

An Agile Internet of Things (IoT) based Software Defined Network (SDN) Architecture

Rowayda A. Sadek

Faculty of Computers and Information, Helwan University, Cairo, Egypt

rowayda_sadek@yahoo.com

Abstract

Industry, Business, Society, governments are excited for the endless applications that can be done by Internet of Things (IoT) technology. Managing and controlling high dynamic IoT network overlaid huge number of ad hoc things/devices is a tough task. The traditional networks architecture cannot afford this task efficiently. Software Defined Networking (SDN) provides the agile dynamic solution that can cope with the special requirements of the diversity of innovative IoT applications. The Agile network architecture is built on having more softwarization of devices functions to offer more agility than what was provided traditionally by the network architectures cross layer concept. Network functions virtualization (NFV) and Deep Packet Inspection (DPI) could efficiently complement the SDN functions. The paper provides a vision on expanding the need for convergence of SDN and NFV into a swift, Self-organization, self-healing IoT network in heterogeneous environments. This paper presents an agile SDN based IoT network architecture; SDNoT. SDNoT newly considers an efficient merge of SDN, NFV and DPI for worldwide implementation of IoT.

Keywords: *IoT; SDN; NFV; Agile Network; Virtualization*

1. Introduction

IoT provides technology to connect things together in a smart scalable way. Connection could be between devices, between human, and/ or connecting human to device. This enables wide range of applications that provides many services and huge amount of data. Managing and orchestration such a network requires high computation. Traditional networks architecture doesn't efficiently offer this kind of management. SDN provides the dynamic solution that offers these requirements. SDN provides dynamic network deployment and increased agility. Traditional networks with its devices intermediate devices (Routers, switches, firewalls, load balancer, .etc) and edge devices are undergone the diversity of hardware and software platforms vendors. Designing and deploying an efficient network for a specific objective requires long time and overhead complexity, which causes slow down applying continuous users demand. Control, management and security components are usually coupled. Therefore, it is a tough task to adapt each component in each device. The highly demand for adapting the networks currently, provides new level of network computing. Many researchers studied this demand and provided models to have more softwarization less hardware for easily adapting [1-2]. SDN disjoints control and media planes. Control plane dynamically provides orchestrating for any media flow in real time.

NFV disunites software from hardware to enable flexible network deployment and dynamic operation. NFV deployments typically use commodity servers to run network services software versions that previously were hardware-based. These software-based

services that run in an NFV environment are called Virtual Network Functions (VNF). VNFs are such as routing, firewalling, load balancing, WAN acceleration, and encryption. Providers can dynamically offer customers these network services, with the ability to spin them up down on demand via virtualization. SDN-NFV hybrid program was provided for high efficiency, elastic and scalable capabilities [3]. The differences among DPI and SDN and NFV have not been clearly discussed and distinguished before. This clarification is required for understanding their usage in IoT heterogeneous field. Although, SDN, NVI, DPI seem overlapped in their functions in some applications such as cloud computing infrastructure and Internet service provider, they are complement each other in case of complex networks applications such as the one usually used in IoT. IoT networks infrastructure utilize and suffer from being heterogeneous in the end nodes, heterogeneity in communication links used in LAN and WAN scales, mobility in practice, low power devices, etc.

This paper presents an innovative agile SDN based IoT network architecture that considered an efficient merge of SDN, NFV and DPI for worldwide implementation of IoT. The paper provides vision of expanding the need for convergence of SDN and NFV into a swift, Self-organization, self-healing IoT network in heterogeneous environments. The main purpose behind the merging of NFV and SDN with focusing on the consideration of the DPI functions provides agile steering for the context aware traffic and agile service provisioning with QoS that improve the user satisfaction. The paper is organized as follows; second section purposes the IoT architecture and its provided services and the challenges it faces. Section three discusses the SDN architecture and its provided services and its challenges. Section four provides the main architecture for the NFV. Section five reviews the DPI architecture and functions. Section six purposes a new agile SDN based IoT network architecture. (SDNoT). Section seven disputes the conclusion and the challenges and future work.

2. IOT Architecture, Services And Challenges

Internet of Things (IoT) technology provides huge data for anything and everything in any time. IoT deals with connecting things together in a smart scalable way that provides many services and huge amount of data. IoT concept covers not only Internet as a network connects that nodes but also any existed network that may or may not interconnect with the Internet [4-5]. This coexisting of many different networks and heterogeneous devices need to be highly interoperable for supporting the required services [6-7]. Figure (1) shows that IoT merges heterogeneous technologies; cellular, WIFI, WIMAX, Sensor networks, etc. IoT enabling communication technologies are surveyed, protocols, and possible applications [4-5]. Many emerging technologies that are already existed such as SDN, NFV, DPI, cloud computing, Fog computing, new communication technologies, etc. , need to be efficiently adapted for integration with the IoT with its challenges [1]. Things are not limited to sensor, actuators, but includes human [8-9]. IoT should consider device to device, device to human and human to human. Real IoT should include agile mechanisms that could handle the connections with heterogeneous objects [7], [10] as well as supporting dynamic interaction between various internetworking networks via different media, gateways, network controller and different middleware [6]. Many architectures, protocols are required to cope with the challenges of the heterogeneity of IoT applications.

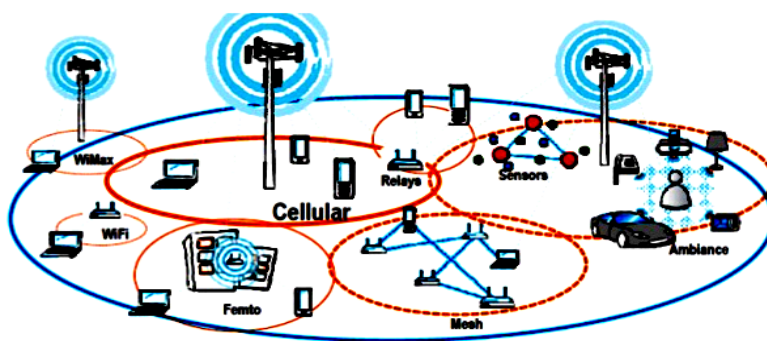


Figure 1. IoT merging heterogeneous technologies

2.1 IoT Architecture

For developing the IoT standards, many researchers provide different multi-layer based architectures. Although many IoT architectures were developed, there is no standard architecture existed [11]. Figure (2) shows the traditional three layer architecture compared to the service based one. Three layer based architecture is the traditional commonly used IoT architecture; application layer, network layer, and sensor layer [12][13]. *Sensor layer* or perception layer is the implemented bottom layer in IoT [12]. This layer deals with the physical interaction through smart sensors, actuators, etc. to measure, sense, collect, and control the devices. It processes the data to be transmitted to upper layer. *Network layer* or transmission layer receives the processed information from sensor layer, aggregates them and then computes how to route information to the IoT hub, switch, gateway, devices, and applications via networks and their various communication technologies (Bluetooth, ZigBee, NFC, LTE, etc). This layer is the most crucial layer since it manages highly heterogeneous devices, networks, communication technologies, etc. *Application layer* receives the data transmitted from network layer and provides required data services such as storage and analysis by using multiple technologies for data mining, analysis and visualization. *Service-oriented Architectures (SoA)* have recently been developed to support IoT [4], [10]. It is designed to connect/reconnect different application services via reusing software and hardware components, which improves the feasibility [4,5,10,14,15]. This is provided by considering an interface between network layer and application layer for service composition and management layer [15]. Application layer or Business layer works to provide complex service requests. Recently, even this service oriented needs more adaptation to comply with recent IoT application in the presence of highly efficient technologies like SDN.

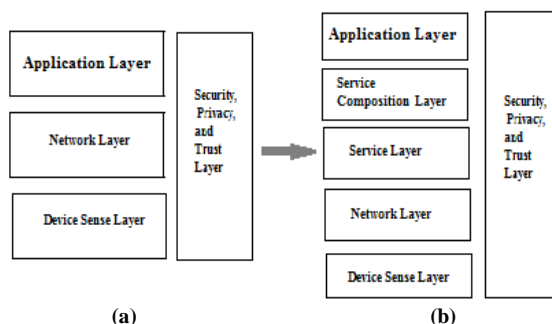


Figure 2. IoT architectures (a) Traditional Technology Architecture
(b) SOA based Technology Architecture [15]

2.2 IoT Protocols and standards

Since the IoT uses the Internet, it was logic to provide its protocol stack based on the one used in Internet which is the TCP/IP. Figure (3) shows the TCP/IP stack with their supported protocols for IoT that suffers from having multiple cross layering recently for sake of more efficient communication especially in the presence of wireless link in one of the IoT network hops [16-18]. Many low power protocols are specifically developed for the IoT in addition to the already developed ones [4,8].

Physical and MAC Layer: The IoT developed low power consumed protocols since it is used for communication among low power sensors. It supports low power communication along with low cost and short range communication which requires a small packet size (<127 bytes), low bandwidth (<250 kbps), and low transmit power (<1mW) with multihop routing over longer distances [19]. **Network Layer:** The network layer is responsible for routing the packets received from the transport layer based on distance vectors. For the scalability purposes, IPv6 is highly required in the IoT networks than IPv4. IPv6 normally consumes power. An adaptation layer; 6LoWPAN is introduced to adapt using IPv6 with less consumption power to be suitable to the low power wireless links such as IEEE 802.15.4. 6LoWPAN efficiently enables IP based devices communication by header compression, fragmentation and link layer forwarding.

Transport Layer: TCP could be used in some web applications but it is not suitable for low power devices because its well-known overhead. Therefore, UDP is preferred for most of the IoT applications for its low overheads. **Application Layer:** It is responsible for data presentation for different services. Although, HTTP is used in some applications especially for the web based application, it is not suitable for limited resource devices. Many IoT environments bases protocols were developed such as CoAP (Constrained Application Protocol) and MQTT (Message Queue Telemetry Transport). CoAP uses EXI (Efficient XML Interchanges) data format [20,21] over UDP, confirmable messages. MQTT is a publish/subscribe protocol that runs over TCP, was developed by IBM [22] primarily as a client/server protocol. MQTT is a lightweight protocol that uses text for topic names, which increases its overhead.

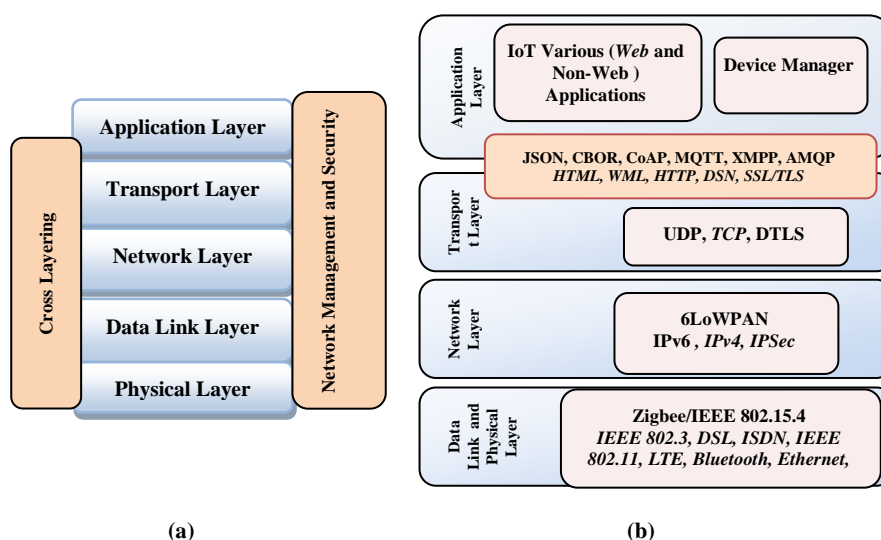


Figure 3. TCP/IP stack with(a) cross-layers (b) corresponding IoT layers

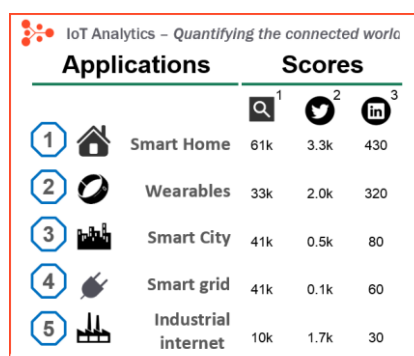


Figure 4. The most 10 popular IoT applications [23]

2.3 IoT Application And Services

The most ten popular IoT applications currently are announced [23]. A new company announces some IoT enabled product, some measures were carried out to know what the really popular IoT applications are right now [23]. Figure (4) shows the most 5 popular IoT applications based on the searching and social media measures based on monthly survey on Google, Tweeter, and LinkedIn. They are smart home, wearable devices, smart cities, industry 4.0, Smart transportation, Connected health, Smart retail, Smart supply chain and Smart farming

Smart homes are widely applied since it reflects directly on the quality of life and security of homes with available components, sensors, actuators with suitable price and consumable energy [36]. *Wearable devices* become a hot topic, since smart watch is developed. *Smart cities* is considered as one of the most complex applications. It covers a wide spectrum of use cases such as traffic management, water distribution, waste management, urban security, electricity management and environmental monitoring. It requires highly agile framework to offer efficient coupling the various types of applications or services (smart grid, smart transportation, smart health, environmental monitoring, etc) on heterogeneous devices [24]. *Padova Smart City* in Italy, has a trial [25],[26].

Smart grid is developed to efficiently utilize the distributed generated electricity. As a start, smart meters and bidirectional communication networks are introduced to provide smart, reliable, effective interactions between customers and utility providers [27]. Second step, is to provide reliable connection between these smart meters and provide more wide power grid that can help customer to optimize his consumption and improve the overall utilization from the dispatch side. *Industry 4.0* is the coming industrial revolution through smart manufacturing. The term “industrial IoT” efficiently drives manufacturing via connectivity, analysis, and automation. *Smart transportation* provides connect, monitor and control smart vehicles via wireless networks [28], [29] Each smart vehicle needs communication interfaces to have, vehicle-to-vehicle (V2V) communication and vehicle-to-Infrastructure (V2I) communication [28] for safety and non-safety messages [30]. *Health Care* system and smart medical devices for companies and people is highly promising

2.4 IoT Challenges

Although IoT based applications are widely developed, there is no existed generic infrastructure. Generic IoT infrastructure is required to efficiently merge multiple applications with using different integrated networks as in smart cities applications (smart health, smart transportation, smart grid, smart agriculture, etc.) [24]. This generalization requires centralizing the resource provisioning, network management, etc. which could be provided by using SDN and Cloud Computing. Many challenges faced IoT [5,32].

3. Software Defined Networking (SDN) Architecture And Its Provided Services

Software Defined Networking (SDN) provides dynamic network deployment and increased agility. Early SDN architectures focused on connectivity challenges at layers 1 through 3 of OSI model without paying enough attention to application-centric challenges at layer 4 through 7 of OSI model. Recent researches consider the other layers [1] Traditionally, router and switch provide controlling and management functions in the system to forward the packets. These complex controlling and management functions such as routing are done in each router provides high communication overheads, high computation, and scalability limitation. SDN inspired the concept of cloud in providing on demand of all the services in limited hardware devices. SDN takes care of the main computational hungry processes and left only the light forwarding processes to the hardware devices. SDN concepts start to be applied on the level of data center virtualization, then virtual central controlling of the core network that resides in data centers and going to be applied in virtual central controlling core network itself that could be resides on fogs or Mobile cloud computing MCC

3.1 Software Defined Networking (SDN) Architecture

SDN is the new architecture that has been designed to enable more agile and cost effective- networks. Simply, detach the network control and management from the forwarding devices such as the routers and the switches. In many dynamic applications, the demand for more software than hardware is increased because of agility requirements. The Open Networking Foundation (ONF) takes leading in SDN standardization. ONF provides an SDN architecture model as represented in Figure (5). OpenFlow specification has emerged as the main mechanism for separating data forwarding functions from control functions. OpenFlow is common way to do SDNs. SDN transforms the way that networks are managed, controlled, and used. SDN provides isolation between the hardware and the software in networking. As decoupling; the router role into the two planes the *control plane* and the *data plane*. The high-bandwidth *data plane* remains on the hardware platform, while the *control plane* (routing protocols, intelligence) is centralized. Open- Flow, or similar software protocols, provides a north-south interfaces between the control plane and data plane.

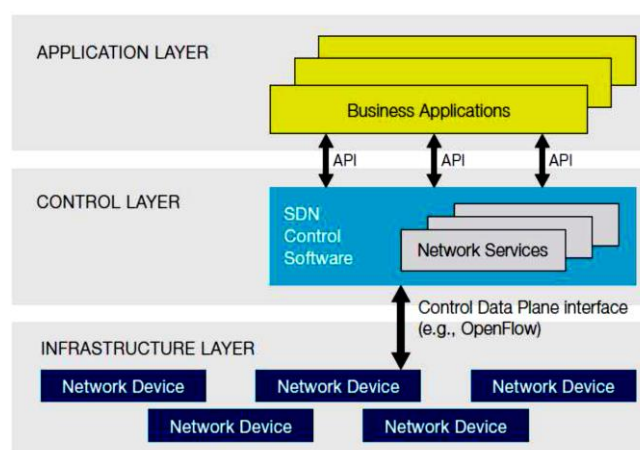


Figure 5. Basic ONF - SDN Architecture

SDN provides more agility programming for the networking management and controlling functions using logical centralized controller and connects to applications via standardized interfaces. SDN virtual centralization of the controller is a core principle,

providing an end-to end view of the network to users and applications. SDN is not just used for business and consumer applications but also for network security, optimization, policy, load balancing, and so on. RFC 3746, starts the concept of SDN architecture by logically separates two planes while residing in the same vendor equipment; without specifying that the control should be done in a centralized controller. Finally, SDN Offers;

1. Network services and Applications become irrespective to particular network physical devices.
2. Agile services can be enabled or disabled on demand basis.
3. Easy launch new services and applications.
4. More utilization for network virtualization, not only in cloud computing but also in different levels of network computing [37].
5. Allow using low-cost, high-performance commercial off-the-shelf hardware network devices; switches, routers
6. Allow replacing the complex routers that have both control and data layers with simple ones that have only the data layer.
7. Offers many more services such as routing, security, load balancing, policy management, etc. via vendor-specific APIs till becoming standardized APIs for all vendors.
8. Supports IoT and all other distributed applications

3.2 SDN Challenges

1. Allow interfacing with the current used complex routers to enhance the overall network performance.
2. Offers new services via standardized APIs for all vendors.
3. Radical impact of deploying current SDN standards such as OpenFlow on existing network operators that will require complete replacement of the existing network devices.
4. Offering hybrid deployment for the new SDN network devices with the existed traditional network devices as the transition step for the later major replacement step.
5. Lack of application awareness in controllers or virtual switches (vSwitches) to provide the required intelligence
6. SDN is limited to L2-4 and doesn't discriminate, and cannot efficiently manage enable the required service to each traffic type which burden the specialized systems to analyze the entire traffic.
7. Suffers from add some redundancy in processing in case of using other network intelligent as NFV and DPI.

4. Deep Packet Inspection (Dpi)

DPI provides advanced network management, Quality of Service (QoS), and security. DPI can work from Layer 2 to layer7 of OSI model. DPI inspiration was to analyze the network traffic to learn the traffic patterns and user behavior in order to be able to provide performance improving; bandwidth diminution, congestion control and QoS provisioning. DPI deployment has been widely and rapidly increasingly applied in all types of networks. DPI routinely tracks flows and packets to; identify applications, device type, session duration, connection frequency, traffic meta data, etc. *Traditional Shallow packet inspection* concerned with packet header inspection. It is network awareness and it covers layer 2-4 from OSI protocol layers. On the other hand, *Deep packet inspection* concerned with packet payload inspection. It is content awareness and it covers also layer 7 from OSI protocol layers

[33],[34]. Figure (6) shows the shallow (traditional) packet inspection versus the deep packet inspection.

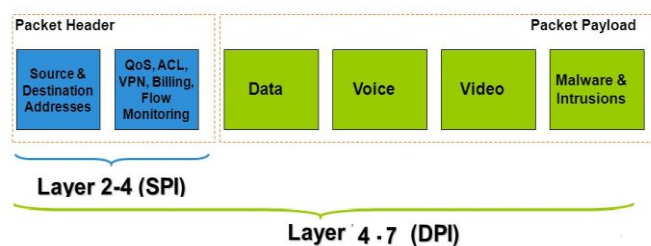


Figure 6. Deep Packet Inspection

4.1 DPI Deployment

DPI can also be found in network probes, which are often at the edge of the network. Other equipment that uses DPI includes load balancers and specialist security software [34]. There are two DPI deployment types, from the physical perspective:

1. DPI physical entity (DPI-PE): DPI Hardware device which can be located in certain places for different purposes. Figure (7) shows an example for DPI-PE deployment in fixed/mobile broadband networks [34]
2. DPI Functional entity (DPI-FE): DPI Software agents that can be deployed in commodity servers or nodes.

There are two DPI deployment scenarios, from the perspective of the end-to-end communication path:

1. Inline mode (known as "In-Path DPI" in: DPI-PE is deployed in a serial manner, the network traffic transverses entirely the DPI-PE.
2. Bypass mode (known as "Out-of-Path DPI" in : DPI-PE is deployed in parallel to the packet path, which implies that the network traffic needs to be duplicated and directed to DPI-PE.

DPI Motives for deployment are:

1. Identify high resource demanded applications such as video streaming traffic to manage their impact on network congestion
2. Understand and manage P2P network applications, since it has large portion of the networking services
3. Provide improve the QoS for Quality of Experience (QoE) applications
4. Provide policy definition and enforcement to guarantee for Service Level Agreement (SLA) based applications.
5. Offer customer traffic analysis to offer and adapt personalized their SLA
6. Offer monitoring web browsing habits for sake of targeted advertizing.
7. Offer the desired security level against different types of threats and attacks; spam, viruses, DDoS attacks, intercepts content systems.

Many DPI appliances are currently available. Although DPI was not specified by this name in some of the mobile network standards, it was implied by their functions. Emerging DPI engines into different type of networking devices (Layer 4-7 switches, gateways, policy and enforcement appliances, load balancers, Application delivery controller (ADC), specialized security appliances such as Intrusion detection (IDS) and intrusion prevention

(IPS)) offers more widely distributing for DPI functions (identifies applications in real-time and applies predefined policies) now and later. Since the QoE is increasingly demand in all applications, providers require big data that can be efficiently and gathered intelligently analyzed by DPI.

4.2 DPI Alongside of SDN

DPI provides *network application-aware*, while SDN provides *applications network-aware*. Although SDN will make radically change in the generic network architectures, it should cope with working with traditional network architectures to offer high interoperability. The new SDN based network architecture should consider all the capabilities that are currently provided in separate devices or software other than the main forwarding devices (routers and switches) such as the DPI, security appliances [34]. It should consider its policies, locations and possibility of the data redundancy that may be created. As noted earlier, the focus has been on Layers 2-3, not Layers 4-7. DPI is seeking to make the network application-aware (e.g., application identification, application measurement, application optimization, etc.). On the contrary, SDN aims at separating network control functions from physical network elements (related to packet processing only) and enable the network to be treated as programmable resource to applications, which means SDN is seeking to make the application network-aware. [34]. DPI PD-FE are widely used in the SDN architecture. Figure (7) shows an example application scenario of DPI in extended ONF SDN [34].

5. Network functions virtualization (NFV)

NFV promises operators a faster service roll out, along with improved capital and operating expense savings. NFV provides pool of compute and network resources to run virtualized instances of services or applications. This promising elasticity accelerates the roll-out of new services. NFV provides covering for the layer 4 to layer7 of OSI for efficient applications.

5.1 NFV Deployment

NFV is the way of replacing dedicated network appliances with software and automation. NFV environment is based on virtual network functions (VNFs). VNF handles specific network functions that run on one / more virtual machines (VMs), on bare metal, or in containers, on top of the physical networking infrastructure. NFV runs on generic servers and switches in virtual machines and is built with standard open APIs. NFV relies on open source development to provides agility, flexibility, and simplicity in a wide range of networking services. Network Functions that are usually carried out using network appliances in traditional network need configuration and reconfiguration. These functions are such as Firewall, Load balancing, Network Address Translation (NAT), Access Gateway, WAN Acceleration, QoS monitoring, DPI, etc. NFV provides these functions on demand basis by using virtual machine instead of physical hardware appliances. NFV offers the functions as VNFs running on top of commodity hardware [35]. Figure 8 shows NFV functional overview. The benefits of NFV implementation include but not limited to;

1. More Network flexibility via programmatic provisioning versus the rigorous hardware.
2. Open source software usage offers rapid developments.
3. Lower cost (operational expenditure (opex), capital expenditure (capex)) with better performance by replacing with commodity hardware rather than specific function hardware.
4. Reduced power consumption and space utilization

5. Orchestration efficiency especially in network complex applications in datacenters or for services providers.
6. SLA-driven resource allocation
7. Boosts performance and provides QoS
8. Application level infrastructure support

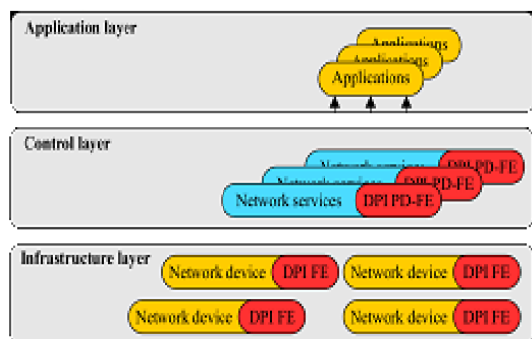


Figure 7. Example application scenario of D in extended ONF SDN [34]

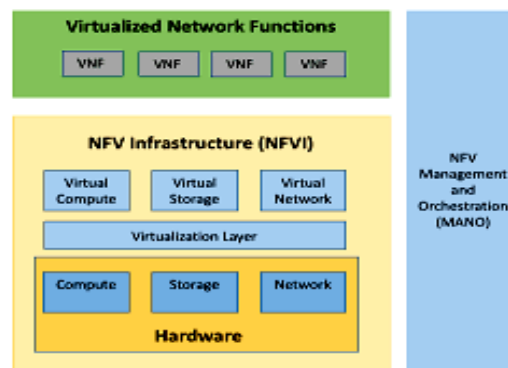


Figure 8. NFV functional overview [35]

5.2 NFV alongside SDN architecture

Although, NFV and SDN are complementing each other, they are independent solve different problems in different environments across different domains. SDN makes network devices programmable and controllable from a central element. NFV aimed at accelerating service innovation and provisioning using standard IT virtualization technologies. SDN requires new interfaces, control modules, and applications, while NFV typically involves moving networking applications to virtual machines or containers that run on commodity hardware [35]. Figure (9) shows the deployment junction of SDN and NFV. Hybrid NFV-SDN is highly important in a complex network such IoT. SDN flexibility in controlling and routing the network traffic is promising in agile networks with huge number of static and dynamic devices. NFV flexibility in provisioning network functions via virtualization also offers easily adding many functions and devices at any time. Therefore, virtualization can be applied to the data plane functions of the routers and other network functions, including SDN controller functions. So, either can be used alone, but the two can be combined to reap greater benefits [1]. Figure (10) shows the merging between the SDN and NFV architectures. Table 1 illustrates the comparison between NFV and SDN, although they are shared the theory of raw devices usage with advanced agile software in controlling these devices. SDN provides the agility of controlling the generic forwarding devices such as the routers and switches by using SDN controllers. On the other hand, NFV agility is provided for the network applications by using virtualized servers.

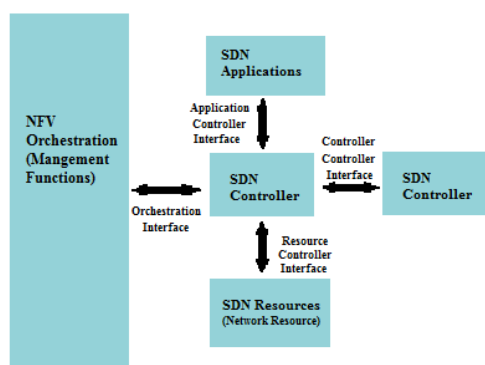


Figure 9. SDN and NFV deployment

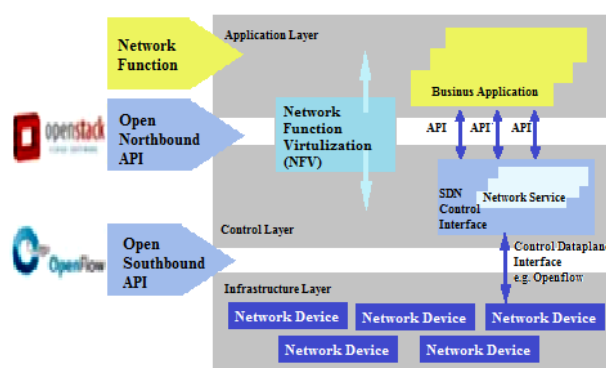




Figure 10. Hybrid SDN-NFV architecture

Table 1. SDN Versus NFV

	SDN	NFV
Basic Concept	Separate control and data layer in forwarding elements	Relocate the network functions from dedicated appliances to generic/virtualized servers
Target Location (Initiated by)	Enterprise network, Data Centers sectors	Service provider, Telecommunication sectors
Target Devices	Switches and Routers	Routers, DPI, Firewall, CDN
Standard Protocols	Openflow	Open Stack
Working Group	Open Networking Foundation 	ETSI NFV 
OSI Layer Stack	Focused (primarily) on L2-L4	Focused on L2-L7
Main Hardware	SDN Controller	Virtualized devices on Standard Commodity Server

6. Proposed agile SDN based IoT network architecture (SDNOT)

This paper presents an innovative agile SDN based IoT network architecture that considered an efficient merge of SDN, NFV and DPI for worldwide implementation of Internet of Things. Although, the DPI deployment will be functionally applied in SDN control plane as DPI-FE. DPI-PE may be needed in IoT networks or M2M networks near the end host. This boosts the deploying of the software based DPI agents over than the hardware based; DPI-PE. This will offer much better analysis capabilities, as well as simpler mechanisms for deployment, update, testing, and to scale it to changing workloads [33] .

Network intelligence becomes fully service-aware, therefore the merging between the DPI, NFV and SDN is highly required since they are complement each other. Although the term network intelligence was proposed before [33], it was not widely defined or used. IoT could be emerged when networking facilitates its requirements. IoT will excel when networking gains much more intelligence in controlling management of the available resources; devices, communication links .etc. Since Intelligence in networking requires being context aware of the application type, it should cover L4-L7. This was done in traditional network using cross layer approaches. In the new, intelligent network, NFV and some DPI-FE that applied on the network edge helps SDN to work more efficient. Since the paper proposes a new architecture for the wide heterogeneous IoT applications spectrum, there was an urgent

need to give a new classification for the IoT networking application based on its scale. IoT applications can be classified into two categories;

- Local IoT (LIoT): Isolated smart networks that are connected to the internet to enable monitoring and controlling simple objects; such as smart home and wearable applications.
- Wide IoT (WIoT): Wide distributed network that needs much more orchestration to enable the controlling and supervision of the whole network; such as smart grid and smart transportation

The proposed system architecture; SDNoT provides building wide range of LIoT and WIoT applications with utilizing intelligence and virtualization network system such as SDN, NFV and DPI. Figure 11 shows the SDNoT deployment. Structural Definition: The main layer in the intelligent network was recently defined as the data or infrastructure layer. This layer is the hardware layer that is better to be based on generic/commodity devices to be intelligently utilized (no need for having the power of intelligent devices). The second layer is the control layer that has the main control intelligently. The third one has the application and required services. There are also two main interfaces; the north and south which play vital role in manipulating the heterogeneity of the devices, and their data coming from the infrastructure layer. Traditional networks infrastructure faces many challenges to provide efficient IoT applications. Proposed SDNoT provides fixation for some of the IoT challenges in traditional networks infrastructure. Table 2 illustrates some provided solutions in SDNoT for some of the IoT challenges. Various IoT applications have many data types, QoS and Security requirements which are not easily and efficiently provided using the traditional network architecture, and therefore SDNoT provides agility for the various requirements for different IoT application. SDNoT utilizes the integrity of the SDN and NFV as well as the DPI in providing the rapid dynamic responses in the IoT real time application which can not be met by the traditional network. Figure 12 shows the SDNoT architecture to facilitate using the NFV in ISP alone or with the SDN for different IoT applications. Since a new classification is provided for IoT application, the figure 12 and figure 11 provide the suitable management for each case.

- LIoT: 1) May require only regular connection to the internet via a gateway. 2) May have only NFV for the efficiency. 3) may have NFV in addition to the DPI-FE in a Fog/Cloud Computing to facilitate more resources.
- WIoT: 1) May use NFV in the in addition to the DPI-FE in a Fog/Cloud Computing to facilitate more resources. 2) May use NFV in the in addition to the SDN and DPI-FE in a Fog/Cloud Computing to facilitate more resources.

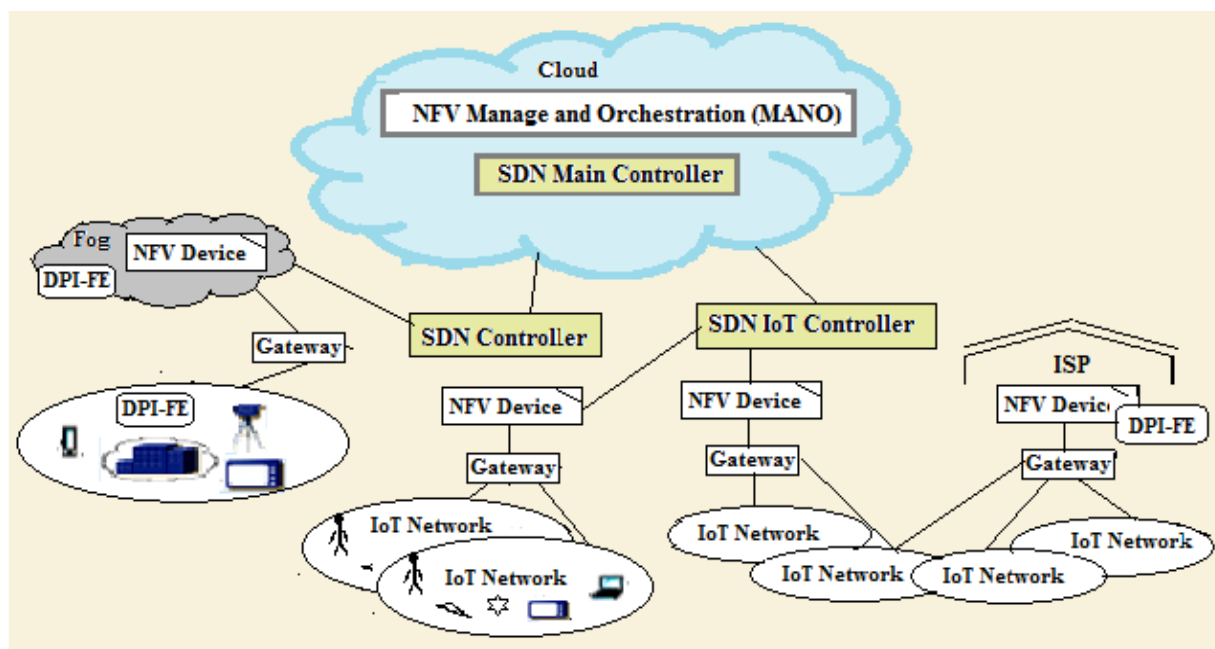


Figure 11. SDNoT deployment

Table 2 SDNoT against IoT Challenges

Traditional IoT Challenges	Solution With SDNoT
1. Lack of the application <i>context awareness</i> in controllers or virtual switches (vSwitches).	DPI-FE and metadata in SDNoT provide this much-needed awareness.
2. SDN is limited to L2-4 ; can't efficiently enable the required service to each traffic type	Provide intelligence for that based on DPI agents in switches to be able to pick up, manage and provide to each flow type individually. differentiate traffic between various types of L7 applications.
3. Need to <i>radically changes</i> of the Traditional network architecture to enable the requirements for IoT either by replacing equipments with smart ones or by having many cross-layering functions.	Facilitates SDN-Compatible hybrid approach with using traditional devices and proprietary appliances (non-OpenFlow) with SDNoT Ex1. Provide DPI agents/appliance, afford each switch to redirect each application flow to the required specialized service processing (FW, LB, video optimization, etc.) Ex2. With NFV, DPI can migrate from being embedded in each network appliance to being a shared function residing in standard switches and servers.
4. <i>Duplicate processing</i> inside numerous network devices and applications consuming resources	SDNoT environment, DPI and NFV are used by controller and applications to efficiently use the available resources (eg. CPU, memory, bandwidth, consumption) with less overwhelming.
5. SDN commonly standard used interface; <i>OpenFlow</i> doesn't have additional fields for the applications information.	SDNoT future infrastructure can provide encapsulation for OpenFlow fields with additional fields as Application IDs and some metadata for each flow. Later, this could be merged in the openflow standard to be used by all switches, gateways, controllers and applications.
6. In IoT, <i>heterogeneous devices/ human (Things)</i> , requires wide and <i>dynamic resources</i> (physical servers, processors, and operating systems).	SDNoT utilizes SDN and NFV which increasingly widespread use of server virtualization. To help in partitioning a single machine into multiple, independent virtualized servers, conserving hardware resources. Provides more flexible and quickly migration of a virtualized server from one machine to another for load balancing or for dynamic switchover in the case of machine failure.

Follow Table 2 SDNoT against IoT Challenges

Traditional IoT Challenges	Solution With SDNoT
7. IoT applications induce <i>Big data demands</i> . Server virtualization is the central element in dealing with the dynamic demand big data applications. Virtualization is difficult in managing in the traditional networks	Virtualization is difficult in managing in the traditional networks architecture in case of rapid changing of workload and interfaces. network manager needs to be able to dynamically add, drop, and change network resources and profiles via utilizing SDN and NFV in SDNoT
8. IoT heterogeneous devices (smartphones, tablets, and Notebooks, sensors) induce <i>dynamic rapid response</i> demand that difficult in application in traditional network switches	Dynamic in rapid response demand could be managed by offering the isolation between the controlling and the switches which is offered by SDNoT . SDNoT can offer agility with the changing the network workload via utilizing the SDN.
9. The <i>mobility</i> of some of IoT devices provides rapid attach/detach points .	SDNoT provides intelligent managemet through using SDN and DPI for mobile devices
10. IoT variable requirements for the management of traffic flows, <i>QoS levels and security levels</i>	Existing network traditional infrastructures may provide some kind of IoT requirements on expense of much time-consuming especially in case of using multiple vendors devices which requires separate configuration for controlling performance and security parameters on a per-session, per-application basis, per device, per each creation/changing of the VM. SDNoT smoothly and efficiently provides the variable requirements of QoS and security levels via using SDN and NFV .
11. Heterogeneity in IoT used in <i>LAN and WAN scales</i>	SDNoT proposes wide scalable solutions for different IoT applications.
12. <i>Low power devices</i> ,	SDNoT provides migrating most of the hungry processes from the low power devices into the virtualized severs and the SDN controllers.

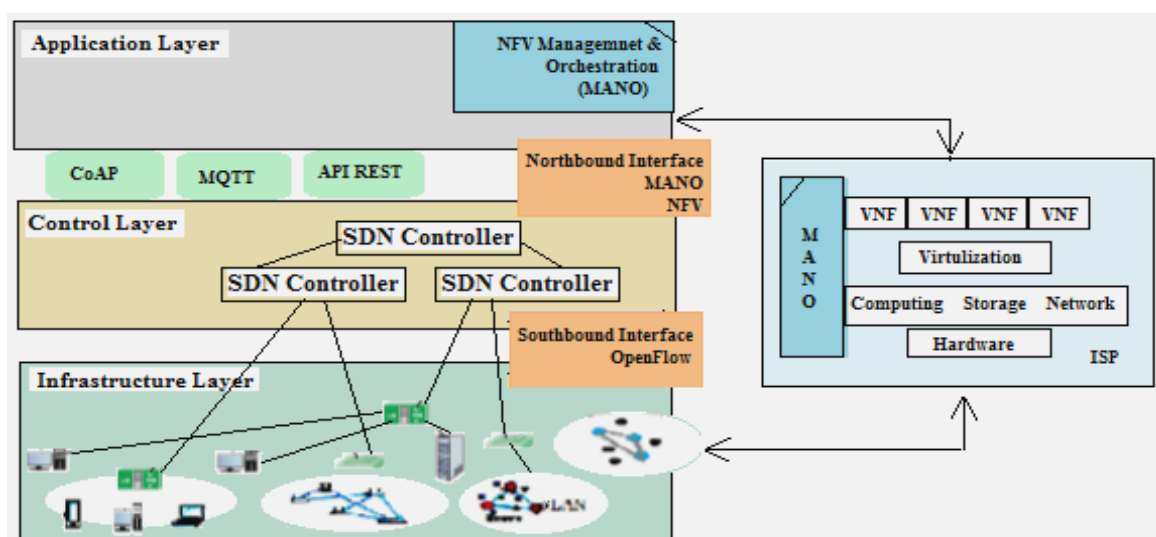


Figure 12. SDNoT architecture

6. Conclusion

Network Computing brings multiple enabling technologies into different level of services and applications. IoT is a new wide multi-technologies application that faces a main challenge in managing complex heterogeneous nodes network. SDN redistribute the network logics management among nodes and central controller. SDN framework can be adapted

dynamically for different required approaches for different IoT application scales. The paper provides a vision on expanding the need for convergence of SDN and NFV into a swift, Self-organization, self-healing scaled IoT network in heterogeneous environments. The proposed agile framework dynamically matches software defined network services with the IoT requirements. Dynamic agile framework is Internet of thing using software defined network (SDNoT) with the presence of already existed NFV and DPI. It also offers more operability for the transition transferring period from traditional network to fully SDN based Network. In Future work; the proposed framework needs to be deployed to examine and analyze its performance in case of having a SDN controller compared to distributed SDN controllers.

References

- [1]. William Stallings, " Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud" Pearson Education, 2016.
- [2]. Jie Lin_, Wei Yuy, Nan Zhangz, Xinyu Yang_, Hanlin Zhangx, and Wei Zhao, " A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", *IEEE Internet of Things Journal* , pp 1125 – 1142, Volume: 4, Issue: 5, Oct. 2017
- [3]. "Verizon Network Infrastructure Planning :SDN-NFV Reference Architecture v1.0", White paper, Feb. 2016
- [4]. A. Al-Fuqaha et. al. " Internet of things: A survey on enabling technologies, protocols, and applications",. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, 2015.
- [5]. L. Atzori, A. Iera, and G. Morabito. ,"The internet of things: A survey", *Computer Networks*, 2787–2805, Oct. 2010.
- [6]. M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont)", *Internet Technologies and Applications (ITA)*, pp.216-222, Sep. 2015.
- [7]. J. Wu and W. Zhao. Design and realization of winternet: From net of things to internet of things. *ACM Transactions on Cyber-Physical Systems*, 1(1), Article 2, 12 pages , November 2016.
- [8]. J. A. Stankovic, "Research directions for the IoT",. *IEEE Internet of Things Journal*, 1(1):3–9, Feb.2014.
- [9]. J. Tan and S. G. M. Koo,"A survey of technologies in internet of things". *IEEE International Conference on Distributed Computing in Sensor Systems*, pp. 269-274 May 2014.
- [10]. L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey", *IEEE Transactions on Industrial Informatics*, 10(4):2233–2243, November 2014.
- [11]. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan., "Internet of things (iot) security: Current status, challenges and prospective measures", 10th *International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336--341.December 2015.
- [12]. L. Atzori, A. Iera, G. Morabito, and M. Nitti., "The social internet of things (siot) when social networks meet the internet of things: Concept, architecture and network characterization", *Computer Networks*, 56(16):3594 – 3608, November 2012.
- [13]. M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du., " Research on the architecture of IoT", 3rd *International Conference on Advanced Computer Theory and Engineering (ICACTE)*, volume 5, pp. 484-487, Aug. 2010.

- [14]. L. D. Xu. , " Enterprise systems: State-of-the-art and future trends", *IEEE Transactions on Industrial Informatics*, 7(4):630–640, November 2011.
- [15]. H. Suo, J. Wan, C. Zou, and J. Liu., "Security in the internet of things: A review", *International Conference on Computer Science and Electronics Engineering (ICCSEE)*, volume 3, pp.648-651, March 2012.
- [16]. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", *Journal of Electrical and Computer Engineering* , Article ID 9324035, 25 pages, Volume 2017 (2017)
- [17]. Rowayda A.Sadek, Aliaa Youssif and Amal Elaraby, "MPEG-4 Video Transmission over IEEE 802.11e Wireless Mesh Networks using Dynamic-Cross-Layer Approach", *National Academy Science Letters, Springer* , April 2015, Volume 38, Issue 2, pp 113–119
- [18]. Amal Elaraby, Rowayda A.Sadek and Aliaa Youssif, "MPEG-4 Video Transmission over IEEE 802.11e", *IEEE- 2014 31st National Radio Science Conference (NRSC)*, pp. 236-243, Cairo, Egypt, April 2014.
- [19]. J. P. Vasseur, C. P. Bertrand, B. Aboussouan et al., "A survey of several low power link layers for IP smart objects," White Paper, IPSO Alliance, 2010
- [20]. W. Colitti, K. Steenhaut, N. De Caro, B. Buta, and V. Dobrota, "Evaluation of constrained application protocol for wireless sensor networks," 18th IEEE Workshop on Local and Metropolitan Area Networks (LANMAN '11), pp. 1–6, IEEE, USA, October 2011.
- [21]. Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," Tech. Rep., RFC7252, IETF, 2014.
- [22]. D. Locke, "MQ telemetry transport (MQTT) v3. 1 protocol specification," IBM developerWorks Technical Library, 2010, <http://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html>.
- [23]. IoT analytics (Update Q3/2016), Web Site: <https://iot-analytics.com/10-internet-of-things-applications/>
- [24]. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, February 2014.
- [25]. P. Casari, A. P. Castellani, A. Cenedese, C. Lora, M. Rossi, L. Schenato, and M. Zorzi., "The wireless sensor networks for city-wide ambient intelligence (wise-wai) project". *Sensors*, 9(6): pp. 4056-4082, May 2009.
- [26]. N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi., "The deployment of a smart monitoring system using wireless sensor and actuator networks", *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 49-54 October 2010.
- [27]. J. Lin, W. Yu, and X. Yang, "Towards multistep electricity prices in smart grid electricity markets", *IEEE Transactions on Parallel and Distributed Systems*, 27(1):286–302, January 2016.
- [28]. M. Khanjary and S. Hashemi., " Route guidance systems: Review and classification", *6th Euro American Conference on Telematics and Information Systems (EATIS)*, pp. 269-275, May 2012.
- [29]. R. Kim, H. Lim, and B. Krishnamachari., " Prefetching-based data dissemination in vehicular cloud systems", *IEEE Transactions on Vehicular Technology (TVT)*, 62 (1), 292-306, January 2015.

- [30]. Islam Z. Ahmed, Taha M. Mohamed, Rowayda A. Sadek, "A Low Computation Message Delivery and Authentication VANET Protocol", 12th IEEE International Conference on Computer Engineering and Systems (ICCES2017), Cairo, Egypt, pp.204-211, December 2017
- [31]. A. P. Athreya and P. Tague.; "Network self-organization in the internet of things", *IEEE International Conference on Sensing, Communications and Networking (SECON*, pp. 25-33), June 2013.
- [32]. K. Sha, W. Wei, A. Yang, and W. Shi; "Security in internet of things: Opportunities and challenges" International Conference on Identification, Information & Knowledge in the IoT, pp. 512-518 Oct. 2016.
- [33]. Graham Finnie , December 2012 | White Paper | The Role Of DPI In An SDN World
- [34]. Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks, ITU-T Y.2770 series – Supplement on DPI use cases and application scenarios, 05/2015
- [35]. Network Function Virtualization: Use Cases; ETSI GS NFV 001 V1.1.1 (2013-10), http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf
- [36]. Sarah Osama, Marco Alfonse, and Abdel-Badeeh M. Salem, "Intelligent Techniques for Smart Home Energy Management Based on Internet of Things (IoT) Paradigm", Egyptian Computer Science Journal Vol. 41 No.3, pp.33-43, September 2017
- [37]. Mona Saad Khalil Morgan, " Comparative Analysis of Cloud and Grid Computing Paradigms", Egyptian Computer Science Journal Vol. 41 No.3, pp.53-76, September 2017