Definition and Applications of SDN, NFV, Edge Computing and AI/ML Techniques

[1]Fabio Caccioli Capra
[1]Computer Science and Engineering, London Global University, London.
[1]fabiocapra121@hotmail.com

ArticleInfo
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202202015
Received 25 January 2022; Revised form 18 March 2022; Accepted 10 May 2022.
Available online 05 July 2022.

Abstract – A surge in Artificial Intelligence (AI) services and applications has been spurred by advances in deep learning. Massive data generation at the network edge is being sparked by the fast advancements in mobile computing and Artificial Intelligence of Things (AIoT). Big data can only be completely realized if the AI frontiers are pushed to the network edge, propelled by the successes of AI and IoT. It is hoped that Edge Computing would help to fulfil this trend by supporting AI applications that are computationally heavy on edge devices. Machine learning algorithms may be deployed to the end devices in which the data is created thanks to Edge AI. For every individual and business, Edge Intelligence has the ability to give AI at any moment, any place. This paper is limited to evaluating the definitions, history and applications of Software Defined Networks (SDNs), Network Functions Virtualization (NFV), Edge Computing (EC), Artificial Intelligence (AI)/Machine Learning (ML) techniques.

Keywords – Edge Computing (EC), Software-Defined Network (SDNs), Network Functions Virtualization (NFV), Artificial Intelligence (AI), Machine Learning (ML)

I. INTRODUCTION

Edge intelligence, often known as "intelligence on the edge," refers to a new phase of edge computing. Manufacturing plants, retail stores, workplaces and even whole cities are becoming more intelligent thanks to edge intelligence [1]. Currently, it is possible to do analyses that were previously only available in the data center or in-house data centers on the edge. Before transferring information to the server or another storage system, an autonomous remote sensor network might make an immediate judgement or transmit it to gateways for additional screening.

Smartwatches, vehicles, agriculture and industry are just some of the things that are becoming more and more technologically advanced. Smart gadgets, also referred to as "connected things," have become more popular as a result of the proliferation of internet-linked devices. Every effort was made to increase computational power in a single system during this time period. When a mainframe was connected to several dumb terminals in the 1980s, the phrase distributed computing was used for the first time. In the previous decade, cloud computing has mostly been the trend towards centralized data processing. In spite of cloud computing's widespread adoption, new and growing needs and workloads necessitate new and more complex cloud-based workflows. IoT has been a term for years, but in recent years we have witnessed a rise in the number of organizations using the technology. Nearly 6 billion IoT terminals were expected to be linked by 2020, according to [2]. Computers are being pushed back to the "edges" of local area networks and smart gadgets because of this massive spike in Internet of Things (IoT) usage.

Data processing takes place outside of the source in both conventional and cloud computing. Architectures that can be quickly scaled to distributed infrastructure are becoming more necessary as new systems, applications, and tasks emerge. For both today's needs (retail business analytics, communications networks) as well as tomorrow's advances (smart vehicles, cities, AR/VR), cloud capabilities at distant locations are essential. To keep up with ever-changing needs, cloud computing increasingly necessitates an expansion across numerous locations and platforms. The border between cloud intelligence and cloud analytics is quite thin. The term "edge analytics" refers to the collecting and analysis of data that takes place at or near a device's edge. Cloud-based analytics [3] are then performed on this data. In contrast to edge analytics, edge intelligence uses Artificial Intelligence to conduct operations directly at the edge of the network. To put it another way, this is a departure from cloud intelligence and cloud analytics where we transfer all this information across the network to a single data storage for analysis and decision making.

An example of how edge intelligence and edge analytics function together is shown in the diagram below (see **Fig. 1**). Metadata may be stored on an edge intelligence device. Only critical process data/reports are transferred to the cloud to evaluate the functioning of various edge devices. Additionally, this data is critical to understanding the activities of edge

devices and making subsequent choices like as re-training edge models for higher accuracy, re-training models with new data, etc. However, companies desired more from Edge Analytics, which allowed interconnected devices to undertake complicated event computation at their own end, resulting in real-time analytics. In a paper by Tsai, Venkatasubramanian, and Hsu, here is an excerpt: A rate of 30 billion images per second; a rate of 100 trillion images each hour. Surveillance videos across the world will record this much data in 2020 [4]. There will be double the number of cameras now installed at traffic junctions, mass transport hubs, and other places where the general public congregates, making our societies safer and more intelligent. Additionally, they'll be found in retail establishments, service centres, depots, and more to ensure security, manage inventory, and enhance service in any Smart Building or AI City project.

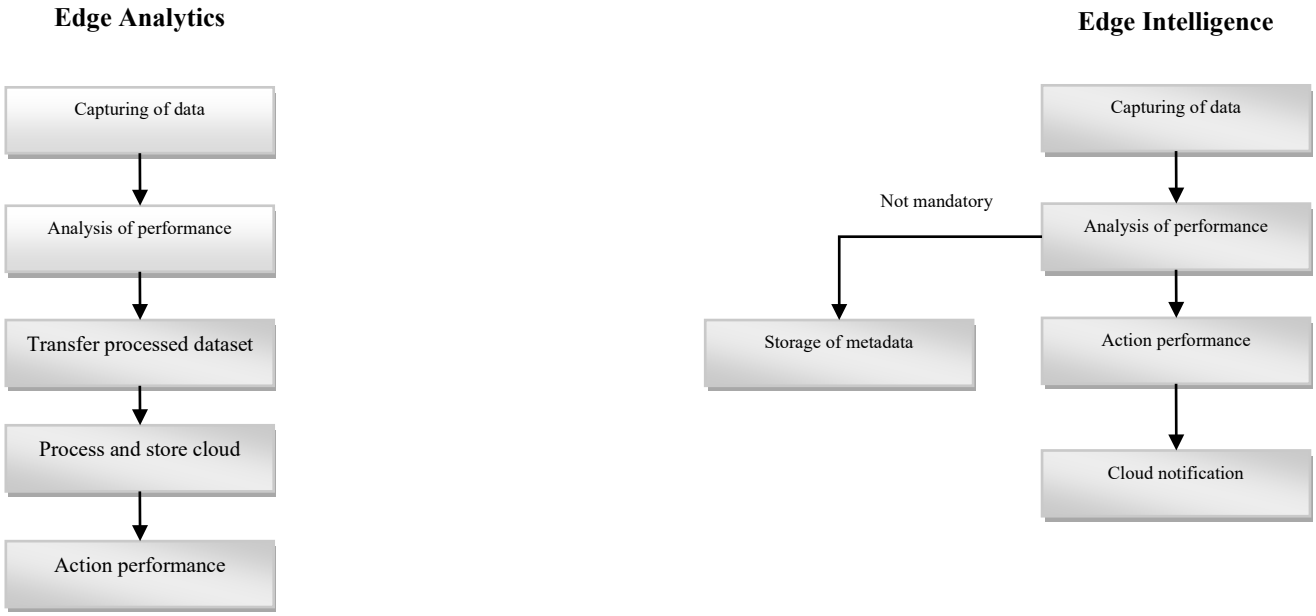

Fig 1. Flowchart between edge intelligence and edge analytics

Our world will soon be filled with much more than this, and it will be filled quickly. Data from cameras all across the world is being used to compile this extract. When we include in additional globally linked devices like smartphones and other detectors, the total is astonishing [5]. As a result, edge analytics has evolved into edge intelligence. Edge analytics has to evolve because (i) the quantity of data created by edge gadgets is expected to expand year on year, they must be able to perform functions beyond than CPE and analytics; (ii) data is so large, edge devices must be intelligent enough to function independently even when just a rudimentary link to the cloud is available; (iii) edge devices are currently being equipped with very fast microcontrollers, large storage capacity, and I/O connectors that are both fast and general; and (iv) edge devices may readily identify, connect, and interact with other smart objects that are in close proximity to their current location.

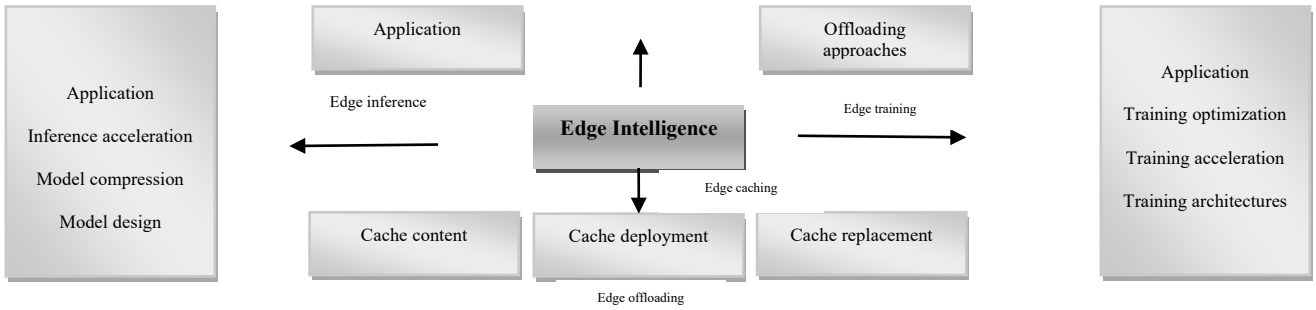

Fig 2. Components of edge intelligence

The rise of GPUs has provided considerable computational capability to edge devices, allowing the transition from edge analytics to edge intelligence to be completed as smoothly as possible. There is a drive to deliver artificial intelligence functionality from the network to the endpoints, so transforming them into edge intelligences as part of the shift from interconnected devices to smart objects. Investigation on edge intelligence has led to the discovery of four primary elements in edge intelligence infrastructure, as illustrated in **Fig. 2**. These components are: edge caching, edge offloading, edge inference, and edge training.

Despite the fact that Edge Intelligence is in its infancy, academics and businesses alike are eager to explore and use it. This study focuses on the definitions, history, and applications of edge intelligence enabling technologies. Section II presents a critical analysis of the enabling technologies i.e., Software Defined Networks (SDNs), Network Functions Virtualization (NFV), Edge Computing (EC), Artificial Intelligence (AI)/Machine Learning (ML) techniques. Section III draws conclusions to the research and proposes directions for future research works in edge intelligence.

II. ANALYSIS OF ENABLING TECHNOLLOGIES

Software-Defined Network (SDN)

Definition

Software-Defined Networking (SDN) [6] is more like cloud - based solutions than conventional network administration, allowing for dynamic, dynamically effective system design and management. Static network design is addressed with SDN technology. Data-plane separation from control-plane integration is one-way SDN aims to consolidate system intelligence in a single network element. There are one or more processors in the SDN network that are called the network's brains and are responsible for all of the network's functions. When it comes to reliability, scalability, and flexibility, centralization presents its own set of issues. When SDN first appeared in 2011, it was often used in conjunction with the OpenFlow protocol (for remote communication with network plane components for the determination of routes within the network packet over the switches of the network). Even though the word has been used since 2012 by proprietary software: These include Cisco's Open Communication Network and Nicira's virtualized network technology.

History

In order to ease provisioning and administration in the telephone system, it was necessary to separate the control and data planes, which was first implemented in the public telephone network long before similar design was used for data networks. As part of a proposed interface standard issued in 2004, titled "Forward and Control Element Separation (ForCES)," the Internet Engineering Task Force (IETF) started investigating different methods of decoupling the control and forwarding operations. In addition, Chan, Lau, and Lui [7] suggested a SoftRouter Architecture as a complement to the ForCES. In addition to the Linux Netlink as a Path Computation Element (PCE)-Based Architecture and an IP Services Protocol, two more early Internet Engineering Task Force specifications sought to separate control from data.

There were two main reasons why these early initiatives failed to acquire traction. One is that many members of the Internet community believed that decoupling control from data was a hazardous proposition, particularly given the possibility of a breakdown in the control plane. The second reason was that manufacturers were afraid that the creation of common Application Programming Interface (API) between both the control and data planes could lead to an increase in competitive pressures on their products. The Ethane research at Stanford's computer engineering department is credited with establishing the precedent for the usage of open programs in split data/control plane designs. OpenFlow was born as a result of Ethane's straightforward switch design.

In 2008, the first API for OpenFlow was established. NOX, an operating system for networks, was developed in the same year. SDN, an operating system for networks, internet infrastructure computing units, and a way to partition virtual networks depending on functionality were all described in patent applications submitted by separate academics in 2007. There are no restrictions on using the data in these patents, as these patents have been cancelled and are no longer patentable. Many other emulators were used in the investigation of SDN, including the well-known vSDNEmul, as well as EstiNet and Mininet. Works on OpenFlow at Stanford continues, including the establishment of testbeds to examine the protocol's utility in a single university network and as a gateway for linking many campuses over the Internet.

There have been a few university research and operational systems built on OpenFlow from NEC and HP, as well as on Quanta Software whiteboxes, beginning in 2009. Beyond the academics, the first implementations were made by Nicira in 2010 to operate OVS from Onix, which was created in collaboration with NTT and Google. Google's B4 rollout in 2012 was a significant example. Later, Google announced the simultaneous deployment of OpenFlow and Onix in their datacenters. China Mobile is another well-known massive rollout [8]. SDN and OpenFlow were promoted by the Open-Source Foundation, which was created in 2011. Avaya exhibited software-defined networking utilising shortest route bridging (IEEE 802.1aq) with OpenStack as an autonomous campus at the 2014 Metaprogramming and Tech Fields Day, expanding robotics from the datacentre to the end system and eliminating human deployment from delivery of services.

Application

Software-Defined Mobile Networking (SDMN)

It is possible to create mobile networks using SDMN, which is a software-defined method that makes use of modular and commodity software and hardware to execute all protocol-specific functionalities, both in the peripheral and wireless networking devices. As an augmentation of the SDN paradigm, it is being suggested to add wireless network-specific features. With the PFCP protocols, a Control User Plane Segregation has been implemented in Mobile Network Infrastructure topologies since 3GPP Rel.14.

Software-Defined Wide Area Network (SD-WAN)

Leveraging software-defined networking concepts, a Software-Defined Wide Area Network (SD-WAN) manages a Wide Area Network (WAN). It is the primary goal of SD-WAN to reduce WAN expenses by utilising publicly accessible leased lines instead of more costly MPLS connections. Using central controllers, setup and control are simplified since they are handled independently of the infrastructure.

Software-Defined Local Access Network (SD-LAN)

Local area networks (LANs) [9] designed on software-defined networking principles are known as SD-LANs. However, there are significant changes in the architecture of SD-LANs as well as information security, monitoring and management of applications, administration, and service standards. Data plane decoupling and policy-driven design are two of the key benefits of the SD-LAN standard for wireless and wired Local Area Networks (LANs). SD-LANs are typified by their usage of a cloud control systems and wireless communication without the inclusion of hardware controllers.

Security Employing SDN Model

Due to the operator's centralized perspective of the networks and the data plane's ability to be reprogrammed at any moment, the SDN paradigm may allow, facilitate, or improve network security mechanisms. Security in SDN architecture is still an open subject that has been explored by the research community on a few occasions, however the following subsections mainly concentrate on security technologies made feasible or revisited by SDN. SDN controller-based security applications have previously been studied in a variety of ways by several research initiatives. Distributed denial of service (DDoS), botnets, and worm dissemination are all examples of how such technologies may be put to use. The concept is to gather network data from the forwarding devices of the networks on a regular basis (e.g., using Openflow) and then use classification techniques to that information in order to identify any network abnormalities. There are times when the data plane must be reprogrammed in order to reduce an anomaly.

Moving Target Defence (MTD) techniques may also be used as a security application to exploit the SDN controller. Essentially, MTD techniques are employed to make any assault on a particular systems or networks more complex than normal by concealing or modifying essential aspects of that network or networks at regular intervals. MTD algorithms are not easy to apply in conventional networks because it is challenging to construct a central authority capable of determining, for each element of the systems to be secured, whether critical attributes are concealed or modified. The primacy of the controllers makes these duties easier in an SDN network. For example, a controller may give virtual IP addresses to network hosts on a regular basis, and the application can subsequently translate those virtual addresses to their actual counterparts. In order to generate substantial noise during an attacker's surveillance phase (e.g., scanning), another programme may imitate false open, blocked, or censored interfaces on randomized nodes within the network.

Additionally, the use of FlowVisor and FlowChecker in SDN-enabled networks provides additional benefit in terms of security. The former makes use of a specific hardware forwarding devices in order to share numerous logical networks that are geographically dispersed. It's possible to employ the same hardware components for creation and processing while also separating surveillance, management, and web traffic such that each scenario has its own logical architecture, which is known as a slice. Additionally, FlowChecker allows users to test new OpenFlow rules they publish using their own slice in combination with this method. Most SDN controller programs are often implemented in large-scale settings, requiring extensive testing for probable programming mistakes. System dubbed NICE was first discussed in 2012 for this purpose. SDN needs a long-term strategy to implement a robust security framework. There are several approaches to protect SDN without sacrificing scalability since it was first introduced. The SN-SECA (SDN+NFV) System Design is one example of this kind of design.

Group Delivery of Data Employing SDN

Replication of data is a common practise in distributed systems that operate across several data centres for synchronisation, fault robustness, load balancing and to bring data closer to the end user's fingertips (that minimizes latency for users and enhances perceived throughputs). Data is replicated over many racks in various systems, such as Hadoop, to enhance fault tolerance and simplify data recovery. There are a number of processes that need the transfer of data from one computer or datacenter to another. "Reliable Groups Data Delivery" refers to the method of reliably providing data from one system to numerous machines (RGDD). An SDN switch may be used to implement RGDD by the introduction of rules that enable traffic to be sent to numerous outbound ports. In OpenFlow, for example, this has been feasible since edition 1.1, which provides provision for cluster tables A centralized server can build up RGDD forwarding trees with care and intelligence using SDN. Network latency and load levels might be taken into consideration while building such trees. While MCTCP depends on the consistent and well-structured architectures of datacenter connections to transport data and content to numerous nodes in the same datacenter, DCCasting and QuickCasting are ways to rapid and efficient information and content reproduction between datacenters via secure networks.

Network Functions Virtualization (NFV)

Definition

In Network Functions Virtualization (NFV), functionalities are decoupled from their specialized hardware platforms and executed as software inside virtual servers. NFV utilises virtualized network nodes to enable a network architecture that is completely decoupled from its underlying hardware. It is possible to virtualize and use commercial off-the-shelf (COTS) technology, such as x86 servers, to provide typical computation, storage, and networking operations. As a result of virtual servers, the x86 user's resources may be allocated to individual virtual machines (VMs). To make use of the remaining spare resources, numerous virtual machines may operate on a single server. As a result of this, resources are less likely to go to waste, and data centres with virtualized architecture may be put to better use. NFV allows for the virtualization of both the data layer and the control layer inside the data centre and on the external network.

History

A white paper on Software-Defined Networking (SDN) and OpenFlow was presented at a symposium in Darmstadt, Europe, in October 2012. It was thanks to the White Paper that the European Telecommunications Standards Institute (ETSI) formed the NFV Manufacturing Specification Group (ISG). The ISG was constituted of telecom sector professionals from throughout Germany and the rest of the world. Protocols, APIs, testing, dependability, security, and future developments are only a few of the topics addressed by the ETSI ISG NFV.

NFV's origins can be traced back to telecom operators who desired to speed up the process of incorporating fresh network services or applications. As previously stated, there was no one standard organisation, but rather a number of alternative ones. It was decided that certain network operators will go with an open data methodology to the development of a common NFV framework. NFV standards were initially published by the European Telecommunications Standards Institute (ETSI) in October 2013 and have been widely adopted thereafter. Network Orchestration (NOC) and Management and Orchestration (MANO) have been defined by the ETSI ISG NFV (NFV MANO). Collaboration initiatives like OPNFV also benefit from ETSI's involvement.

For the first time since May 2021, the ETSI NFV ISG has scheduled the launch of its fifth set of standards, which will include new requirements and updates to existing ones. There have been over a hundred articles from the group since the white paper was published, and many of them are now being used in well-known open-source programs like OpenStack, Open-Source MANO (OSM), ONAP. The ETSI NFV standards are also referred to in other SDOs like as ETSI MEC, IETF, 3GPP, and others due to proactive cross-liaison efforts.

Application

There are 6 network function virtualisation applications shown in this subsection that show how NFV is now being utilised to solve a wide variety of issues and offer better options to these and other connectivity barriers in order to improve services and minimise outlays.

Network Virtualization

NFV technologies [10] are utilised primarily by telecom firms throughout the globe for network virtualisation, which is the primary use case. Hardware and software are no longer intertwined with NFV. A virtual network is created on top of the physiological network. This divergence of software and hardware enables service suppliers to enlarge and speed up the development and advancement of their services. ' Provisioning, for example, is made easier as a result. Virtualization of network elements such as DNS, prefetching, firewalling and IDS has become increasingly popular as a way for consumers to better manage their network services. Instead of hardware, they can now run-on software thanks to this solution. When it comes to deploying new internet services, network operators may benefit from increased agility and flexibility thanks to network virtualization. They save money by not having to buy as much cumbersome physical gear and by not having to pay as much to operate, operate, and repair it as often. The new MEC and SD-WAN are excellent instances of virtualization technology. Despite this, network virtualization isn't the only use case for Network Function Virtualization (NFV).

Mobile Edge Computing

Another technical advance that has grown in prominence in the last several years is Mobile Edge Computing (MEC). Going into the year 2022, this innovation seems to be just becoming stronger. What is the relationship between internet function virtualisation and mobile edge computing? What's the connection between them? As a matter of fact, the two are inextricably intertwined and have a direct impact on each other's progress and potential use. Allowing edge devices to execute computational services and offer network functions through the use of either a single or numerous network functional Virtual Machines (VM). There are several examples of these techniques, such as Multi-Access Edge Computing (MEC). Ultra-low latencies are provided by the MEC via the use of Mobile Edge Computing (MEC). Five-generation (5G) wireless networks are the inspiration for this new technology. The MEC's topology is comparable to the NFV's in that it consists of distinct components (see **Fig. 3**).

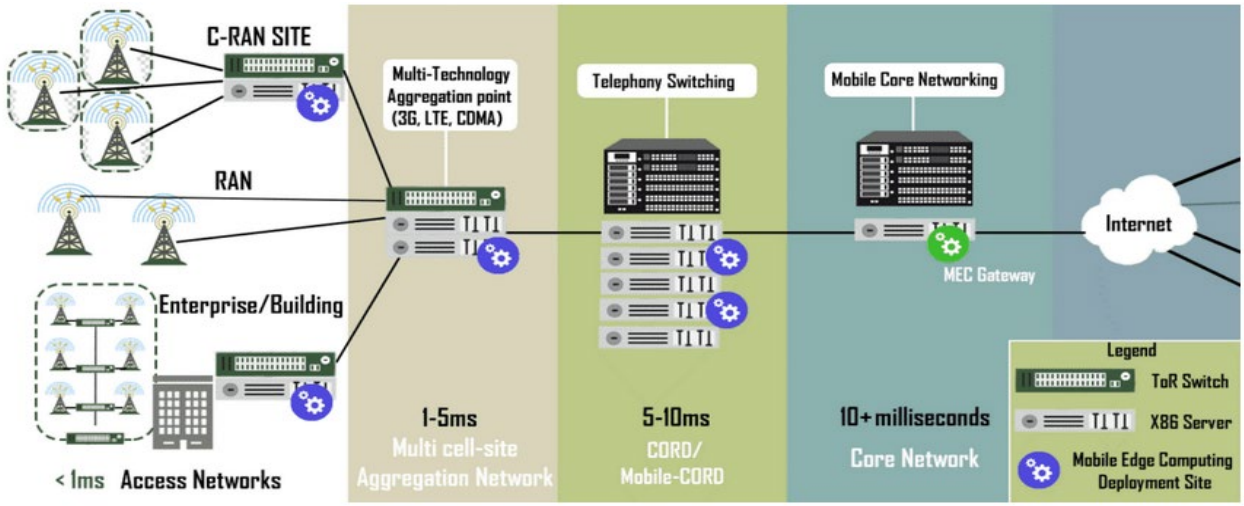

Fig 3. Mobile edge computing topology

The term "edge computing" alludes to elements such as transmission towers, mini-data centres, and localized data centres when it pertains to "mobile" computer technology. Mobile networking service functionalities are translated from software to hardware through NFV, which takes use of virtualization technology [11]. NFV, among other technical and network breakthroughs like SDN and AI, are anticipated to become the primary solutions for the future network difficulties as they are early integrated and combined.

Orchestration Engines

The applications for orchestration engines are among the most useful. Due to the absence of automated procedures and warnings and the inability to adapt quickly, legacy networks are very restricted in their capabilities. Unintentional mistakes made by humans are a major source of network outages. Automated machines are in great demand because of this reason. In addition, these systems save money on upkeep and maintenance expenses since they need much less human interaction. Network functionalities and operations are connected by NFV orchestration, which makes use of programming technologies. The orchestration takes care of the NFVi and the VNFs. Centralized orchestration engines might be a great investment for those that are eager to get started. Most experts agree that the following characteristics are necessary in any centrally managed automated engine: Network segregation and transparency; certificate administration for Public Key Infrastructure (PKI); and It's ready to go from the get-go

Video Analytics

Since the introduction of the Internet of Things, video surveillance technologies and applications have also witnessed a significant boost in their capabilities. Employing IoT cameras and smart devices put in their workplaces, shops, offices, and even farms, corporations can now collect vast volumes of data from their operations. Cloud-native apps or sophisticated servers in the cloud are often used for high-performance AI visual analytics. On-premises data must be transferred into the cloud for evaluation, and this presents a significant problem. In the modern networking, end-to-end latencies may be a major problem for applications and services that are susceptible to network latency, like video surveillance. For this reason, businesses have turned to NFV and SDN designs in an attempt to minimise network resource consumption and enhance latency timeframes. According to some suggestions, these solutions might cut bandwidth utilisation by up to 90 percent when paired with video surveillance at the networking edge. Devices such as Lanner's NVA-3000, which uses video surveillance, are one example. Designed for surveillance videos and robot navigation, this NVR may be used in large enterprises. Video from many sources, e.g., surveillance footage, may be collected by an NVR and sent over the network through a low-latency connectivity, like 5G or LTE. When a request comes in, the VNF operator immediately dispatches network services to the network's edges (see **Fig. 4** below).

It is becoming more vital to use big data with video surveillance systems and applications, as IoT, intelligent and edge technologies enable more dataset to be created and gathered. Virtualisation of network functions serves as the basis for these technologies' architectures.

Security

To safeguard our virtual and physical assets, the instruments we employ to do so have changed in response to recent digital advancements, much as the instruments we utilize to grow crops or build automobiles. Virtual gates are already available from a number of security firms. F5's Gi Gateway VNF Services is one of the more prevalent NFV systems with firewall features, for instance. NFV and SDN will be used to virtualize firewall, but in actuality, they are only one kind of security equipment that will be digitized in the near future. The concept of centralised management and evenly dispersed

compliance is one of the most appealing aspects of virtualized encryption. Firms trying to improve their security are flocking to these sorts of technologies because of these two reasons.

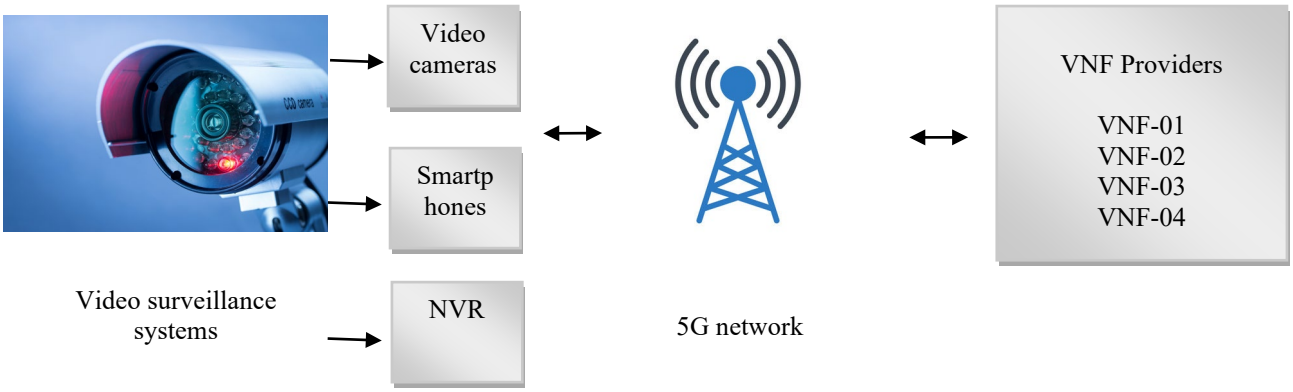

Fig 4. Video analytics system

Network Slicing

Since the start of 5G development and implementation [12], network slicing has grown in popularity. The goal of this technique is to divide a physical infrastructure into many smaller ones. There is a strong correlation between system slicing and NFV, and NFV is anticipated to play a significant role in 5G network slicing. As with advanced Virtual Private Networks (VPNs), cutting the network is a process that might include both physical and virtual components. One physical network may be divided into many logical networks using this technique. It is possible to personalize and customize every case or "slice" for certain purposes and assign them to various departments. In many cases, the slice is delivered in the form of a Virtual Network Function (VNF).

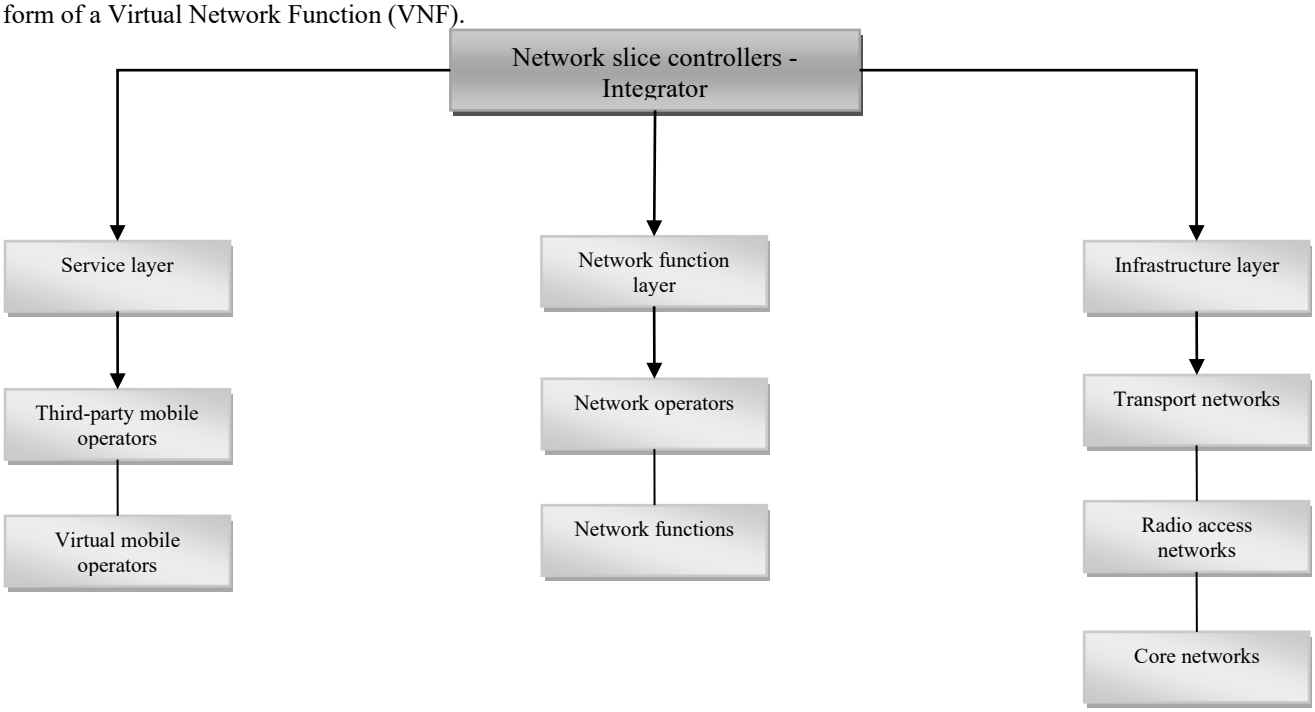

Fig 5. Basic paradigm for 5G network slicing based on three layers: Infrastructure, Network function, and Service function

Network Slicing in 5G: Surveys and Constraints, a publication published by IEEE, proposes the following basic paradigm for 5G network slicing based on three layers: Infrastructure, Network function, and Service function (see **Fig. 5**). When a VNF is pushed from the service layer to the functionality layer, it executes on modular hardware in the data centre. All three levels are sliced by the integrator. Network Function Virtualization (NFV) dynamically allocates resources to every segment of the system at the appropriate quality of service (QoS) and overall performance. Some of the advantages of network slicing include providing configurability and optimize certain services; integrate agility, efficiency, and flexibility to end-users; minimize OpEx, and CapEx; and finally enhance the deployment timeframe for network service.

Edge Computing

Definition

Any software tool that gives low latency closer to the demand is one concept of edge computing. "Edge computing" is described by Karim Arabi as all computing that occurs outside the clouds and in systems where real-time handling of data is necessary, in an IEEE DAC 2014 inaugural and an authorized session at MIT's MTL Seminars in 2015. Cloud technology, on the other hand, relies on "large datasets," whereas edge computing relies on "immediate data," which really is data created by detectors or clients. Fog computing is commonly referred to as "fog computing." "In closeness to the final mile networks," per the Status of the Edge survey, edge computing focuses on servers. ETSI MEC ISG specifications subcommittee chair Alex Reznik describes "edge" as "everything that's not a typical data centre." 1 or 2 hops distant from the user, the edges nodes utilised for gameplay are referred to as "gamelets." Edge nodes are often only 1 or 2 hops distant from the client machine in order to fulfil real-time gaming requirements in the game streaming scenario, say Anand and Edwin. The deployment and operation of a broad variety of programs on network edge could well be simplified by the use of virtualisation technologies in edge computing.

History

A Content Delivery Network (CDN) from Akamai, which added nodes at places closer to the end user, may be dated to the 1990s. These nodes are used to store photos and movies that have been previously accessed. Using edge computing, nodes may execute simple computation activities. Computer scientist Brian Noble showed in 1997 that edge computing might be used for voice recognition on mobile devices. More than a decade later, the same technique was applied to increase the battery capacity of smartphones. Both Apple's Siri and Google's voice recognition systems use a technique called "cyber forage," which was coined at the time. Peer-to-peer technology made its debut in 1999. Since the introduction of Amazon's EC2 service in 2006, businesses have flocked to the convenience and cost savings that come with cloud technology. Cloud technology and latency are intertwined, as detailed in "The Arguments for VM-Based Cloud users in Computing Technology," released in 2009. There was an essay that proposed a "two-level architectural features: the first layer is today's unaltered distributed system, and the second comprises of distributed parts termed 'cloudlets with state retained from the first level' In 2012, Cisco used the phrase "fog computing" to describe a distributed cloud architecture aimed to increase the flexibility of the Internet of Things (IoT).

This takes us to the present cutting-edge options, which are many. Blockchain, peer-to-peer, and mixed platforms like Greengrass and Microsoft Azure IoT Edge are all examples of edge computing that are pushing the adoption of IoT. What's next for Edge Computing (EC)? A lot of end-user gadgets are already using these technologies to increase their functionality, usefulness, and battery life. We're already seeing edge technologies in a variety of applications that weren't previously possible, such as virtual reality headphones, driverless cars, drones, smart clothing, and augmented reality gadgets. Healthcare, manufacturing, transportation, and building automation are just a few of the sectors only now beginning to adopt IoT technology into their marketing strategies. This proliferation of IoT gadgets is expected to persist for some time. Many current cloud systems are becoming decoupled from their centralised foundations as a result of advances in edge computing technologies. Instead of being region-locked, applications are being redesigned to perform their duties at the edge point closest to the request's place of origin. Emergent edge technologies like bitcoin and fog computing are also developing. A lot of people are excited about blockchain's prospects because of its decentralised structure and complicated algorithms, which may be used for purposes beyond Bitcoin. In both logistics and polling, where security and fraud detection might be aided, it could be useful.

Application

Autonomous vehicles

One of the earliest uses of driverless cars is anticipated to be in the platooning of vehicle convoies. As a number of trucks drive in a caravan, they save money on gasoline and reduce traffic. Edge computing will allow vehicles to connect with each other with ultra-low latencies, eliminating the requirement for an operator in all but apart from the front of the vehicle.

Remote surveillence of resources in oil/gas industry

Experiencing an oil or gas breakdown might be catastrophic. As a result, it is necessary to keep a close eye on their assets. Plants for extracting oil and gas tend to be located in outlying areas. Real-time monitoring may be performed nearer to the resource using edge computing rather than relying on excellent connection to a centralized node.

Smart Grid

With increasingly ubiquitous use of smart grids, businesses may better monitor their energy use via the use of edge computing. The utilisation of monitors and Internet of things devices linked to an edge system in manufacturing facilities, plants, and offices allows for real-time analysis of energy use. Using real-time monitoring, businesses and energy providers may come up with innovative arrangements, such as running high-powered machines during off-peak periods. As a result, a company's use of environmentally friendly energy sources like wind power may grow.

Predictive Maitainability
Detecting and analysing changes in manufacturing lines is a top priority for manufacturers. With the aid of edge computing, data handling and storage may be moved closer to the hardware itself. Low latency and real-time data analyses are possible because to this technology.

In-hospital Monitoring of Patients
There are several cutting-edge prospects in the healthcare industry. Monitoring equipment (such glucose metres, health instruments, and other monitors) are now either not linked, or huge volumes of raw data from gadgets must be kept on a third-party cloud service provider's server. Concerns about patient safety may arise as a result. A local interface on the medical centre might process data to ensure data privacy. Using analytics and artificial intelligence (AI), Edge can also provide messages to clinicians at the exact appropriate moment about unexpected patient patterns or actions, and it can create dashboards for patients with a 360-degree perspective for complete visibility.

Virtualised Radio Networks (vRAN) and 5G
It is becoming more and more common for cellular services to be virtualized. This is a win-win situation for both costs and versatility. With the introduction of the new virtualized RAN hardware, a high level of complexity and low latency are required. Virtualizing the RAN near the cell tower necessitates the use of network edge.

Cloud Gaming
Gaming in the cloud relies heavily on latencies since it delivers a live broadcast of the gameplay to the user's device rather than processing it and hosting it in a data centre. To minimise latencies and deliver a more immersive gameplay experiences, cloud gaming businesses are building edge servers as near to players as feasible.

Artificial Intelligence (AI)/Machine Learning (ML) Techniques
Definition
Machine learning (ML) is the examination of computational models that are able to adapt and develop themselves via experiences and data. As a component of AI, it's often regarded as useful. Based on a model built from training examples, machine learning techniques may make predictions or judgments without being formally coded. In many fields, e.g., computer visioning, speech recognition, health analysis and email filtering, it is nearly impossible or difficult to structure traditional techniques that can do the required tasks that machine learning techniques can.

Artificial Intelligence (AI) represents a computer programme or a robot operated by a computer that is capable of performing functions usually reserved for highly intelligent individuals. The term is globally utilized to define the purposes of defining the purposes of formulating models, which are capable of reasoning, uncovering definitions, generalizing and learning from prior experiences.

History
"Machine Learning (ML)" [13] was invented by Arthur Samuel, a forerunner in games consoles and artificial intelligence, in 1959. This period of time also saw the usage of the phrase "self-taught computers." When it comes to machine learning approaches in the 1960s, Nilsson's Learning Engines is a good place to start since it deals primarily with pattern categorization. The enthusiasm in pattern classification persisted far in the 70s, according to Hart and Duda in 1973. It was analysed in the early 1980s that neural networks are capable of learning and distinguishing forty items ie four special characters, ten numbers and twenty six letters) from a centralized computer applying training approaches. "A computational model has been said to learn from experiences E with reference to a subclass of task "t" and an appropriate performance "p" if its competency at tasks in "t", as measured by "p", grows with experiences "e"," according to Tom M. Mitchell's comprehensive explanation of machine learning techniques. When it comes to defining machine learning, this term gives a practical rather than a philosophical definition. When it concerns to computing mechanisms and intelligence, Alan Turing's query "Can computers do what humans (as thinking beings) can achieve?" substitutes Turing's original question "Can computers think?"

Contemporary machine learning includes two goals: one is to categorise data using designs that were constructed, and the other is to forecast future events using these systems. When it comes to learning to recognise malignant moles, supervised learning and machine vision could be used in a theoretical algorithm. When it comes to predicting the future, a stock-trading deep learning system may be able to help. Machine learning was born out of the search for artificial intelligence. Early on, several AI researchers were intrigued in letting robots learn from their own experiences via data. Symbolic approaches and "artificial neural" were used to try to solve the issue, however they were largely perceptrons and other frameworks that were subsequently proven to be reinterpretations of the generic linear frameworks of statistical data. Automated clinical diagnosis, in particular, made use of stochastic reasoning techniques.

Artificial Intelligence (AI) and Machine Learning (ML) are currently at odds because of an increased focus on logical reasoning. Data collection and representation are thorny issues on the side of stochastic networks. Expert systems had taken over AI in the 1980s, and analytics had faded into obscurity. Study in inductive logic coding and knowledge-based/symbolic training was carried on inside AI, while the more analytical line of studies in pattern classification and data

extraction was now carried out beyond of AI proper. After a brief period of time, neural networks study was discontinued by both artificial intelligence and computer programming. As "connectionism," academics external of the AI/CS area maintained this line of thinking as well, particularly Hinton, Rumelhart, Hopfield. It was in the mid-1980s that they re-invented back-propagation. In the 1990s, Machine Learning (ML) was restructured as a distinct subject. The area has shifted its focus from artificial intelligence to solving real-world challenges. The emphasis moved away from AI's symbols methodology and toward statistical and stochastic theory's methodologies and concepts. The distinction between Machine Learning (ML) and Artificial Intelligence (AI) is often erroneously construed. As ML trains and forecasts by passive observations, AI implies an agent that interacts with the surroundings to optimize its chances of succeeding in its objectives. By the year 2020, many people believe that machine learning will still be considered part of artificial intelligence. Others argue that only a "smart subset" of Machine Learning (ML) must be deemed AI.

Application

There are numerous ML applications e.g. Food production, morphology, dynamic website, human computer interaction, astronomy, corporate finance, computational biology, central nervous system interfaces, cheminformatics, translational research, internet technology, object tracking, credit-card fraud sensing, data quality, DNA encoding indexing, economic history, banking system evaluation, handwriting identification, data retrieval, healthcare, internet fraud prevention, graph data embedding, philology, ML command, machine impression, language processing, machine interpretation.

When Netflix launched its inaugural "Netflix Prize" contest in 2006, it was looking for a way to increase the reliability of its Cinematch film recommender system by at minimum 10% while also effectively anticipating customer interests [14]. Big Chaos and Pragmatic Theory collaborated with AT & T Labs-Research on an ensemble classifier that won the Grand Prize for $1,000,000 in 2009. Netflix quickly discovered that ratings weren't the greatest measure of a viewer's watching habits (everything is a suggestion), and they made changes to their recommended algorithm. The fiscal collapse was predicted using machine learning by the business Rebellion Research in 2010, according to a Wall Street Journal article. In 2012, Vinod Khosla, the co-founder of Sun Microsystems, estimated that 80 percent of healthcare physicians' occupations will be replaced by automatized learning clinical detection software over the next 2 decades. Computer-aided analysis of fine art artworks may have unearthed heretofore unknown connections between artists, according to a paper published in 2014. 2019 saw the release of a new machine-learning-based research book from Springer Nature. In the year 2020, scientists turned to machine learning technologies to assist in the diagnosis of COVID-19 and the development of a treatment. Lately, deep learning has been used to anticipate human desired behaviours. In recent years, computer science has been used to improve the responsiveness and thermal response of handsets depending on the user's engagement with the device.

III. CONCLUSION AND FUTURE DIRECTIONS

In the edge intelligence, which is placed near the gadgets that utilise and produce data, a convergence of enhanced interconnectivity, condensed computing capacity, and Artificial Intelligence (AI) exists. Data analytics, cloud computing, and Artificial Intelligence (AI) combine to provide a new paradigm for industrial surveillance, autonomous manufacturing, utility control, and telecommunication. Intelligence at the edge enables data to be operated on immediately or filtered for just the most critical pieces, so that only the most relevant information is sent to the core. It is possible that the edge intelligence may significantly improve distant operations by bringing cloud applications to them.

Recent years have witnessed a huge development in artificial intelligence (AI) services and applications, from personalized assistants to recommendations algorithms to video/audio surveillance, thanks to improvements in deep learning technology. Internet of Things (IoT) and the Mobile Computing have recently expanded to the point that billions of smartphones and IoT devices are now linked to the Internet, generating vast amounts of data at the network edge. To fully unlock the promise of edge big data, it is imperative that the AI boundaries be pushed to the edge node. For this reason, edge computing has been widely seen as a feasible configuration, a developing architecture that moves computing tasks and services out from the core of the network and closer to the network's edge. EI is the novel interdiscipline that has emerged as a result of this. Research into EI is currently in its infancy, and a dedicated forum for exchanging information about EI's progress is a high priority for both computer systems and the AI world alike. The widespread use of EI does not imply that a centralised Cloud Intelligence (CI) is out of the question It's true that a continuous stream of intelligent capabilities and functionalities across all cloudified foundations necessitates the organised use of edge and clouds virtual resources. This is one of the biggest obstacles to a robust and prospective 5G networks.

References

[1]. M. H. Siddiqi and I. Alrashdi, “Edge detection-based feature extraction for the systems of activity recognition,” Comput. Intell. Neurosci., vol. 2022, pp. 1–11, 2022.

[2]. M. Li, Z. Yang, X. Wang, L. He, and Y. Teng, “Research on batch detection technology of common network security vulnerabilities in IoT terminals,” in 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2021.

[3]. M. K. Senapaty, G. Mishra, and A. Ray, “Cloud-based data analytics: Applications, security issues, and challenges,” in The Role of IoT and Blockchain, Boca Raton: Apple Academic Press, 2022, pp. 373–389.

[4]. M.-H. Tsai, N. Venkatasubramanian, and C.-H. Hsu, “Analytics-aware storage of surveillance videos: Implementation and optimization,” in 2020 IEEE International Conference on Smart Computing (SMARTCOMP), 2020.

[5]. A. Penn and K. Al Sayed, "Spatial information models as the backbone of smart infrastructure," Environ. Plan. B Urban Anal. City Sci., vol. 44, no. 2, pp. 197–203, 2017.
[6]. Z. Guan, L. Bertizzolo, E. Demirors, and T. Melodia, "WNOS: Enabling principled software-defined wireless networking," IEEE ACM Trans. Netw., vol. 29, no. 3, pp. 1391–1407, 2021.
[7]. B. C. B. Chan, J. C. F. Lau, and J. C. S. Lui, "OPERA: An open-source extensible router architecture for adding new network services and protocols," J. Syst. Softw., vol. 78, no. 1, pp. 24–36, 2005.
[8]. R. K. Das, M. Jha, and S. Harizan, "Performance appraisal of 6LoWPAN and OpenFlow in SDN enabled edge-based IoT network," in Advances in Intelligent Systems and Computing, Singapore: Springer Singapore, 2022, pp. 21–29.
[9]. L. Yang, "Data acquisition and transmission of laboratory local area network based on fuzzy DEMATEL algorithm," Wirel. netw., 2021.
[10]. W. S. Atoui, N. Assy, W. Gaaloul, and I. G. Ben Yahia, "A model-driven approach for deployment descriptor design in network function virtualization," Int. J. Netw. Manage., vol. 32, no. 1, 2022.
[11]. Y. Li and Y. Hong, "Prediction of football match results based on edge computing and machine learning technology," Int. j. mob. comput. multimed. commun., vol. 13, no. 2, pp. 1–10, 2022.
[12]. S. Jain, S. Gupta, K. K. Sreelakshmi, and J. J. P. C. Rodrigues, "Fog computing in enabling 5G-driven emerging technologies for development of sustainable smart city infrastructures," Cluster Comput., 2022.
[13]. M. Z. Naser, "Deriving mapping functions to tie anthropometric measurements to body mass index via interpretable machine learning," Machine Learning with Applications, vol. 8, no. 100259, p. 100259, 2022.
[14]. D. Jackson, "The Netflix Prize: How a $1 million contest changed binge-watching forever," Thrillist, 07-Jul-2017. [Online]. Available: https://www.thrillist.com/entertainment/nation/the-netflix-prize. [Accessed: 07-Feb-2022].