages. NoSQL key-value stores are gaining popularity as storage technologies for their support of big data storage with no reliance on relational schema or strong consistency requirements typical of relational database systems. Storage can also be decentralized for autonomous IoT systems, where data is kept at the objects that generate it and is not sent up the system. However, due to the limited capabilities of such objects, storage capacity remains limited in comparison to the centralized storage model.

· **Processing/Analysis:** This phase involves the ongoing retrieval and analysis operations performed and stored and archived data in order to gain insights into historical data and predict future trends, or to detect abnormalities in the data that may trigger further investigation or action. Task-specific preprocessing may be needed to filter and clean data before meaningful operations take place. When an IoT subsystem is autonomous and does not require permanent storage of its data, but rather keeps the processing and storage in the network, then in-network processing may be performed in response to real-time or localized queries.

Data Management Framework for IOT-Most of the current data management proposals are targeted to WSNs, which are only a subset of the global IoT space, and therefore do not explicitly address the more sophisticated architectural characteristics of IoT.

· WSNs are a mature networking paradigm whose data management solutions revolve mainly around in-network data processing and optimization. Sensors are mostly of stationary, resource- constrained nature, which does not facilitate sophisticated analysis and services.

· The main focus in WSN-based data management solutions is to harvest real-time data promptly for quick decision making, with limited permanent storage capacities for long-term usage. This represents only a subset of the more versatile IoT system, which aims at harnessing the data available from a variety of sources; stationary and mobile, smart and embedded, resource- constrained and resource-rich, real-time and archival.

· The main focus of IoT-based data management therefore extends the provisions made for WSNs to add provisions of a seamless way to tap into the volumes of heterogeneous data in order to find interesting global patterns and strategic opportunities.

IOT Cloud Based Services-As these devices start to become connected, we need a place to send, store, and process all of the information. Setting up your own in-house system isn't practical anymore. The cost of maintaining, upgrading and securing a system is just too high, and there are some great services available.

· **Amazon Web Services IOT Platform-**Amazon dominates the consumer cloud market. They were the first to really turn cloud computing into a commodity way back in 2004. "ince then they've put a lot effort into innovation and building features, and probably have the most comprehensive set of tools available.

Unit -2

Topics to be covered

Machine-to-machine (M2M), SDN (software defined networking) and NFV (network function virtualization) for IOT, data storage in IOT, IOT Cloud Based Services.

Machine-to-machine (M2M)

· Machine to machine (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. M2M communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor when a particular item is running low. M2M communication is an important aspect of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and telemedicine.

.

It forms the basis for a concept known as the Internet of Things (IoT). Key components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link and autonomic computing software programmed to help a networked device interpret data and make decisions. The most well-known type of M2M communication is telemetry, which has been used since the early part of the last century to transmit operational data. Pioneers in telemetric first used telephone lines and later, on radio waves -- to transmit performance measurements gathered from monitoring instruments in remote locations. The Internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday use in products like home heating units, electric meters and Internet-connected appliances. Products built with M2M communication capabilities are often marketed to end users as being smart.

Fig. 2.1 M2M Communication

SDN (software defined networking)-SDN deployment will enable Internet of Things devices to share network resources efficiently and reliably, and further cut hardware investment, but the possibilities are still emerging. Software-defined networking will meet the Internet of Things (IoT) at the crossroads of VPN exhaustion, uptime challenges and limited network resources. The expected result is that SDN will help drive the expansion of IoT-enabled devices, enable more efficient network resource sharing and improve IoT service-level agreements (SLAs).

SDN Benefits-SDN brings three important capabilities to IoT:

· Centralization of control through software that has complete knowledge of the network, enabling automated, policy-based control of even massive, complex networks. Given the huge potential scale of IoT environments, SDN is critical in making them simple to manage.

· Abstraction of the details of the many devices and protocols in the network, allowing IoT applications to access data, enable analytics and control the devices, and add new sensors and network control devices, without exposing the details of the underlying infrastructure. SDN simplifies the creation, deployment and ongoing management of the IoT devices and the applications that benefit from them.

· The flexibility to tune the components within the IoT (and manage where data is stored and analyzed) to continually maximize performance and security as business needs and data flows change. IoT environments are inherently dispersed with many end devices and edge computing. As a result, the network is even more critical than in standard application environments. “DN’s ability to dynamically change network behavior based on new traffic patterns, security incidents and policy changes will enable IoT environments to deliver on their promise.

Features of SDN-

· SDN will make it easier to find and fight security threats through the improved visibility they provide into network traffic right to the edge of the network. They also make it easy to apply automated policies to redirect suspicious traffic to, for example, a honey net where it can be safely examined. By making networking management less complex, SDN allows IT to set and enforce more segmented access controls.SDN can provide a dynamic, intelligent self-learning layered model of security that provides walls within walls and ensures people can only change the configuration of the devices they're authorized to "touch." This is far more useful than the traditional "wall" around the perimeter of the network, which won't work with the IoT because of its size and the fact the enemy is often inside the firewall, in the form of unauthorized actors updating firmware on unprotected devices.

· SDN will allow IT to effectively program the network to make automatic, real-time decisions about traffic flow. They will allow the analysis of not only sensor data, but data about the health of the network, to be analyzed close to the network edge to give IT the information it needs to prevent traffic jams and security risks. The centralized configuration and management of the network, and the abstraction of network devices, also makes it far easier to manage applications that run on the edge of the IoT.

· For example, SDN will allow IT to fine-tune data aggregation, so data that is less critical is held at the edge and not transmitted to core systems until it won't slow critical application traffic. This edge computing can also perform fast, local analysis and speed the results to the network core if the analysis indicates an urgent situation, such as the impending failure of a jet engine.

NFV (network function virtualization) for IOT-

· Utilizing NFV (network function virtualization) capabilities is one way to address the IoT network challenges providing secure network resources for IoT. Network functions virtualization (also Network function virtualization or NFV) is a network architecture concept that uses the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create communication services.

· NFV relies upon, but differs from, traditional server-virtualization techniques, such as those used in enterprise IT. A virtualized network function, or VNF, may consist of one or more virtual machines running different software and processes, on top of standard high-volume servers, switches and storage devices, or even cloud computing infrastructure, instead of having custom hardware appliances for each network function.

· For example, a virtual session border controller could be deployed to protect a network without the typical cost and complexity of obtaining and installing physical network protection units. Other examples of NFV include virtualized load balancers, firewalls, intrusion detection devices and WAN accelerators.

The NFV framework consists of three main components-

· Virtualized network functions (VNFs) are software implementations of network functions that can be deployed on a network functions virtualization infrastructure (NFVI).

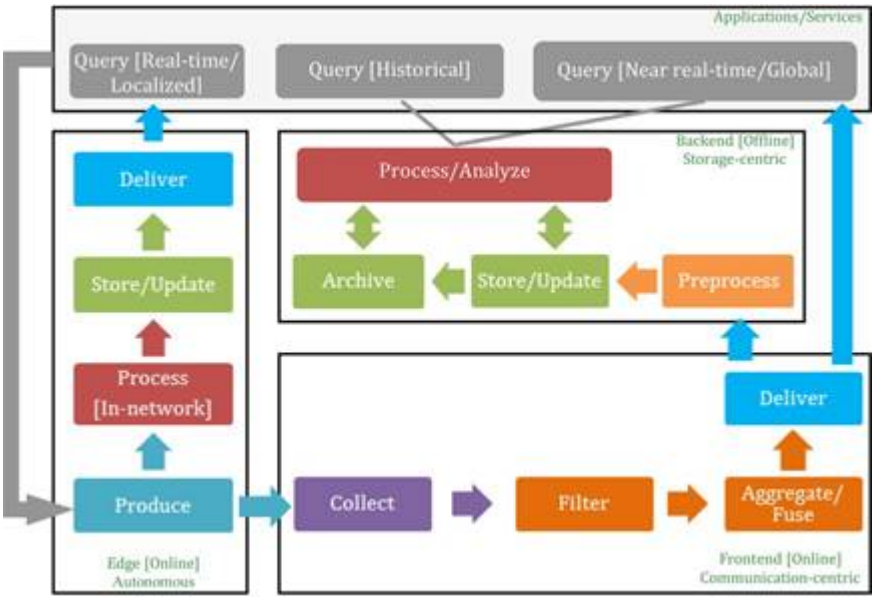

Fig 2.2 data Production

Storage operations aim at making data available on the long term for constant access/updates, while archival is concerned with read-only data. Since some IoT systems may generate, process, and store data in-network for real-time and localized services, with no need to propagate this data further up to concentration points in the system, edges that combine both processing and storage elements may exist as autonomous units in the cycle. In the following paragraphs, each of the elements in the IoT data lifecycle is explained.

· **Querying:** Data-intensive systems rely on querying as the core process to access and retrieve data. In the context of IoT, a query can be issued either to request real-time data to be collected for temporal monitoring purposes or to retrieve a certain view of the data stored within the system. The first case is typical when a (mostly localized) real-time request for data is needed. The second case represents more globalized views of data and in-depth analysis of trends and patterns.

· **Production:** Data production involves sensing and transfer of data by the “Things” within the IoT framework and reporting this data to interested parties periodically (as in a subscribe/notify model), pushing it up the network to aggregation points and subsequently to database servers, or sending it as a response triggered by queries that request the data from sensors and smart objects. Data is usually time-stamped and possibly geo-stamped, and can be in the form of simple key-value pairs, or it may contain rich audio/image/video content, with varying degrees of complexity in- between.

· **Collection:** The sensors and smart objects within the IoT may store the data for a certain time interval or report it to governing components. Data may be collected at concentration points or gateways within the network where it is further filtered and processed, and possibly fused into compact forms for efficient transmission. Wireless communication technologies such as Zigbee, Wi- Fi and cellular are used by objects to send data to collection points.

· **Aggregation/Fusion:** Transmitting all the raw data out of the network in real-time is often prohibitively expensive given the increasing data streaming rates and the limited bandwidth. Aggregation and fusion techniques deploy summarization and merging operations in real-time to compress the volume of data to be stored and transmitted.

· **Delivery:** As data is filtered, aggregated, and possibly processed either at the concentration points or at the autonomous virtual units within the IoT, the results of these processes may need to be sent further up the system, either as final responses, or for storage and in-depth analysis. Wired or wireless broadband communications may be used there to transfer data to permanent data stores.

· **Preprocessing:** IoT data will come from different sources with varying formats and structures. Data may need to be preprocessed to handle missing data, remove redundancies and integrate data from different sources into a unified schema before being committed to storage. This preprocessing

· **Microsoft Azure IoT Hub**-Microsoft is taking their Internet of Things cloud services very seriously. They have cloud storage, machine learning, and IoT services, and have even developed their own operating system for IoT devices. This means they intend to provide a complete IoT solution provider.

· **IBM Watson IoT Platform**-IBM is another IT giant trying to set itself up as an Internet of Things platform authority. They try to make their cloud services as accessible as possible to beginners with easy apps and interfaces. You can try out their sample apps to get a feel for how it all works. You can also store your data for a specified period, to get historical information from your connected devices.

· **Google Cloud Platform**-Search giant Google is also taking the Internet of Things very seriously. They claim that Cloud Platform is the best place to build IoT initiatives, taking advantage of Google's heritage of web-scale processing, analytics, and machine intelligence.
