



ISSN:1991-8178

## Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



### NGCC: Certain Investigations on Next Generation 2020 Cloud Computing-Issues, Challenges and Open Problems

<sup>1</sup>Prof.S.Balamurugan, <sup>2</sup>A. Brindha, <sup>3</sup>S. Gayathri, <sup>4</sup>Dr.Gokul Kruba Shanker, <sup>5</sup>Duruvak kumar V.S. and <sup>6</sup>V.M. Prabhakaran

<sup>1</sup> Anna University, IT Department, KIT-Kalaignarkaranidhi Institute of Technology, Coimbatore, Tamilnadu, India

<sup>2,3,6</sup> Anna University, CSE Department, KIT-Kalaignarkaranidhi Institute of Technology, Coimbatore, Tamilnadu, India

<sup>4</sup>VGM Hospitals-Institute of Gastroenterology, Consultant Surgical Gastroenterologist, Advanced Laparoscopic and Bariatric Surgeon, Coimbatore, Tamilnadu, India

<sup>5</sup>CEO icliniq.com and Managing Director -Orane Healthcare Private Limited, India

#### ARTICLE INFO

##### Article history:

Received 3 October 2015

Accepted 31 October 2015

##### Keywords:

Cloud Computing, Next Generation, Knowledge Management Systems, Bigdata, Healthcare, Mobile Phone Sensors.

#### ABSTRACT

Introduction: In a short period of time cloud computing has spread worldwide and thus most of the IT corporate and industries are moving towards cloud. Cloud computing network are well known for providing internet – based services and on - demand services. Information flow control (IFC) is considered as a way of expressing, enforcing and demonstrating data protection policies and laws. Objective: The objective of this paper is to provide a detailed investigation on future trends of cloud computing. The paper provides an immense foresight on the next generation cloud computing, the developments expected till 2020. Results: An inference and prediction of future cloud system techniques/strategies/methodologies/algorithms is derived. Conclusion: The paper concludes by enumerating strong points to of the tremendous growth of cloud systems in future. This paper would promote a lot of research in lot of un-invaded areas of application of cloud computing.

© 2015 AENSI Publisher All rights reserved.

**To Cite This Article:** Prof.S.Balamurugan, A. Brindha, S. Gayathri, Dr.Gokul Kruba Shanker, Duruvak kumar V.S. and V.M. Prabhakaran., NGCC: Certain Investigations on Next Generation 2020 Cloud Computing-Issues, Challenges and Open Problems. *Aust. J. Basic & Appl. Sci.*, 9(33): 234-241, 2015

### INTRODUCTION

The Cloud Computing has emerged as a new computing paradigm which aims to provide dependable, personalized, dynamic computing environments focused towards enhanced value of service and IT infrastructure. Cloud computing has been obtainable in recent years with new innovations and business applications. Cloud computing will persist to increase and control users information communication because it offers many compensation, allowing users to have easy instantaneous and individualized access to tools and information, in portable manner when and wherever they need also locatable from any networked device. Cloud computing in healthcare has become tight bond relationship between the care provider and the patient. Cloud technology supports cooperation and team based care delivery and the ability to use applications based on their necessities and a general set of medical information. It can be done on a platform that allows healthcare organizations to deliver, use and integrate the medical data to the authority which hold all the sensitive data. This will require maintaining a level of security and privacy

equal to or greater than what conventional IT provides. A cloud provider may provide services from different geographic locations. In such a case, the data is processed from one cloud to another cloud in order to maintain load balance. As we know already cloud services are classified into three broad categories. They are, Infrastructure – as – a – service: cloud service provider's controls management of network, hardware and hypervisor. Software – as – a – service: cloud service provider's handles all the applications. Platform – as – a – service: cloud service provider's aids the smooth functioning of OS.

Cloud provider is an organization that provides cloud services to the client. A client or an end user is the one who requested for specific cloud services. Sometimes, a tenant acts as a broker between the cloud provider and end user. IFC is responsible for reducing compliance against data protection and settling legal disputes. IFC formulates the policies and standards based upon the data location. If the location of the data is traced and monitored, then the data misuse practices and scandals will be avoided. It will improve the transparency and accuracy of data.

The rest of the paper is organized as follows: Section 2 describes the concept of Expressing and

**Corresponding Author:** Prof.S.Balamurugan, Anna University, IT Department, KIT-Kalaignarkaranidhi Institute of Technology, Coimbatore-641402, India.  
Tel: +91 9952521935; E-mail: sbnbala@gmail.com.

Enforcing Location Requirements in Cloud using Information Flow Control. Section 3 gives a broad overview of Using Mobile Phone Sensors to Detect Rapid Respiratory Rate in the Diagnosis of Pneumonia. Section 4 gives a detailed survey of various Effects of Cloud Computing Systems in Terms of Service Quality of Knowledge Management Systems. Section 5 portrays Hardware and Software Verification Process Through Cloud Computing. A study of cloud-based smart home framework is depicted in Section 6. Section 7 speaks about Insurability of Cyber Risk. Various Services, Security Challenges and Security Policies in Cloud Computing are dealt in Section 8. Conceptualization Proposal in Cloud Computing prevailing in literature is discussed in Section 9. Section 10 gives a broad overview of Architecture of 5G Mobile Communication System in Higher Frequency Band depicted in literature. Section 11 concludes the paper giving the future research direction.

## **2. Expressing and Enforcing Location Requirements in Cloud using Information Flow Control:**

Thomas F. J.-M. Pasquier and Julia E. Powles (2015) say that Policy enforcement points (PEP) are managed by standard data access control mechanisms where the user should be authenticated to access the cloud resources. IFC will always trace the path of data where it has reached and where it is currently used throughout its life span. Usually encrypting all the data in cloud will be a huge risk factor. In such cases IFC can be used to execute computations by making use of unencrypted data. An IFC system incorporates security context with two main properties such as secrecy and integrity of data. The secrecy concerned data adopts no – read up, no – write down rule. Secrecy provides some restrictions for the destination where the data is being sent. The integrity concerned data adopts no – read down, no – write up rule. Integrity provides few restrictions over the source of data. A process having both secrecy and integrity properties in a specific location will allow the data to be transferred only within that specific location.

Processes at different locations will transfer its data using declassification and endorsement methods. Declassification eliminates the secrecy conditions so that the flow of data will be more convenient. Endorsement verifies whether the data received is trustworthy or not. IFC architecture that implemented in cloud has the following components.

### **IFC OS enforcement mechanisms:**

Contains IFC conditions to execute unaltered cloud applications.

### **Context Manager:**

Is interfaced with the client and responsible for managing security context where the cloud applications are executed.

### **Messaging Middleware:**

IFC is interfaced with data centres to establish communication among virtual devices.

### **Audit system:**

IFC logs are used to distribute only the required information to the client.

IFC - enabled platform makes the client who requested for cloud services to set their own policies in order to manage the security context. IFC policies generally detect two things:

- 1). the location where the data is asked to flow.
- 2). the location from where the data comes.

The location of data becomes transparent and accurate when the secrecy and integrity tags are assigned properly. IFC through cloud network is a better way for expressing and enforcing policies and standards for providing cloud services. But still international legal disputes among cloud providers are becoming a difficult work to resolve.

## **3.using mobile phone sensors to detect rapid respiratory rate in the diagnosis of pneumonia:**

According to Xingjuan Li (2016(a)) pneumonia is a common spreading disease and it is caused by bacteria, fungi and viruses. It kills about two million children per year. Difficulty in breathing, lower chest pain, cough, fever, headaches, loss of appetite are the symptoms of pneumonia. The main fact to determine pneumonia is to identify the respiratory rate. Currently, mobile phones are commonly used for communication purpose only. But the sensors like accelerometers and gyroscopes embedded inside mobile phones are capable of detecting the physical signs produced as a result of breathing activity.

The sensors inside the mobile phones will record all the physical signs. The data recorded by these sensors can be read by smart phones like android and the data is then processed and the results are observed under matlab to determine the rapid respiratory rate. There are several other methods that can be used to determine respiratory rate. They are,

1. By keenly observing the pressure wave generated by oxygen.
2. Analyzing haemoglobin in blood with the help of pulse oximeters.
3. By observing modifications happening in volume of gas using spirometer.

These methods always needs some expertise and advanced equipment to find the rapid respiratory rate. One method of detecting rapid respiratory rate is to use smart phones without introducing medical instruments into the body. This is called as “Non-invasive” way of determining respiratory rate.

The system incorporates three main parts.

1. Android app – capable of reading the data stored in sensors of smart phones.
2. Data processing part- eliminates noise signal that interrupts breathing signal.
3. User feedback part – submits a report to the user.

Both the sensors accelerometer and gyroscope uses separate apps like accelerometer app and gyroscope app to monitor the physical signs and data recorded inside these sensors because android phones makes use of various timestamps. These sensors also requires three user interfaces – data reading interface, sensor capability interface and canvas interface to elaborate sensor values. The accelerometer and gyroscope app involves 20,000 microsecond data delays. In order to capture the motion produced by breathing, we need to place the mobile phone in front of the abdomen or chest.

Data Acquisition is a process of transforming analog signals into its equivalent discrete signals. During this process, few data may get lost. In order to regain the lost data, we need to record the time during which the sensor data is passed to the system additionally. The data processing technique is stored in the cloud. So that the patient suffering from pneumonia after identifying their rapid respiratory rate will load their data in cloud for later data processing. The results obtained from final step will undergo few tests to ensure the optimality of the result. The results seem to contain an error rate of only + or\_ 2 breaths per minute. This accuracy is not obtained in any other technique. The benefit is that the smart phones records the rapid respiratory rate in a minute. But still smart phones are exposed to some limitations even though it is convenient to use.

#### **4.Effect of Cloud Computing Systems in Terms of Service Quality of Knowledge Management Systems:**

Hamed Rezaei, Behdad Karimi and Seyed Jamalodin Hosseini (2016 (b)) Cloud Computing plays an efficient role in information systems and data processing. Cloud computing brings an effective means of communication. It is a secure and accurate way of sharing computer resources of network with minimum expenditure. Cloud computing is one of the best platform to build a knowledge management systems.

In an organization, the knowledge management system will prevent the users from data loss by forming an intelligent backup module. It is helpful in projecting an organizational knowledge graph. The main advantage of using knowledge management systems is that it increases the system quality and accelerates the knowledge manufacturing cycle faster. The “Quality of Service” is an important factor in any knowledge management systems.

The success of an organization entirely depends upon the success scenario of information system. If this is the case, then we need the following facts to be considered in any information systems.

- i. System quality
- ii. Information quality
- iii. System usage
- iv. Service quality
- v. User satisfaction
- vi. Net benefits

Above all service quality acts as a main factor from which all other qualities are derived. Any information system must possess a high quality of service to satisfy user’s request. To run an information system successfully the suitable platform is Cloud computing. Cloud computing is an external storage application where the organization need to pay and store their data in cloud (third party).

Cloud servicing model are of three types: SaaS, PaaS and IaaS.

- a. Software – as – a – Service (SaaS): indicates the system that accepts user’s request, process it and supplies the service to the user through network with the help of application and system software.
- b. Platform – as – a – Service (PaaS): serves the user with requested resources to implement their applications on a server without the use of software.
- c. Infrastructure – as – a – Service (IaaS): to run software successfully we need a good infrastructure to be designed that will help the user by providing services on – demand.

A cloud study of an organization tells that the “Quality of Service” is increased when the knowledge management systems are deployed in cloud. This is an amazing factor that will take cloud to a far extent. Surely, the success scenario of “Quality of Service” will indicate the success of an organization

#### **5.Hardware and Software Verification Process Through Cloud Computing:**

Ousama Esbel and Ng Ah Ngan Mike Christian(2016(c)), say that most commonly microcontrollers are used for integrating hardware and software devices to build automated systems. Automated systems reduce man power and it is useful in finding accurate and error free results. It is versatile in nature. Hardware and software devices can be integrated together to use it as a common communication interface. A well known example of an automated system is smart home that makes the user to be convenient, secure, comfort and energy efficient.

Some communication interfaces that are widely used are Bluetooth, WiFi and GSM network. The difference between Bluetooth and WiFi is that WiFi technologies are more expensive than Bluetooth based systems. A GSM based technology can be used to overcome distance restrictions. But the GSM networks are not user friendly; and also there is no proper protection mechanism to secure data.

In a HAS system (Home Automation System) the web services are provided with help of upcoming mechanisms called “Internet of Things” (IoTs). We

can access the HAS system by using the application layers such as SOAP and RESTful. A remote user can efficiently communicate with its home appliances with the help of RESTful web services.

Locally Controlled Systems (LCS) are controlled by range of mobility and a local user can handle only the hardware devices that are placed in a specific range of operation. Remotely Controlled Systems (RCS) incorporates a remote user to handle the hardware devices till the internet connection is provided. RCS systems are very expensive when compared to LCS systems. The huge drawbacks seen in both these systems are that it does not provide, scalability and flexibility.

The issues in these systems can be fixed by implementing hardware and software devices through cloud computing network. A cloud computing network includes a shared data centre through a multitendency architecture. By using cloud we can avoid the requirement of complex hardware, software, their licenses, experts, network resources, etc. A HAS system incorporates android device, cloud networking, wireless communication and power – line communication to handle home appliances. This system employs three main parts:

1. Cloud server – handles the overall browser – based applications and it is not required to install software and hardware licenses on client system.
2. Client – handles the hardware devices employed in home.
3. Hardware – it is a microcontroller that uses analog to digital converters.

Generally, Firewalls are used to avoid unnecessary communication between the devices. But when these firewalls are installed they eventually block most of the incoming communication from one device to another in a network.

Another main drawback is that whenever a new connection is established the public IP address will be changed drastically. So, requesting a user to provide a constant IP address will make no sense. Several methods are available that can be implemented to overcome these issues.

1. Relay server – a middleman called “Relay server” without firewall can be used to provide proper and secure communication between the devices. Relay server makes use of an algorithm called “port mapping” to establish bidirectional communication between the server and the device. The server and the device communicate through socket programming.
2. Hosted services – hosted services is similar to Service – Oriented Architecture (SOA) (supplies only needed functions and services to the organization). Additionally, it includes Event – Driven Architecture. It is helpful in aiding mobile platforms. Some popular examples of hosted services are Facebook Parse, Pusher, Google cloud messaging. The benefit of this method is that it needs only fewer resources.

3. Software – to – software – integrates two mobile servicing devices like android with arduino with the help of a development kit called ADK. The huge bottleneck of this method is that it is suitable only for devices having compatibility with android ADK.

The common techniques used in all these methods are

- Addressing
- Delivery
- Description
- Control
- Event notification

Thus by implementing the hardware and software devices through cloud network will provide scalability, flexibility; handling the device becomes easier; avoids redundancy; improves security of information; less expensive. Although it has many benefits, developing such an architecture where all these needs to be satisfied is not possible.

### **6. A Framework for Cloud – Based Smart Home:**

Virtualization is the main feature of cloud computing that builds a virtual machine to deploy the user applications on physical machine. Similarly, other applications like mobile interactive app, parallel batch processing, business analytics app, compute intensive desktop app and economic analysts can also implemented in cloud computing. We can access cloud services anywhere, anytime due to two extreme features of cloud computing,

- Scalability
- Availability

Thanh Dat Dang(2017) proposed Smart home as an environment independent and it enables humanized services like smart home entertainment, remote communication and control of smart home. It makes use of a common interface to manage devices and systems automatically. Local computers are not capable of using smart home software; hence there will be no use in installing software for smart home in local systems.

Cloud computing and smart home both are emerging technologies. Collaboration of both the technologies will bring more advantage low expenditure and more advanced techniques. But it is a difficult task for the software developers to form a framework for cloud and smart home. Making sure of the data security and privacy, the cloud – based smart homes are build on cloud infrastructure that provides various services to the users on – demand.

In order to serve the user with the required service, smart home will produce necessary data and it will be stored in cloud to avoid security barriers. Cloud employs user role based access control policies, standards and strong encryption mechanisms to secure data stored in the cloud.

With the help of cloud based smart homes, the user can request for home anywhere, anytime. The infrastructure of cloud based smart homes should be capable of satisfying the user’s request. The

infrastructure is designed in such a way that it includes software layer, infrastructure layer and platform layer.

1. Software layer – it includes service interface, service control and service directory to interact with the user for delivering the services. Service control analyzes processes and sends responses to serve the user's request. The communication between mobile client and residential multimedia server is established using client container, media management, home gateway and cloud storage. A mobile phone or a tablet can be used to measure and visualize sensor data.

2. Platform layer – designed on the basis of Platform – as – a – service that enables resources and security management. Security components are employed to secure data from hackers. Similarly, virtualization management components are employed to monitor virtual machines along with load balance and fault detection.

3. Infrastructure layer – enables physical resources to deploy cloud services. Here, we use visualization components to monitor computing power, storage space, network resources and smart home. This layer incorporates DFS (Distributed File Systems) to make redundant copies of data block and assigns them to different nodes for easy access of data. This layer also supplies resources for virtual home (VHome) to deploy home services that are requested by the user.

Though cloud based smart homes provides us vast applications to use, there are many barriers that come into existence on the aspect of security and mobility. The framework for cloud based smart home that we design should have the ability to overcome all the barriers. Such a framework should come across various validation and evaluation tests to prove that it is worthy to use.

#### *7. Insurability of Cyber Risk:*

Christian Biener, Martin Eling and Jan Hendrik Wirfs (2018(a)) Present insurance policies and standards are not sufficient to overcome the problem of data breach or system failure that leads to high financial and reputational loss. Cyber attacks are considered to be the biggest threat that causes high economic and social significant losses to our global economy. Insurance is one of the major factors that are suitable to avoid cyber risks.

Generally, cyber risk means any risk of financial loss, disruption or damage affecting the reputation of an organization and failure of its information and technology systems. Based upon the aspects of insurance, the cyber risk is viewed as an operational risk. Operational risk defines the strategies that affect the confidentiality, integrity and availability of information. Cyber risk are classified into four different classes,

- Actions of people
- Systems and technology failures
- Failed internal processes

- External events

As a whole, insurance market includes commercial property and liability insurances. But none of the insurance policies cover the loss of cyber risk. Hence a new specialized market that includes all insurance policies related to cyber risk has come into view. But still these insurance policies remain unused due to inadequate knowledge of it.

To distinguish insurable and uninsurable risks, we need to make a complete study about the insurance market. Insurable risk policies indicate the financial compensation on the event of damage or loss information. When we design insurable cyber risk policies and their features, we need to consider the following factors.

1. Development of frequency and severity of losses is a policy that incorporates several self – protective steps to be taken at the time of loss due to cyber attacks.

2. Risk policy – the dependent relationships among various cyber risks are high. Thus the outcome of cyber insurance market will probably develop the capacity to create awareness about cyber insurance policies worldwide.

3. Scarcity of data – lack of knowledge about the cyber insurance policies to solve major cyber attacks.

4. Risk of change – using same insurance policy will not be suitable in all cases. Cyber exposures changes drastically.

5. Information asymmetries – inspite of using proper insurance policies, the market value is brought down due to adverse selection. Data loss is one of the major impediments in adverse selection.

6. Product value – present cyber insurance policies does not include the risk of accessing unauthorized websites and the policy holders will not be compensated with the financial loss of the product.

As the cyber space technology becomes larger day – by – day, the threats faced due to cyber risks also increases. Thus the existing cyber insurance policies and standards is insufficient to protect information systems from cyber attack. Even though the market development and insurance capacity increases due to lot of protective measures taken, still finding a way to protect the information system completely from cyber attacks is a big question mark.

#### *8. Services, Security Challenges and Security Policies in Cloud Computing:*

In the view of Dattatray B. Pawar, A.S. Devare(2018(b)), cloud computing has become a main part of communication technology and information security for most of the IT sectors. A fact says that comparatively, cloud has increased about 10% than last year in providing services to organizations. In the upcoming decade, each and every organization will be moving towards cloud to exploit their operations in a secure way. Public cloud is one of the main causes for the drastic growth in

cloud computing because it has increased its workload by 33%.

There are three cloud servicing models that indicate the organizations scope, the type service to provide and control among its computational resources.

1. Software – as – a – service (SaaS): delivers services and computational resources based upon the requirement of the user. This will decrease total expenditure including maintenance, operations and development cost.
2. Platform – as – a – service (PaaS): it gives a platform to compute and develop applications that can be implemented on the same platform. The main advantage of using PaaS is that managing platform is easy.
3. Infrastructure – as – a – service (IaaS): provides a service interface where virtualized objects are created to serve many computing infrastructures with the services needed.

In addition to above services, Database – as – a – service (DaaS) is a new emerging service in the IT sector. This service is either provided by public or private cloud. Generally, in any case, we need a Database Administrator (DBA) to maintain the database. But DaaS does not require a DBA. Some merits using DaaS are,

- Low cost
- Speeds up implementation
- Efficiency
- Availability
- Loss complexity
- Provides high security

There are four types of cloud deployment models.

1. Private cloud – a private organization manages the infrastructure provided by the cloud based upon its demand.
2. Community cloud – multiple organizations form a community to use the same infrastructure.
3. Public cloud – the infrastructure can be used only by a public or an organization that supplies cloud services.
4. Hybrid cloud – it is a combination of any two clouds.

Though cloud plays a major role in communication and technology, there are many security issues that come into existence. One of the main issues is trust. In case of public cloud, the trust issues are less because the owner of the infrastructure takes control over the security policies and standards of services. Whereas in case of private cloud, we do not need any security policies because the infrastructure is maintained by the private organization.

When we use on – demand service and shared technologies, the threats will be more. Another major drawback in cloud computing is data breach. Data breach refers to an incident in which the sensitive or confidential data is stolen by some unauthorized

person. About 110 million data has been breached out in last few years. Even when there is no backup of the data or if an external hard fails or crashes, the data will be lost. An intruder who is so good in hacking will surely modify user's data, steal account details of a customer, manipulate transactions. This is called as Account Traffic Hijacking.

More concentration should be needed when we design an API, since it should possess good authentication, encryption and access control techniques. The cloud customer must keep the encryption key with himself/herself rather than storing it in the cloud because the attacker may track the key quickly. A hacker can generate pirated software in order to gain data of a cloud customer. This is called as "Cloud Abuse".

Organizations moving towards cloud should have thorough knowledge of security policies and scope. The stable and standard security policies should be formulated; good data protection methods, strong encryption and authentication should be employed to avoid the data loss in cloud. The cloud users should be aware of all security challenges beforehand.

### **9. Conceptualization Proposal in Cloud Computing:**

Brent Fultz, Simon Billinge, Houman Owjadi, John Rehr and Mark Stalzer (2019) conceptualization proposal includes some methods of computational material science to calculate the state of scientific computing in X – ray and neutron scattering science (SIXNS). An intellectual benefit of this effort is to create an environment that will enable us to design new workflows for scattering science. Workflows will enable a scientist to gain more fundamental knowledge of structure and dynamics of materials that are not understood by experiments.

Conceptualization Phase will incorporate new tools at the stage of discovery where various scattering science community based techniques are defined. The X – ray and neutron scattering research has found that spallation neutron source has increased its magnitude to a high level. As well as Linac coherent Light source has orders of magnitude along with brightness. We can efficiently convert the computational tools into workflows for scattering science by merging computing and scattering science together.

The methods of computational materials science are required to calculate electronic structure, molecular dynamics, atomic structure and dynamics. Quantum mechanics and statistical mechanics are more useful in providing information for scattering science research. The main role of Conceptualization Phase is to verify all the goals of each community of scattering science for well understanding.

The Elastic Scattering research has determined that different diffractions will have same structure with different atoms arranged in different order.

When these different diffractions are joined together, they will produce optimal and reliable results.

The third generation X – ray sources have come into existence by using X – ray spectroscopic techniques like Non – resonant and Resonant inelastic scattering. Non – resonant inelastic scattering calculates the dynamic structure factor whereas data of high resolutions are produced by Resonant inelastic scattering.

We should select a suitable workflow for creating new scattering science. This is in Conceptual phase itself. Some of these workflows are used at the time of beta testing. Visualization of scattering community illustrates that data and requested services are distributed by cloud. The cloud establishes large opportunities of communicating between communities.

A huge bottleneck in this conceptualization effort is that it is difficult to identify systematic errors and clear them. To overcome this, prototyping and empirical testing's employed. Uncertainty Quantification is a method to study about scattering of data. But this method results in space complexity by producing infinite dimensions.

### **10. Architecture of 5G Mobile Communication System in Higher Frequency Band:**

Yi Wang, Jain Li, Lei Huang, Yao Jing, Andreas Georgakopoulos and Panagiotis Demestichas (2020), next generation 4G mobile systems are expanding into higher data rate of above 6GHz. Spectrums with high frequency bands is needed to be implemented in order to aid 10Gbps transmission successfully. IMT spectrum is a new emerging one that requires spectrum within the range of about 1340 – 1960MHz in 2020. At present, IMT makes use of only 885 – 1181MHz spectrum, we need to find more spectrum bands for 5G. For this reason, the Millimetre – wave (mm-wave) bands has been considered for research.

Millimetre – wave bands (3 – 300GHz) support point – to – point communications of 115Gbps data rate. But still Non – Line – Sight (NLOS) channel is an issue for mm – wave communication. There are basically two links,

1. Uplink which utilizes only licensed spectrum.
2. Downlink exploits user data in unlicensed spectrum.

Higher frequency band supports both wireless radio access and backhaul transmission by providing more advanced scheduling and routing techniques. There are large numbers of high frequency spectrum bands that can be used for ultra high data transmission.

There are three main basic things to be considered before selecting a spectrum.

1. The spectrum should be capable of allocating the spectrum administration and regulations properly.
2. The spectrum should be of contiguous spectrum so as to provide more flexibility in spectrum allocation.

3. The candidate spectrum that we select should have the ability to handle multiple channels and also should exploit any mobile communication services.

E- Band can be used as candidate spectrum for 5G in mm – wave because some higher frequency bands may result in larger propagation loss. Currently, 3GPP has announced to provide LTE in unlicensed spectrum but works on the basis of licensed – assisted manner.

The architecture of 5G mobile communication comprises of Macro base stations (MBs) and millimetre – wave base station (mBs) in first layer. MB carries most important control – plane data whereas mB carries user – plane data as well as backhaul data. In second layer, a single platform is used by both radio access and backhaul transmissions to schedule the usage of resources efficiently. The third layer consists of both lower frequency and millimetre – wave frequency in order to access MB's or mB's.

Load – centric backhauling is a technique used in hybrid network that identifies defects like traffic loads that causes changes in the network. Comparatively, fixed backhauling lacks capacity to distribute traffic loads than adaptive backhauling.

Hybrid network also aid multi – frequency transmission to supply ultra high data rate using multiple frequency carriers. Multi – frequency transmission employs two characteristics. First one is called as “C/U splitting technique” where control – plane data and user – plane data are separated from each other depending upon their requirements. Second will be unlicensed spectrum access. The performance of unlicensed spectrum will start decreasing when unexpected interference occurs. Hence it is advisable to use only user – plane data in unlicensed spectrums.

Intelligent and knowledge based management of mobile communication systems will give us more efficiency and optimality in selecting appropriate bands, providing necessary services and decisions making. This is achieved by using following components.

1. Context recognition and acquisition.
2. Developing knowledge on how to handle contexts.
3. Reasoning regarding how to handle contexts.
4. Conducting optimal context handling technique,

The hybrid networks architecture is characterised with load – centric backhauling, multiple – frequency transmissions and intelligent control techniques that support 5G mobile communication. Combination of radio access and backhaul transmissions succeeds in obtaining optimal knowledge – based solutions.

### **11. Conclusion And Future Work:**

This paper provided a detailed investigation on future trends of cloud computing. The paper depicted an immense foresight on the next generation cloud

computing, the developments expected till 2020. An inference and prediction of future cloud system techniques/strategies/methodologies/algorithms was successfully derived. The paper elucidates strong points to of the tremendous growth of cloud systems in future. This paper would promote a lot of research in lot of un-invaded areas of application of cloud computing.

### ACKNOWLEDGEMENT

S.Balamurugan, V.M.Prabhakaran A.Brindha and S.Gayathri wishes to thank the Management, Director and Principal of their institute, KIT-Kalaighnarkarunanidhi Institute of Technology, for providing all the necessary facilities and never ending support for the work. Their special thanks go to, Dr.R.Nedunchezian, Director-Research and Vice Principal, for sowing the seeds of thinking big in research within them, his expert guidance, continuous motivation and quality time spent by him.

### REFERENCES

- Thomas, F.J., M. Pasquier, Julia, E. Powles, 2015. "Expressing and Enforcing Location Requirements in the Cloud using Information Flow Control".
- Xingjuan Li, 2016a. "Using Mobile Phone Sensors to Detect Rapid Respiratory Rate in the Diagnosis of Pneumonia", International Journal of Engineering and Technology, 8(4).
- Hamed Rezaei, Behdad Karimi and Seyed Jamalodin Hosseini, 2016b. "Effect of Cloud Computing Systems in Terms of Service Quality of Knowledge Management Systems", Lecture Notes on Software Engineering, 4-1 .
- Ousama Esbel and Ng Ah Ngan Mike Christian, 2016c. "Hardware and Software Verification Process through Cloud Computing", Lecture Notes on Software Engineering, 4-2.
- Thanh Dat Dang, 2017. "A Framework for Cloud - Based Smart Home", Submitted on 28 th August.
- Christian Biener, Martin Eling and Jan Hendrik Wirfs, 2014. "Insurability of Cyber Risk", Newsletter Insurance and Finance, the Geneva Association, 14.
- Dattatray, B., Pawar and A.S. Devare, 2014. "Services, Security Challenges and Security Policies in Cloud Computing", International Journal of Research in Engineering and Technology, 03.
- Rent Fultz, Simon Billinge, Houman Owhadi, John Rehr and Mark Stalzer, 2011. "Conceptualization Proposal".
- Yi Wang, Jain Li, Lei Huang, Yao Jing, Andreas Georgakopoulos and Panagiotis Demestichas, 2020. "Architecture of 5G Mobile Communication System in Higher Frequency Band".
- Prabhakaran, V.M., S. Balamurugan, S. Charanyaa, 2015. Data Flow Modeling for Effective Protection of Electronic Health Records (EHRs) in Cloud, in International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798, 3-1.
- Prabhakaran, V.M., S. Balamurugan, S.Charanyaa, 2015. A Novel Activity Flow Model for Effective Protection of Electronic Health Records (EHRs) in Cloud, in International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798, 3-1.
- Prabhakaran, V.M., S. Balamurugan, S. Charanyaa, 2014. Certain Investigations on Strategies for Protecting Medical Data in Cloud, in International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798, ISSN 2393-8021, 2-10.
- Prabhakaran, V.M., S. Balamurugan, S. Charanyaa, 2014. Privacy Preserving Personal Health Care Data in Cloud, in International Advanced Research Journal in Science, Engineering and Technology, ISSN 2393-8021, 1-2.
- Prabhakaran, V.M., S. Balamurugan, S. Charanyaa, 2014. A Strategy for Secured Uploading of Encrypted Microdata in Cloud Environment, in International Advanced Research Journal in Science, Engineering and Technology, ISSN 2393-8021, 1-3.
- Balamurugan Shanmugam, 2013. Visalakshi Palaniswami, Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): 316-323
- Balamurugan, S., P. Visalakshi, V.M. Prabhakaran, S. Charanyaa, S. Sankaranarayanan, 2014. Strategies for Solving the NP-Hard Workflow Scheduling Problems in Cloud Computing Environments: Australian Journal of Basic and Applied Sciences, 8-6.
- Balamurugan Shanmugam, Visalakshi Palaniswami, R. Santhya, R.S. Venkatesh, 2014. Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art Survey: Australian Journal of Basic and Applied Sciences, 8-5.