COVID-19 and Nigeria's National Policy on Virtual Meetings

By Emmanuel Okewu

Health challenges posed by the Corona Virus Disease 2019 (COVID-19) means safety of workers, like any other segment of the population, has to be prioritized (WHO, 2020). COVID-19 is a highly infectious global pandemic that originated in China (Hange, 2020; Ahmad et al., 2020). To reduce physical contacts during meetings, Ministries, Departments and Agencies (MDAs) have started conducting virtual meetings (Vanguard News, 2020). This consolidates the e-governance drive of the government and stimulates greater sense of the digital economy.

The first incidence of COVID-19 in Nigeria was reported on 27th February, 2020 in the commercial city of Lagos (NCDC, 2020). The metropolitan nature of Lagos and its status as the economic nerve centre of Nigeria quickly reflected in the spread of the virus across the country. This has forced many states to implement COVID-19 protocols such as physical distancing; regular hand washing, use of sanitizers and wearing of face masks (Ohia et al., 2020). Though the index case was through international travel, currently community transmission is responsible for the spread. Though there is currently no vaccines for the virus, studies have shown that strict observance of preventive guidelines could be effective (Unhale et al., 2020; Gennaro et al., 2020; Rothan and Byrareddy, 2020).

The civil service remains the engine room of any economy as it provides the machinery for the implementation of public policies, programmes and projects. Safeguarding public servants is therefore key to sustained socio-economic development. Physical distancing apart, other COVID-19 protocols for a safe workplace are indicated in Figure 1.

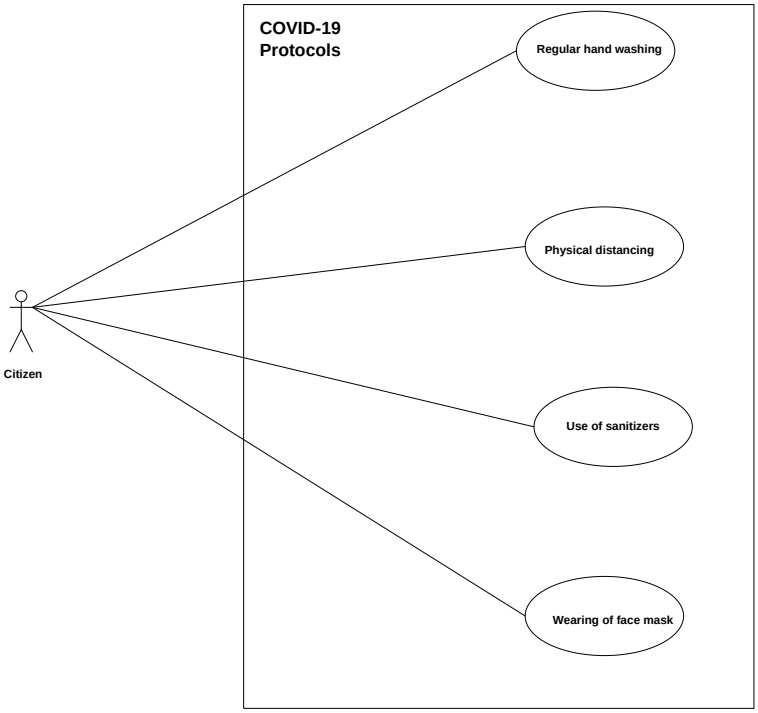

Figure 1. COVID-19 Prevention System

A minimum distance range of 1.5m to 2.0 m has been benchmarked as safe physical distance between individuals (NCDC, 2020). Other measures as indicated in Figure 1 include wearing of face mask, use of sanitizer and regular hand washing. COVID-19 is highly infectious, air-borne

and transmits through droplets, hence the need to adhere to these preventive actions (measures) by every citizen (CDC, 2020; Shereen et al., 2020).

Initially, the Nigerian Government enforced total lockdown in selected cities like Lagos, Abuja and Ogun. International travels, domestic flights and inter-state travels were also banned. Private businesses and government offices were also shut down. And at both national level and sub-national levels (state and local government), various precautionary measures were activated through relevant institutions as indicated in Figure 2.

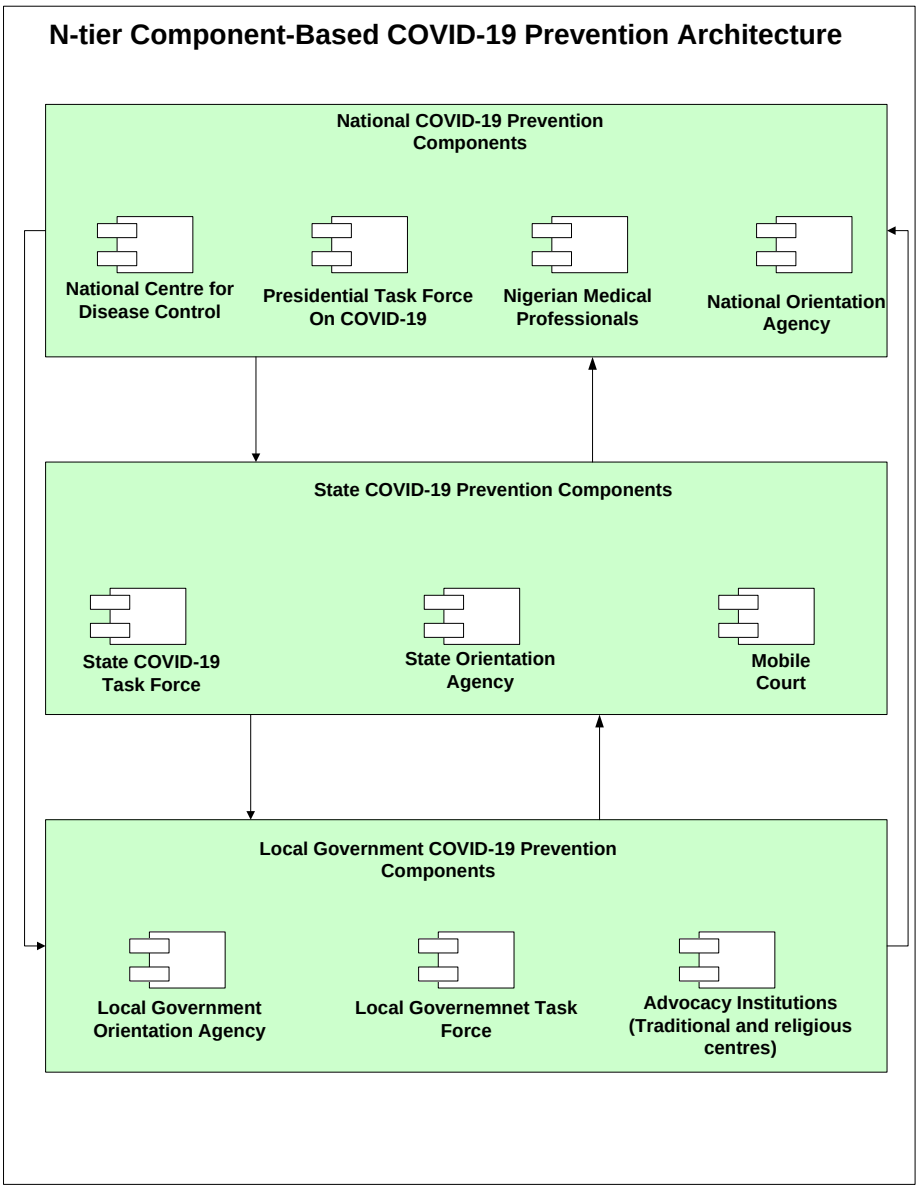

Figure 2. N-tier Component-based Architecture for Nigeria's COVID-19 Precautionary Measures

As indicated in Figure 2, the COVID-19 Task Forces at national, state and local levels enforced lock-down orders, wearing of face masks, regular hand washing and use of sanitizers. The National Orientation Agency and other institutions intensified awareness-creation efforts while offenders are prosecuted by Mobile Courts set up by State Governments. These measures impacted adversely on lives and means of survival. While trying to save lives through stay-at-home order, jobs suffered and the economy nose-dived. To balance safeguarding of lives and sustaining livelihoods,

Government has started implementing gradual easing of the lockdown through the Presidential Task Force on COVID-19.

COVID-19 has changed life style and introduced new normal in all spheres of human endeavor. A new normal that engineers novel work culture is virtual meeting. Though the private sector has been using online meetings to cut cost over the years, same cannot be said of public sector where government officials are interested in travelling for meetings for pecuniary reasons even when such meetings could be hosted online. As a matter of policy, Government has directed that until further notice, MDAs are to avoid physical meetings as much as possible. To sustain the economy, meetings are to be conducted virtually, thereby deepening digital economy in Nigeria. This implies board meetings, extra-ordinary meetings, etc. are to be online real-time. Like any other aspect of the application of information and communication technology for accelerated business processes, virtual meetings need to be regulated to guide against abuse (Dariem, 2020). The Federal Government of Nigeria through the Ministry of Communications and Digital Economy has therefore formulated a National Policy on Virtual Meetings (NPVMs). The feat was achieved in collaboration with the Office of the Head of Service.

The new policy is in sync with the National Digital Economy Policy and Strategy Document (NDEPSD). As encapsulated in NDEPSD, the National Policy on Virtual Meetings will consolidate two pillars: Pillar 4 which is Service Infrastructure and Pillar 5 that focuses on Digital Services Development and Promotion (Adaramola, 2020). The development of the NPVM document is a deliberate measure to promote virtual meetings and engagements for civil servants in a bid to curb the spread of COVID-19. It is also aimed at adapting to the new normal. In a way, the COVID-19 pandemic is helping government to realize its age-long dream of adopting the use of technology in governance. A regulatory framework like NPVMs will ensure e-governance is conducted in an orderly manner.

As the Nigerian cyberspace gets more intensive with nation-wide implementation of online meetings, cyber security experts are quick to point out security implications. Already, all over the globe, there have been reports of hackings of virtual meeting applications such as Zoom, Microsoft Team, Google Meet, among others. Huge and sensitive datasets are transmitted online, making virtual meetings attractive to hackers. It is compelling therefore to put in place efficient and dynamic cyber security measures to protect strategic data.

It is hoped that with the measures put in place at the international, national and sub-national levels which include search for the vaccine and the use of virtual meetings, the pandemic would soon be contained. Equally important is the fact that the ideals of virtual meetings are being internalized and institutionalized for cost-efficient operations in both the private and public sectors.

Emerging Threats in Cybersecurity

Agboola Sodiq Aremu

Today the Internet is a indepensable tool for daily existence. In the present specialized condition numerous most recent technologies are changing the face of the humanity. Be that as it may, because of these developing technologies we can't shield our private information in a powerful manner and thus nowadays cyber crimes are expanding. Today in excess of 60 percent of absolute business transactions are done on the web, so this field required a high caliber of security for security of transactions. Thus cyber security has turned into a most recent issue. The extent of cyber security isn't simply restricted to securing the information in IT industry yet additionally to different fields like cyber space.

Information and Communication Technology (ICT) structures are used basically in a wide range of various foundations. Most affiliations, establishments, associations and government parastatals today depend upon Computer networks to finish both straightforward and complex business exercises, participate in technological advances, and perform interdependent financial trades. Advances in technology have given empowering new openings and focal points, regardless, they have in like manner inspired weakness to crime. Today, as computer structures have turned out to be faster and ended up being even more technologically advanced, cybercriminal activity has exacerbated. The ICT part is dynamically mishandled by jobless energetic adults searching for a basic course to riches, from this time forward the ascent of a subculture called Cybercrime or Computer Oriented Crime. Cybercrime costs various affiliations and administrative bodies generally billions of dollars consistently.

The Internet is by and large an antagonistic situation where attacks can be simple, cheap and might be difficult to avoid, detect or follow. The outcomes are in any case, uncommon as far as time and cash. All in all, it is hard to guarantee the fundamental security objectives which are confidentiality, uprightness and accessibility. There are numerous explanations behind the present security risks on the Internet, the Internet was designed to be an open and disseminated condition with no focal example controlling the correspondence among the clients and common doubt was not of essential concern. It is an offense completed against individuals or social events of individuals with a criminal manner of thinking to purposely make hurt the reputation of the loss or to make physical or mental harm the loss whether explicitly or in an indirect manner, using present day media transmission networks, for instance, internet and mobile phones. Cybercrime consolidates criminal activity against information, copyright, fraud, unapproved get to, tyke sexual amusement, cyber stalking, catching, hacking, phishing stunts, computer/adaptable contaminations, cyber dread based persecution, Mastercard thievery, financial equalization number, etc.

Numerous cybersecurity specialists accept that malware is the key decision of weapon to do pernicious plans to break cybersecurity endeavors in the cyberspace. Malware alludes to a wide class of attacks that is stacked on a system, regularly without the learning of the legitimate proprietor, to bargain the system to the advantage of a foe. Some praiseworthy classes of malware incorporate infections, worms, Trojan steeds, spyware, and bot executables (Jang-Jaccard and Nepal, 2014). Upgrading cyber security and ensuring basic information frameworks are fundamental to every country's security and financial prosperity. Making the Internet more secure (and ensuring Internet clients) has turned out to be indispensable to the advancement of new benefits just as administrative policy. The battle against cyber crime needs an extensive and a more secure methodology. Given that specialized measures alone can't avert any crime, it is important that law requirement organizations are permitted to explore and indict cyber crime viably. Today

numerous countries and governments are forcing severe laws on cyber securities so as to avert the loss of some significant information. Each individual should likewise be trained on this cyber security and spare themselves from these expanding cyber crimes. This paper will review the most recent threats to cyber security rose with technologies and methods like cloud computing, IOT, Drones, Big Data, etc.

The Concept of Cybersecurity

In the course of recent years, specialists and policymakers have communicated expanding worries about shielding ICT systems from cyberattacks intentional endeavors by unapproved people to get to ICT systems, for the most part with the objective of robbery, interruption, harm, or other unlawful activities. Numerous specialists expect the number and seriousness of cyberattacks to increment throughout the following quite a long while (Rainie et al., 2014). The demonstration of securing ICT systems and their substance has come to be known as cybersecurity. An expansive and ostensibly to some degree fluffy idea, cybersecurity can be a valuable term yet will in general challenge exact definition. It for the most part alludes to at least one of three things:

A lot of exercises and different measures proposed to shield from attack, interruption, or different threats computers, computer networks, related equipment and devices programming and the information they contain and impart, including programming and data, just as different components of cyberspace.

2 The state or quality of being shielded from such threats. The wide field of undertaking planned for actualizing and improving those exercises and quality.

As per Baker and Wallace (2007), security approaches characterize activities that can and can't be taken with organization computers. The arrangements layout the adequate activities and utilization of public college's computers and networks by its workers (Metzler, 2007). Information security strategies relate to composed documentation sketching out the structure of the association's security pose. The motivation behind information security involves the protection of confidentiality, honesty and accessibility. Also, authenticity, accountability, non-denial and reliability are different components which relate to information security. Hence, security strategies furnish direction concerning the physical and remote access to data of the public college. Bidgoli (2006) sees that there are three classes of information security arrangements; network security strategies, server security approaches and application security strategies. Liska (2008) takes note of that cut off security approaches help to forestall setup irregularities and causes administrators to react productively to security episodes while network security approaches target securing the network. Then again, application security strategies mean to reliably authorize application security around an association application framework.

2.1.1 Definition of Threats

Cyber threats to states might be characterized as those on-screen characters or foes displaying the strategic conduct and capacity to abuse cyberspace so as to harm life, information, activities, the earth as well as property. The cyber threat scene isn't really progressive (Andersonet al., 2012). The exercises that entertainers representing a threat can embrace are equivalent to those in reality: crime, insight social event and surveillance, ideological activism and 'warfare'. These threats exude from a scope of sources: from displeased insiders to sorted out crime, identity hoodlums and psychological oppressor or dissident gatherings to antagonistic states and their intermediaries. Country state dependence upon cyberspace implies that this area has turned into an inexorably appealing objective for different types of adversary.

2.1.2 The Nature of Threats

Cybercrime arrives in an assortment of structures going from refusal of administration attacks on websites through to robbery, blackmail, coercion, control, and annihilation. The tools are numerous and changed, and can incorporate malware, ransomware, spyware, social designing, and even modifications to physical devices (for instance, ATM skimmers). It's nothing unexpected then that the sheer extent of potential attacks is tremendous, an issue compounded by what's known as the attack surface: the size of the powerlessness displayed by equipment and programming. That is, if a hacking endeavor chips away at Apple iPhones for instance, and everybody in your association has one, at that point by definition the attack surface could go in the handfuls to the thousands relying upon the size of your organization. Or on the other hand, taking a gander at it another way, in the event that anybody with an iPhone is helpless, the attack surface overall sums in the several millions (ACS Cybersecurity, 2016).

Emerging Cyber Security Threats

Every country over the globe is experiencing diverse kind of threats. Basically, any undertaking of Securing the Web and remaining in front of rising threats could be an overwhelming Job; notwithstanding for PC customers who are unreservedly quiet with the technology and language of security authority. There isn't seven days that goes without reports of a Virus infection, Hacking endeavor or 'Phishing trick'. Therefore, different PC customers, even those individuals who have introduced security software, for example, Firewalls, hostile to infection and exact filtering software could be at risk to security threats and software breaks (Babate et al., 2014). Normally these threats could be identified into malicious, network attacks and network abuse. Malicious incorporate computer viruses, spyware, Trojan ponies, key lumberjacks and BOTS. Network attacks incorporate session hijacking, disavowal of administration (DOS), and satirizing and web defacement. In like manner Network abuses incorporate SPAM, phishing, and pharming and essentially a portion of these threats are disclosed beneath as for their Network related fraud cases:

Phishing and email Spamming

This can be defined as a type of threat through the internet, or flooding of the Internet or any unwanted online correspondences. The requests gathers client's credentials using a deception technique. In order way phishing could be described as an Internet fraud in such a way that the attacker will acquire details like, stealing of passwords, bank account details, credit card numbers and other private information (Babate et al., 2014). In recent times, law enforcement agencies and the judiciary appear to be taking cyber-crime more seriously. As in the case of July 2011, an individual was evidently 'sentenced to more than twelve years in federal prison for his conduct in an international phishing and email spamming ring that stole the identities of more than 38,000 people' (Raymond, 2011).

Botnet

A Botnet is a guard of compromised Systems, sometimes called "zombies," that are under the command and control of a solitary "Botmaster." (Babate et al., 2014). A botnet are accumulation of computers networked together that are no doubt regulated by Cybercriminals for malicious and unlawful purposes. Botnets are currently turning into a key threat for the cybercrime since they are designed deliberately to disturb targeted computer systems in so many different ways. Many infected computers can figure out how to disturb and disseminate malicious code, virus and spam (Babate et al., 2014). Figure 1 describes the life cycle and approaches for detecting botnets, and how to combat the growing concern of Bots.

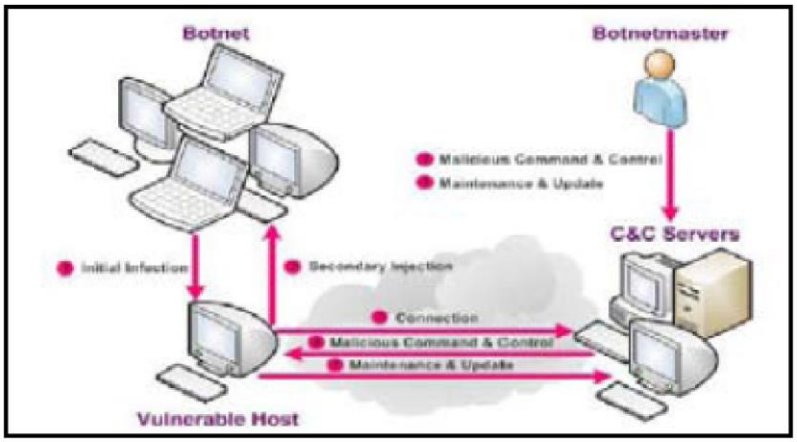

Figure 1: A typical Botnet life Cycle(Babate et al., 2014).

Malware and Spyware

These are malicious program designed to gather computer information without the awareness of the client. Symantec (2011) reportedly identified Malware as one of the key threats to Businesses, Governments and people. For instance, in 2009 the number of new malware signatures was accounted to be just under 2.9 million, a 71 percent increase over 2008, yet more than 286 million new malware variants were discovered by Symantec in 2010. The movement in motivation from interest and fame looking to illegal budgetary increase has been marked by a growing sophistication in the evolution of malware.

Key loggers

Key loggers are programs that can screen and record the client keyboard information while typing into Computer System for later access. Key loggers store the data or send the information secretly to the other programs. They can record usernames, massages and secret key for remote systems and computer application. Some key loggers oblige the right to gain access of the criminal invader or attacker to get the data from the machine while other forcefully transfers the data to different machines by means of email; file transfers etc. Sagiroglu and his Colleagues further find out that the personal use of keyloggers can be beneficial, because the use of keylogger may assist private computer owner to enhance his daily routine with much privacy. With keylogger is possible to recuperate content wrote into word processors, spreadsheets, and computer programming environment after an application or system crash (Babate et al., 2014). Social Engineering ‘Social Engineering (SE) is a developing Science that plays on the trust Component of the human intelligent’. Social engineering is a kind of technique in which it traps or tricks the client to reveal valuable information. The user will think the reason is honest to goodness yet the aim is truly criminal.

Denial of Service (DOS)

This is an attack that upsets the ordinary function of the computer system and thus prevents access to authorized users. Karthik, define DoS attack as an incident in which a Client or organization is deprived of the services of a resource they would regularly expect to have (Babate et al., 2014). DoS is legitimately a resource overloading attacks that may have the likelihood of either smashing the host such that it can't communicate properly with the rest of the System, in this way the services may remain inaccessible to customer clients.

Virus

A virus is a program that spreads itself from one computer to another computer without the users' authorization to do so, and they distribute themselves to the infected files or programs of a PC. Viruses cause negative and unforeseen event when the machine runs. Different kind of viruses has distinctive purpose. Some are designed to trap clients and some are designed to destruct Machine programs. They can harm computer programs and they are actually presented through email attachments (Babate et al., 2014). Consequently computer virus can additionally be spreads by connecting itself to executable files of systems areas, on external storage devices such as USB plash drives.

Worm

A worm is usually a computer Program that moves itself from one machine environment then onto the next machine environment often keeping record of the last environment it has entered. Worms are self-duplicating programs towards oneself which essentially implies that they don't require a host program to attack a victim. When a worm moves to another environment it can do whatever it needs as per the obligatory access controls (Babate et al., 2014). In the case of Virus it requires human intervention but worms do not and it moves round via the internet connection.

Cloud Threats

As more and more organizations are shifting focus on saving data on clouds and using cloud computing more, cloud computing security is at risk. As per McAfee Labs 2017 Threats Predictions November 2016: Cloud service providers are building trust and gaining customers. Increasing amounts of sensitive data and business critical processes are shifting to public and hybrid clouds. Attackers will adapt to this shift, continuing to look for the easiest ways to monetize their efforts or achieve their objectives (McAfee Labs, 2017).

IoT Threats

The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. As per my literature review the year 2017 will bring a large scale IoT security breach, with ecommerce, manufacturing plants, and government organizations at the biggest risk, according to experts. In the past year, IoT security has quickly emerged as a hot issue with multiple threats against the enterprise such as the Mirai botnet (Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots (Software Robot", that can be used as part of a botnet in large-scale network attacks) It primarily targets online consumer devices such as remote cameras and home routers, that affected Twitter, Amazon, and Netflix. What's most alarming, however, is that it's likely only the beginning as more companies deploy IoT sensors and devices across their networks. The Threats n affects will be seen more in 2017 as IoT increases and more and more organizations get evolved.

Ransom Ware

Ransomware is a growing threat that encrypts a user’s files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many

antivirus and intrusion detection systems. In this work, we present CryptoDrop, an early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. Furthermore, by combining a set of indicators common to Ransomware, the system can be parameterized for rapid detection with low false positives. Our experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Our results show that careful analysis of ransomware behaviour can produce an effective detection system that significantly mitigates the amount of victim data loss (Scaife et al., 2016).

Drone jacking

Drones (Unmanned Ariel vehicle) which have become more and more talk of the town these days. Some consider this as a toy for fun some may use it for intruding privacy. What started as a fun toy for kids and a slightly expensive hobby for fanatics has really taken off. Drones are well on the way to becoming a major tool for transporters, law agencies, photographers, the news media, or be it covering the telecast of cricket match and more. We cannot deny the fact that drones are becoming more valuable to businesses and government agencies. As we know Amazon made its first ever delivery of product via drone in December 2016 in US and also dominos delivered its pizza in New Zealand via drone, such is the acceptability and increasing craze for using drones to reduce delivery times and attract more customers (Ali et al., 2017). In the coming year we could see hackers deploy drone over offices or houses for intruding privacy or intercept official communication which could be a major threat to cyber security. As per David Latimer, a researcher on the project, said large companies have not properly prepared for this threat. "A drone could just go land on the roof, sit there and record people's keystrokes, and access the internal network over the wireless".

Threat to Big Data

Establishments have become very dependent on big data, using it in almost every major decision that they have to make. While data analysis is certainly helpful in many areas, some businesses are starting to forget that human intuition is also important. By taking humans almost out of the process, many fear that decisions may begin to suffer. Big data isn't always correct, and using it as the only basis for decisions could result in poor decisions, security vulnerabilities, and other issues. Business owners need to question the validity of their data, their code, and all other information to make certain that the information they're using is correct and current. Many efforts on big data are focused on the 3V challenges today. However, the flourishing of big data relies not only on the promised solutions for 3V challenges, but also on the security and privacy challenges in big data analytics (Ali et al., 2017). It is likely that if the security and privacy challenges are not well addressed, the concept of big data cannot be widely accepted.

Beyond 5G Technology, Challenges and Expectation

Okorie Clinton Chidera

Wireless cellular technology has grown significantly through the years. In the 1980s the first generation of wireless cellular technology (IG) was given birth to, It was mainly analog and used for voice calls only. 10 years later the second generation (2G) came up, this was digital technology and it brought with it instant messaging. In the early 2000. The third generation (3G) of wireless cellular technology came up with increased capacity and support for Multimedia. The fourth generation (4G) came almost 10 years later with internet technology with to support the mobile networks, this was an improvement on the wireless cellular technology and it was a solution to the shortcomings of 3G.

5G which represents 5^{th} Generation is an improvement on 4G, It offers support for users and applications through faster network speeds, lower latency, improved reliability and better network performance. Providing solutions the visible shortfalls of 4G is the is the main goal of 5G, 5G will ride on the successes of its predecessors to open the doors to new services, applications, new business models and transforming societies

In recent years, wireless cellular technology has become more popular due to major developments in mobile technology from 1 G to 5G. This reform is due to service-compatible transmission technology requirements and very strong customer growth in telecommunications.

The mobile cellular age began in 1980, and since then there have been significant changes in wireless cellular technology's and huge development.

1G (FIRST GENERATION): ANALOG CELLULAR NETWORKS

1G is the first generation of wireless cellular technology, introduced in the 1980s, it was based on analog technology. It was used for voice services only and was based on technology called Advanced Mobile Phone System (AMPS). In 1979, the first cellular system developed by Nippon Telephone and Telegraph (NTT) in Tokyo, Japan became operational. The key technological development that differentiated the mobile phones of the First generation from previous generation of phones was the use of cell sites and the ability to transfer calls from one site to the next as the customer traveled between cells during a call.

The main drawback of 1G was limited capacity, poor voice quality, unreliable hand off and little or no security.

Its basic characteristics are:

Speed-2.4 kbps

Use analog signal.

2G(SECOND GENERATION) : DIGITAL NETWORKS

2 G is the GSM-based second generation that arose at the end of the 1980s.First launched in Finland, it transmits data via digital signals. This technology focused primarily on digital signals and offers low-speed

(kbps) text, picture and multimedia messages all digitally encrypted. It uses 30 to 200 KHz bandwidth. SMS text messaging became possible during this era.

Its basic characteristics are:

Data speed was up to
64kbps Use digital signals

Enables services such as text , picture and Multimedia messaging
Provides better quality and capacity than 1G

It uses frequency of 1.8GHz (900MHz) and a bandwidth of 900MHz (25MHz)

2.5G (2G CELLULAR TECHNOLOGY WITH GPRS): DIGITAL NETWORKS

The GSM communication technology continuously improved, leading to development of advanced Technology between 2g and 3g called 2.5G. 2G networks was improved using GPRS (General Packet Radio Switching), this improved technology had the capacity to handle packed based services and was later referred to as “Second and a half generation” (2.5G). Data rates from 64 kbit/s to 114 kbit/s could be provided by GPRS. It could be used for applications such as access to Wireless Application Protocol (WAP), Multimedia Messaging Service (MMS) and Internet communications services such as email and WWW

Its basic characteristics include all the features of 2G and the following additions:

E-Mails

Web browsing
Camera phone

2.75G (2G CELLULAR TECHNOLOGY WITH EDGE) : DIGITAL NETWORKS

After implementing GPRS technology, 2G networks continually improved evolving to EDGE (Enhanced Data rates for GSM Evolution). This improvement came with faster data transfers and more flexibility for data transmission.

(3G) THIRD GENERATION: HIGH SPEED IP DATA NETWORKS

3G launched in 2000 was based on GSM technology. It was developed to provide improved speed in data services. The original technology was improved to allow data up to 14 Mbps and more using packet switching. It uses Wide Band Wireless Network with which clarity is increased. It also offers data, television/video access and services like Global Roaming. It has a frequency range of 2100MHz and a bandwidth of 15-20MHz used for High-speed internet/data services.

It was a challenge to build the infrastructure for 3G back then, It had high bandwidth requirement and the cost to build such infrastructure was quite expensive.

The main features of 3G are:

Speed of up to 2 Mbps

Increased bandwidth and data transfer rates to accommodate audio and video streaming.
Provides faster communication

High speed internet, video conferencing, support.
Large capacities and broadband capabilities

(4G) FOURTH GENERATION

4G was developed to meet the requirements set by forthcoming applications like wireless broadband access, Multimedia Messaging Service (MMS), mobile TV, video chat, minimal services like voice and data, and other services that utilize large bandwidth.

Speed of up to 100mbps can be achieved with 4G, 4G has a lot of similarities to 3G and extra services which include online Newspapers. LTE (Long Term Evolution) is a 4G wireless cellular technologys standard this is an evolution of current technologies and an improvement on it.

The main features of 4G are:

Speed of 10Mbps-1Gbps speed
HD Video streaming

Increase in security and data protection
4G Network Architecture

(5G) FIFTH GENERATION

5G is the next generation of mobile broadband that will eventually take over from 4G LTE. As its previous generations of cellular technology, 5G systems will comprise of small cells separated into parts sending information through radio waves. Every cell is associated with a network backbone that is either wired or wireless.

5G would transmit data over frequencies currently not used by its predecessors that is millimeter waves. It guarantees a more intelligent, faster and productive system.

The objective of 5G is to have far higher speed, at higher limit per area, and at far lower latency than 4G.Each device would have an IPv6 address. 5G works on the idea of World Wide Wireless Web (WWWW). WWWW will be equipped for supporting applications, users systems and interconnecting the entire world. 5G incorporates the most recent innovations such as Internet of things, Beamforming, nanotechnology, and distributed computing.

5G technology is made up of digital cellular networks, where network carriers divided by locations called cells provide service to users.

How 5G Works

Data signals initially sent as analog are digitally converted with the aid of converters and sent as bit streams. Cell communication is by radio waves for all devices in 5G wireless technology, using low energy transceiver and local antennae, data is sent over frequencies assigned by the transceiver, this frequencies are then recycled by other cells in different locations. This antennas are connected to the service provider thorugh optical fiber which serves as the backbone for the connection.

When an individual moves from one position to another he may go out of range of the particular cell tower he was connected to initially and like with existing devices, it moves onto the next cell tower, their cell phone is "handed off" automatically to a new cell.

5G is being set up to make use of millimeter waves. This are smaller in size as compared to the current frequency band and as such have difficulty passing through trees, buildings and obstacle in general. To overcome this challenge we make use of a Massive MIMO(Multiple Inputs Multiple Outputs).The network towers would have multiple antennas on each of them and this antennae would be communicating with different wireless devices sending and receiving information simultaneously.

Although this would likely cause a lot of interference as network signals crisscross each other. Beamforming is one of the technologies that would reduce or completely mitigate the interference. It does this by calculating the best route for network signals to reach a particular device and sending data directly to that device.

THE MAIN FEATURES OF 5G ARE:

Very low latency

1000x bandwith per unit area
Up to 10gbs data rate

Increase in battery life for low powered devices
99.99% availability

Can accommodate a 100% more devices

COMPARISON OF ALL GENERATIONS OF MOBILE TECHNOLOGIES

Table 1. Comparison of wireless cellular technology

	First Generation	Second Generation	Third Generation	Fourth Generation	Fifth Generation
Approximate launch date	1980s	1990s	2000s	2010s	2020s
Theoretical	2kbit/s	384kbit/s	56Mbit/s	1Gbit/s	10Gbit/s

download speed					
Latency	N/A	629 ms	212 ms	60-98 ms	< 1 ms
Network	Primary Analog, Phone Calls	Digital ,Phone Calls, SMS	Phone calls, SMS, Internet	Phone calls, SMS, Faster Internet	Greater speed, larger capacity,
Difference	Mobility	Digital experience	Internet	Faster Internet, Lower Latency	Wider network coverage , much lower latency, Better performance
Shortfalls	poor security, Poor network	Limited network, insufficient support for internet and email	low download and upload speed, intermittent network failure	Complex network, high battery usage	

Edge Computing

Felicia Ajayi

Human interaction and behavior has been significantly impacted by Cloud computing since its advent around 2005 (Gezer et al., 2018). Internet of Things (IoT) was first introduced to the

community in 1999 for supply chain management, and then the concept of “making a computer sense information without the aid of human intervention” was widely adapted to other fields such as healthcare, home, environment, and transports (Gubbi et al., 2013). Now with IoT, we will arrive in the post-cloud era, where there will be a large quality of data generated by things that are immersed in our daily life, and a lot of applications will also be deployed at the edge to consume these data.

First, edge computing arose through the virtualisation of network infrastructure over WAN networks, a step away from the datacenter. The original use cases were motivated by a willingness to utilize a platform that provided the flexibility and easy tools cloud computer users were used to. As modern computing capacities arise, we see an evolving computing paradigm that is no longer necessarily bound by the need to construct centralized data centers. Instead, cloud edge computing takes the lessons of virtualization and cloud computing for certain apps and creates the ability to have possibly thousands of massively distributed nodes that can be implemented to a variety of uses, such as industrial IoT or even wide-ranging surveillance networks to track real-time use of water resources over thousands or millions of places. Without depending on distributed cloud, many proprietary and open source edge computing capacities already exist — some suppliers refer to this as "device edge." This strategy includes components like IoT gateways or Network Function Virtualization (NFV) devices. But apps are progressively in need of cloud versatility on the edge, though the instruments and architectures required to construct distributed edge infrastructures are still in their infancy. Our opinion is that the industry will continue to require better cloud edge computing capacities. To construct an architecture, it is necessary to identify the problems on the present cloud or IoT systems, specify demands, list enabling techniques, and then provide a notion.

Later, the concept can be implemented in an architecture, validated, and evaluated. This paper presents an ongoing work on Edge Computing with its clear description. It also explains its requirements and enablers to solve the introduced issues. The paper also shows an ongoing work of edge computing, a novel server architecture which is capable of performing real-time tasks and applications of technology using case study. The architecture will also be vendor-independent and extensible and it will meet industrial requirements.

What Is Edge Computing?

Edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of IoT services. Here we define “edge” as any computing and network resources along the path between data sources and cloud data centers. For example, a smart phone is the edge between body things and cloud, a gateway in a smart home is the edge between home things and cloud, a micro data center and a cloudlet is the edge between a mobile device and cloud. The rationale of edge computing is that computing should happen at the proximity of data sources. From our point of view, edge computing is interchangeable with fog computing, but edge computing focus more toward the things side, while fog computing focus more on the infrastructure side (OpenFog Architecture Overview, 2016). We envision that edge computing could have as big an impact on our society as has the cloud computing. In the edge computing paradigm, the things not only are data consumers, but also play as data producers. At the edge, the things can not only request service and content from the cloud but also

perform the computing tasks from the cloud. Edge can perform computing offloading, data storage, caching and processing, as well as distribute request and delivery service from cloud to user. With those jobs in the network, the edge itself needs to be well designed to meet the requirement efficiently in service such as reliability, security, and privacy protection.

While most observers agree that Edge Computing is a paradigm shift in computing, there is no singular definition of Edge Computing that has gained consensus. According to ETSI, “Mobile Edge Computing provides an IT service environment and cloud computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN) and in close proximity to mobile subscribers.” IEEE defines Edge Computing as something that places applications, data, and processing at the logical extremes of a network rather than centralizing them. Linux Foundation says something similar - “The delivery of computing capabilities to the logical extremes of a network in order to improve the performance, operating cost, and reliability of applications and services.”

But what are the “logical extremes” of the network? In most instances, they are the enduser devices – smartphones, sensors, automobiles, health monitors, etc. From an Edge Computing perspective, the location (not necessarily the physical location) is defined by the task at hand and how do you get capabilities to the node that needs it in a most cost-effective and scalable manner. For example.

- If one is looking for location data for a few hundred devices at the same instance in a local district, the base station is ideally most suited to have that information that can be dispersed to the entity that needs it, so the base station is the edge in this instance.
- For a drone that is collecting images in real-time on an oil pipeline and is trying to determine if there are noticeable changes, the drone itself is the edge device which can do this determination.
- In some instances, the vehicular traffic data must be aggregated to predicting congestion in cities. In such scenarios, the aggregation layer is the edge.
- In healthcare use cases, depending on the state of the application and the task supply-chain, the edge could vary from being at the device on the patient (like smart watch or the heart monitor), at the RAN (in operator's network), at the local hospital chain (that is processing the data from multiple patients) or at data aggregation point (that is looking at the national data streaming in).
- In the case of facial recognition based security systems at schools, using facial vectors for authentication can be done using a local small cell or access point (in which case that will be the edge) while if you are trying to compare a face to a wanted database, typically, you will do it with the help of aggregation nodes or centralized cloud as such the edge moves back in the network. However, if you are doing a recognition to validate the user for a device, the device itself is performing all the computations and authentication and becomes the edge.

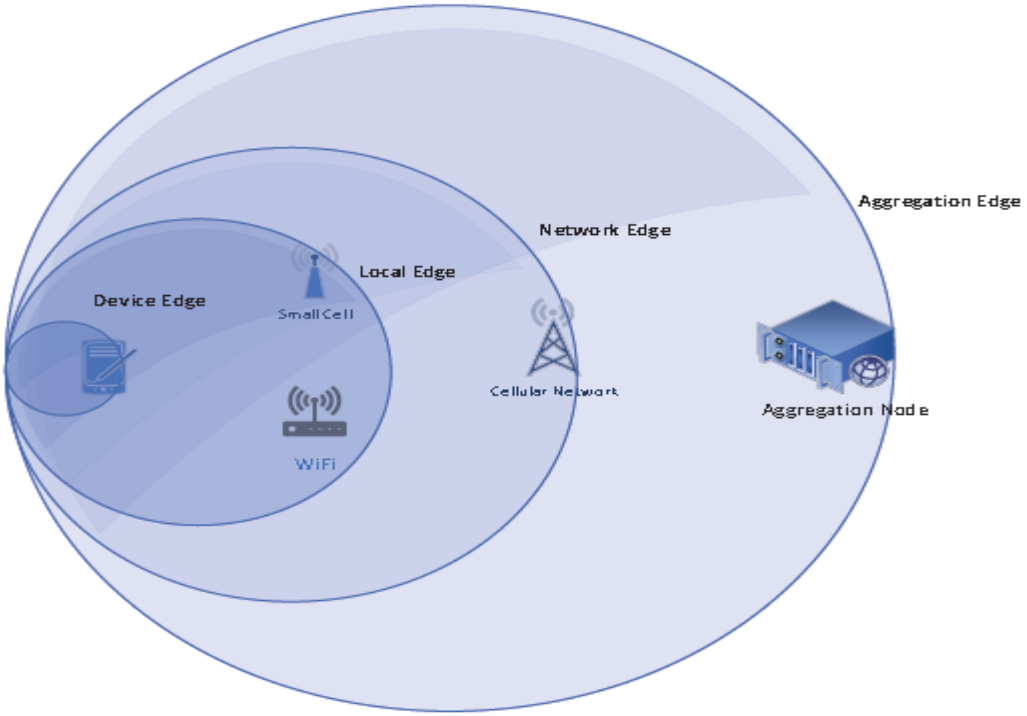

Figure 1. Edge Computing Network

The key in all these examples is that the intelligence is programmed for the highest efficiency. Resources are instantaneously distributed to the node closest to the point of need. This is done through the capabilities available at the device, network, and the cloud. It should be internalized that Edge is not optional but rather a core element of the framework through which every application and service will be designed. In the next section, we will take a look at the market forces that are enabling the Edge Computing cycle.

2.3 Architecture Design

An Edge Server must be capable of gathering, aggregating the data, computing and transferring it back to the end device. However, in the meantime, the servers must be able to communicate with other Edge Servers within the network, in case their resources are not enough to perform the task. Alternatively, they must be able to offload the data

to the Cloud. In other words, the Edge Servers must have a reliable and communicable network between each other and the Cloud. For seamless task handling and communication, the servers must follow some standards compatible with each other. This is not a simple task, since this technology contains several aspects to consider such as resource allocation, scheduling, scaling, storage, etc. The architecture must also be able to handle time-critical or real-time tasks. The software must also be designed or modified to work with the real-time capable system (Rostedt, 2013). Last but not least, the server must be extensible with plug-and-play modules to advance or add new functionalities via hardware or software modules. These extensions must be validated before usage, to keep the system functional and to prevent intrusion. Such architecture design is divided into Hardware Modules and Software Components which are explained in the next subsections.

A. Hardware Modules

As mentioned in the previous sections, to solve the problems of Cloud Computing, Edge Servers or ”Edge Nodes” need to have more computing power than the end-devices. However, the hardware in the Edge Tier is also limited compared to the Cloud. Therefore, to keep the balance between the performance and costs, first, the use cases for the Edge Servers must be defined, then, the resource must be considered to handle these defined use cases in-time. The data produced by the end-devices are not directly sent to the Cloud or back-end infrastructure, but initial computing is performed on these servers. Considering the number of connected devices and the data they produced, these servers are used to aggregate, analyse, and process the data before sending it into the upper layer, the infrastructure, or back to the device. The proposed Edge Server

architecture is to be designed modular and should provide functionalities for real-time and non-real-time control, as well as real-time communication. Each server in our proposal has a Core Node of which functionalities can be extended by plugging additional optional modules in.

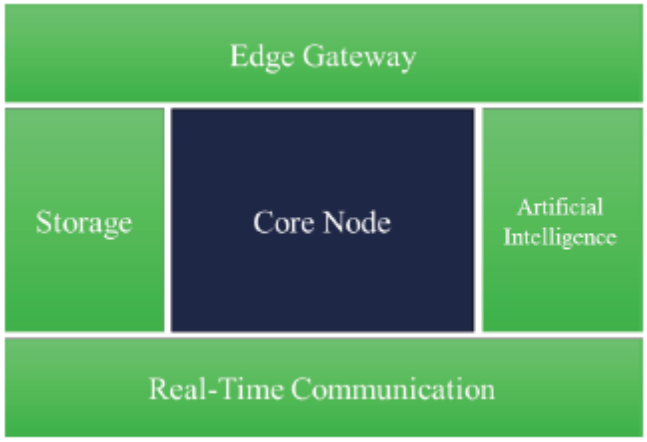

Figure 2. View of the proposed extensible Edge server architecture with its major functionalities, where green blocks extend the functionalities for the blue core node. (Gezer et al., 2018)

B. Software Components

As mentioned, the server has a Core Node which is capable of performing real-time tasks. Before implementing the software architecture of such system, it is important to define the roles of software, clarify, and assign separate roles to the components. Rather than choosing the technologies or languages, which the software components are going to be implemented in, all components defined here can be implemented in any language as long as they satisfy the requirements (Gezer et al., 2018). Time-sensitiveness requires implementation of several components which are compatible with each other. These components should enable a reliable, stable in-time response and take correct actions (Gezer et al., 2018).

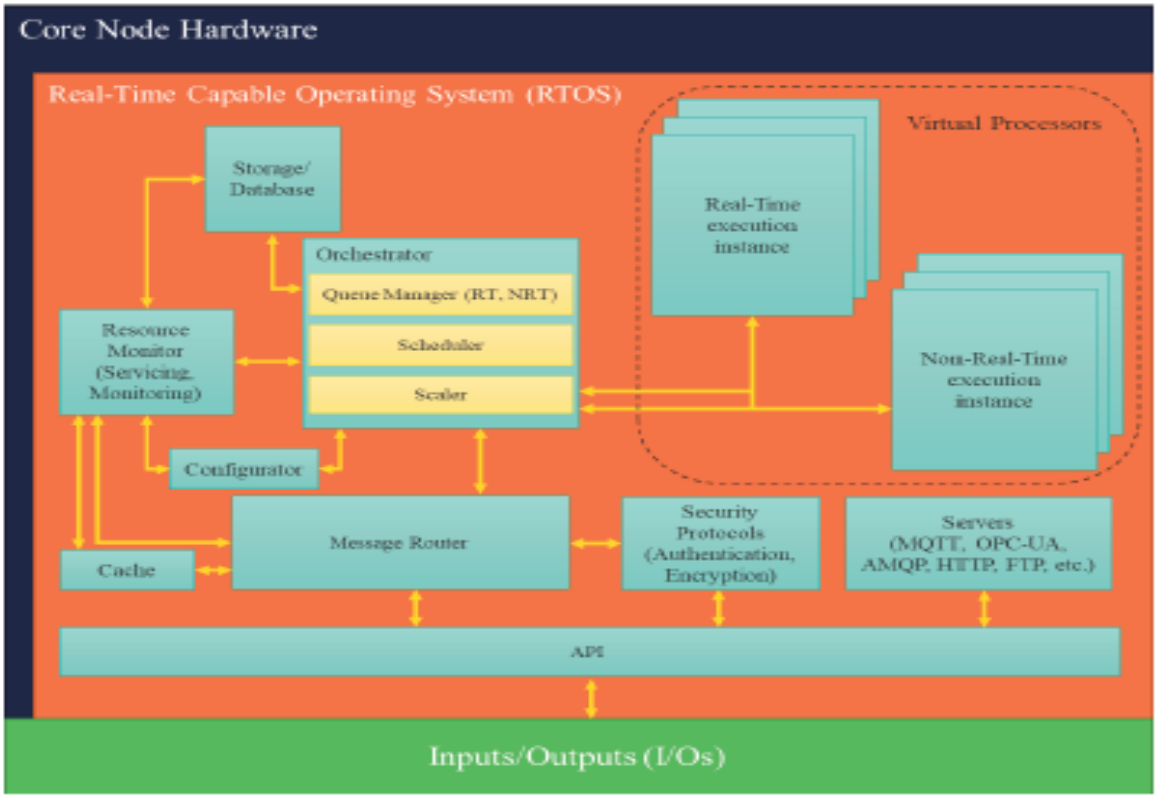

Figure 3. Software Architecture of Core Node (Gezer et al., 2018)

Figure 3 shows the required software components inside the Core Node to fulfil the requirements. Below, these components are explained:

Real-Time Capable Operating System (RTOS): To implement software components, the operating system (OS) in the hardware must also be real-time capable. There are many OSes which can handle real-time tasks. However, the choice of the OS should be made by considering its available support, availability of the source code or openness for modifications, and applicability of the OS into the chosen hardware platform. Having a real-time capable kernel does not mean that the system will work in real-time. Applications, APIs, and the system must be designed properly to benefit from real-time functionality (Huang, 2014). It should have a native support for the chosen Core Node hardware that it is running on. (Projects, 2007).

Inputs/Output (I/Os)s: I/Os are the interfaces which connect the hardware with the software. These are also used to connect other physical modules with the core node such as Edge Gateway for real-time communication.

API: APIs will be used for all communication with the I/Os, the end-devices, or the Cloud. An API is necessary to abstract the functionalities of other components. It allows internal modifications in case a new software component is added without requiring complete change in the system. It also guarantees that the requests cannot interfere with the internal components since direct access to the individual modules or components is not allowed. Another goal of the architecture is to keep the migration efforts at minimum. Therefore, it is important to choose an accepted and standard language for the API to make it compatible with as many device and software as possible. Another aspect to consider is to choose a lightweight, yet stable API as a low latency is desired. Last but not least, the API should make sure that the requests are always authorized. This is performed by evaluating the request with Security Protocols component.

Message Router: As soon as the task or data arrives, this component retrieves and routes it to the location where task should be handled by communicating with Resource Monitor component. In case there are no resources available in this server, the task will either be transferred to another Edge Server or to the Cloud. This component always makes sure that the incoming task is from a trusted device by interacting with the Security Protocols component.

Configurator: The server and their modules are automatically configured as soon as they are attached. Nevertheless, their manual configuration or tweaks are performed via this component. It provides a Web-based and shell-based administrator panel to modify server

properties, monitor the status, perform low-level resource allocations, and adjust orchestrator parameters, etc. Additionally, this component detects other nearby servers in the same network and configures the server to use them, when necessary. Similar to other components, this component is also accessed through the API.

Storage/Database: This component is used to store temporary data for the active or waiting tasks. However, the component will not keep the permanent data of the tasks. To keep the permanent data, storage module or the Cloud is recommended.

Servers: Standalone servers which are used out-of-thebox with only configuration changes are encapsulated in this component. The servers enable API communication as well as internal communication among the components. The servers are configured through the API via Configurator component.

Security Protocols: One of the most important requirement for the Edge Computing is keeping the data secure and private. Security itself is a vast aspect to consider. Therefore, a dedicated component to handle all security-related issues is necessary. This component monitors all incoming connections and takes the necessary actions in case the request is unexpected or unauthorized. Since the Edge Server will be accessible via the Cloud, the component is also responsible to prevent Internet-based attacks. Moreover, the component makes sure that the data privacy is preserved by encrypting, decrypting the data and issuing and exchanging keys, etc.

Resource Monitor (RM): The computing power in the Edge Server hardware is limited. RM actively monitors all available resources of Edge Servers in the network. It is also aware of all the other connected Edge Servers and their attached modules. RM directly interacts with the Message Router and decides whether the task received must be

processed in this server or offloaded to another location. If the task is to be executed in another server, this component informs the Message Router and points the target without further action. This decision is made by bi-directional communication with Orchestrator.

Cache: A temporary storage component to serve the data faster for the future requests. It is especially used when Resource Monitor decides that the task is not going to be executed in the current server. Virtual Processors: For performance and power reasons, it is typical to have multi-core hardware. In multi-core hardware, one thread is generally executed on a single core. If a software is not optimized for multi-core, it cannot benefit from multicore hardware. On the other hand, multi-threaded software execution is distributed among the cores. However, in either case, it is possible to set central processing unit (CPU) affinity of a process, that is a running instance of the software or program. Low-level programming makes configuration of the kernel possible to add virtual processors, limit or specify the available resources, and assign specific processes to these virtual processors.

Orchestrator: If RM allows execution of the task in this server, this component becomes active. Using event-based communication with the RM, the task is handled according to its urgency or the priority. If there is enough resource to execute the task, the task is immediately executed. If not, determined by the availability of the resource, task can be handled in different ways using the sub-components. This component has three different sub-components, namely: Scheduler, Scaler, and Queue Manager.

Scheduler: If a task is chosen to be executed in this server, it must be carefully scheduled to avoid deadline misses, especially for real-time tasks. Although multi-threaded

software is usually scheduled by the OS and assigned to the CPU cores, the affinities may need to be adjusted. Depending on urgency or the priority of the new task, this component is responsible to set CPU affinities for the running tasks taking their priorities into consideration. The scheduler should be designed to minimize the waiting time of paused tasks.

Scaler: Scheduler sorts the execution times of the tasks. In the proposed architecture, some of the cores are dedicated for real-time tasks. Tasks not optimized for multi-core systems are by default assigned to run on a single core. If Scheduler is not able to meet the deadlines of the critical tasks, this component can increase the available core count for the real-time tasks to have them run on multiple cores, even if the cores are not assigned to execute real-time tasks. Of course, this is only possible provided that the tasks are multi-threaded.

Queue Manager: If a task cannot be executed immediately, one other possibility is to queue it. The queue contains both real-time (RT) and non-real-time (NRT) tasks. This component communicates with the Scheduler, and stores the tasks marked to pause and forwards the paused tasks to scheduler, following a variable scheduling algorithm.