CMI Computing A Cloud, MANET and Internet of Things Integration for Future Internet

Tanweer Alam [1]

[1]Islamic University of Madinah

October 30, 2023

Abstract

The wireless communication is making it easier for smart devices to communicate with one another in terms of the network of the Internet of Things. Smart devices are automatically linked and built up a network on their own. But there are more obstacles to safe access within the network itself. Mobile devices such as smart home automation access point, smart washing machines, mobile boards, temperature sensors, color-changing smart lighting, smartphones, wearable devices, and smart appliances, etc. are widespread in our daily lives and is becoming valuable tools with wireless communication abilities that are using specific wireless standards that are commonly used with IEEE 802.11 access points. On the realism of the Internet, security has been perceived as a prominent inhibitor of embracing the cloud paradigm. It is resource storage and management that may lay in any since the cloud environment is a distributed architecture, which place of the world, many concerns have been raised over its vulnerabilities, security threats and challenges. The involvement of various parties has widened these concerns based on each party's perspective and objective. The Cloud point of view we mainly discuss the causes of obstacles and challenges related to security, reliability, privacy and service availability. The wireless communication Security has been raised as one of the most critical issues of cloud computing where resolving such an issue would result in constant growth in the cloud's use and popularity. Our purpose of this study is to create a framework of mobile ad hoc network mobility model using cloud computing for providing secure communication among smart devices network for the internet of things in 5G heterogeneous networks. Our main contribution links a new methodology for providing secure communication on the internet of smart devices in 5G. Our methodology uses the correct and efficient simulation of the desired study and can be implemented in a framework of the Internet of Things in 5G.

JAMBURA JOURNAL OF INFORMATICS
Vol. 2, No. 1, April 2020
http://ejurnal.ung.ac.id/index.php/jji

CMI Computing: A Cloud, MANET and Internet of Things Integration for Future Internet

Tanweer Alam

Faculty of Computer and Information Systems
Islamic University of Madinah, Saudi Arabia
email: tanweer03@iu.edu.sa

Please cite this article

Tanweer Alam. " CMI Computing: A Cloud, MANET and Internet of Things Integration for Future Internet.", *JAMBURA JOURNAL OF INFORMATICS*. Vol 2, No. 1, 2020. DOI: 10.37905/jji.v2i1.4539

Abstract

The wireless communication is making it easier for smart devices to communicate with one another in terms of the network of the Internet of Things. Smart devices are automatically linked and built up a network on their own. But there are more obstacles to safe access within the network itself. Mobile devices such as smart home automation access point, smart washing machines, mobile boards, temperature sensors, color-changing smart lighting, smartphones, wearable devices, and smart appliances, etc. are widespread in our daily lives and is becoming valuable tools with wireless communication abilities that are using specific wireless standards that are commonly used with IEEE 802.11 access points. On the realism of the Internet, security has been perceived as a prominent inhibitor of embracing the cloud paradigm. It is resource storage and management that may lay in any since the cloud environment is a distributed architecture, which place of the world, many concerns have been raised over its vulnerabilities, security threats and challenges. The involvement of various parties has widened these concerns based on each party's perspective and objective. The Cloud point of view we mainly discuss the causes of obstacles and challenges related to security, reliability, privacy and service availability. The wireless communication Security has been raised as one of the most critical issues of cloud computing where resolving such an issue would result in constant growth in the cloud's use and popularity. Our purpose of this study is to create a framework of mobile ad hoc network mobility model using cloud computing for providing secure communication among smart devices network for the internet of things in 5G heterogeneous networks. Our main contribution links a new methodology for providing secure communication on the internet of smart devices in 5G. Our methodology uses the correct and efficient simulation of the desired study and can be implemented in a framework of the Internet of Things in 5G.

***Keywords**: Mobile Ad Hoc Networks (MANET); Mobility Models; Cloud Computing; Internet of Things; Smart Devices; 5G Heterogeneous Network.*

INTRODUCTION

The proposed research is a step forward in the field of cloud and internet of things in 5G heterogeneous networks where we propose a new mobility model framework using cloud computing for communicating on the internet of smart devices of the 5G network (Palattella, 2016). The proposed research work in this research is an enhancement and implementation of existing mobile ad hoc network communication using the cloud in the

framework of the internet of things (Yuste, 2011). The research outcome is to establish a new framework for secure communication on the internet of smart devices. The proposed research uses the correct and efficient simulation of the desired study and can be implemented in a framework of the Internet of Things.

The most wireless network of today consists of cells. Each cell contains a base station that can be wired or wirelessly connected. The smart devices have a very useful feature Wi-Fi Direct. Using this feature any device can connect and form an ad hoc network. If one device has internet, then this device can connect to the cloud and create an internet of smart devices. It is expected that by 2025, the development of the internet of smart devices connected exponentially with 75 billion smart devices (Statista, 2020). This development will not depend on mankind's population but the reality that units we utilize consistently (See figure 1 for statistics between 2015-2025) (Statista, 2020).

The reality of interconnectedness things is cooperating man to machines and machines to another machine. They will be talking with each other. But Monitoring and tracking of movable devices are some of the most comprehensive issues. The definition of the internet of things can be described as "a pervasive and ubiquitous system which empowers screening furthermore control of the physical earth by collecting, processing, also analyzing that information created eventually sensors" (Alam, 2018).

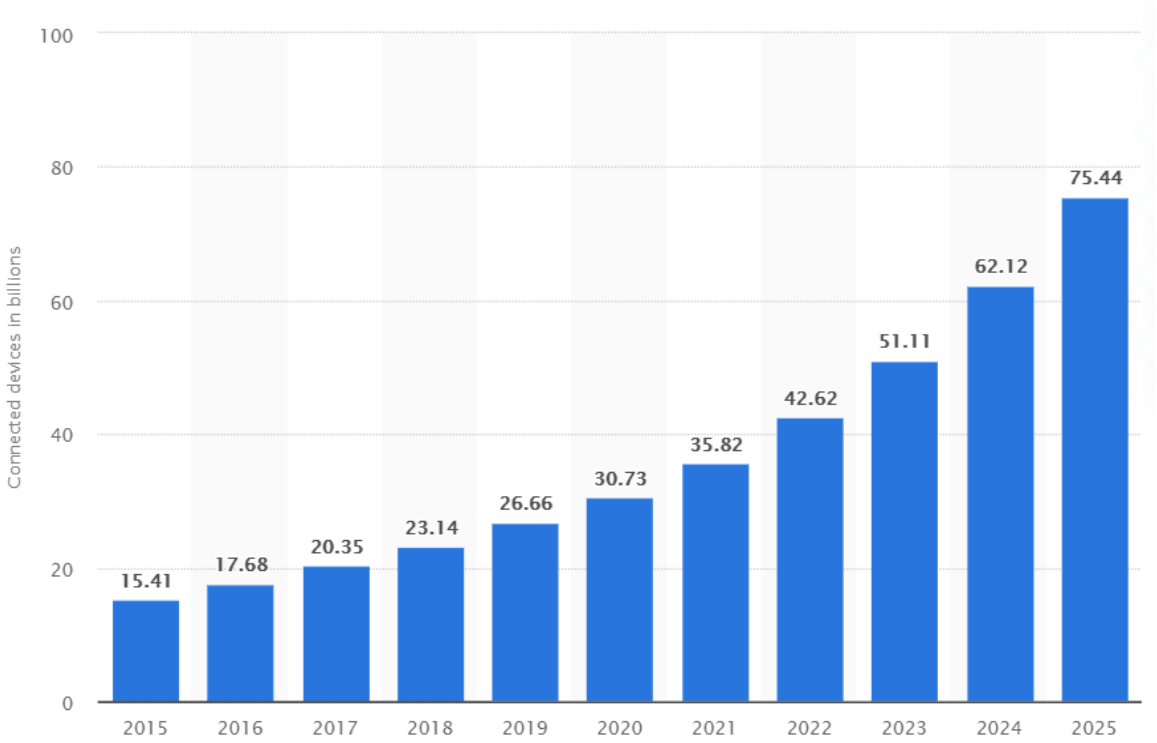

Figure 1. IoT device statistics between 2015-2025

This evolutionary paradigm enables its users to deploy a connection to a network of computing resources in an effortless fashion, where users can rapidly scale up or down their demands with trivial interaction from the service provider.

Growth of the Internet of Things

The growth of the internet of things initially started in 2008 by connecting the physical objects to the internet (Alam, 2010). The physical objects are connected to a smart database that has a collection of smart data. The framework has the image recognition technology for identifying the physical object, buildings, peoples, logo, location, etc. for business and customers. Now the internet of things is shifting from information-based technology to operational based technology i.e. IPV4 (man 2 machines) to IPV6 (machine 2 machines) (Alam, 2015). It combines sensors, smart devices and interfaces like Smart Grid. In wider respect, each of the previous consumers has their concerns over cloud computing vulnerabilities and challenges which might prevent them from their objectives.

The following are the components of the internet of things (Alam, 2020).

I. Identifiers

II. Sensors

III. Communications

IV. Computations

V. Services

VI. Semantics

Three technologies contributed to the internet of things growth.

The ubiquitous computation that has the capacity of intelligent physical objects that execute on the computation framework (Rahmati, 2010). Internet Protocol (IPV6) using ubiquitous computing that covers the area of network and support talking from machine to machine. IPv4 internet has a drawback to adding billions of smart gadgets together, but it is possible in IPv6 internet because it enables the internet of things to connect billions of smart gadgets securely (Alam, 2019).

Connection using ubiquitous computing that uses the fixed cell network or mobility with using sensor connectivity. These technologies should be enhanced regularly so that it allows the progress of internet of smart devices including multi-sensor framework to store, compute, analyze and process capabilities with smaller in size and lowest energies required. The main contribution of this article links a new secure communication model using cloud computing and MANET technologies in the area of the internet of things. The communication security idea depends on three main points in the designing of the internet of things architecture. It is not easy to manage information getting from millions of sensors in a centralized framework of smart devices collection. It is not easy to manage network resources in a large network that can collect environmental information from the centralized framework. It is very hard to manage sensors that execute the same kind of data-parallel and stored in the centralized framework (Alam, 2020).

The time is not far away when billions of physical things linked together in real-time. They can communicate with each other and forwarding, and process required data in the cloud. But there is a lack of technical standardization security perspective on the internet of smart things (Alam, 2019).

Cloud Computing

Cloud computing has been regarded as one of the most popularized computing paradigms. It came likewise an outcome for developments done past computing paradigms that incorporate parallel computing, grid computing, disseminated computing also other computing paradigms (Alam, 2018). Cloud computing gives its customers with three essential administration models: SaaS, PaaS, and IaaS. Software as a service (SaaS) is mainly intended to end users who need to use the software as a part of their daily activities. Platform as a service (PaaS) is mainly intended for application developers who need platforms to develop their software or application. Infrastructure as a service (IaaS) is mainly intended to network architects who need infrastructure capabilities (Baha, 2020). The communication security challenges and threats for communicating in a cloud perspective internet of smart devices are the most important aspect (Alam, 2018). In this article, the author identified some security challenges and three ats. The first challenge is Service disruption due to attacks. In recent times, external attacks can be held responsible for major security breaches in a cloud environment.

Therefore, the cloud provider must step up preventive measures to diminish the severity of these attacks. The second challenge is the Denial of service attacks (Singh, 2019). It is provisioned as unique, frequent and simple attacks. The difficulty arises when it comes to distinguishing the illegal packet from the legitimate packet. These attacks need time collaboration, where it can be triggered by amateur hackers since they only have to run simple codes and tools. As a result, the targeted service provider will be flooded by packets and become out of service. The mitigation of such attacks can be handled through various technologies (Nayyar, 2019).

One of these technologies is the intrusion detection system. It is a software that demonstrates its efficiency especially when attack duration for a long period. Nowadays, there are efforts to make a brand-new hybrid intrusion detection technology that can sustain a variety of attacks. The third challenge and threat are Service hijackings. This risk of service hijacking illustrates a crucial issue that compromises the confidentiality, integrity and the availability of service. Intruders mainly tend to attack software vulnerabilities or use specified software to gain critical information such as passwords and usernames. As a result, attackers would gain full control of cloud service and endanger it (Deep, 2019).

The mitigation of such attacks can be addressed by preventing the exchange of critical information such as passwords and usernames (Alam, 2018). The next challenge and threat are VM-level attacks. Since the cloud environment is entirely built around the concept of virtualization, the cloud provider must deploy a virtual machine (VM) technologies. One of these technologies is a hypervisor which is accountable for running and managing the VM. Service providers should critically consider all major weak points within hypervisors. Finally, the cloud provider must crucially inspect security models of their interfaces. Next is Cloud Multitenancy. The cloud environment promises its consumers by the leverage of shared resources (Alam, 2019). To materialize the concept of sharing, cloud provider employs multi-tenancy. Practically, it is provisioned as software architecture to implement a full utilization of resources.

Cloud-MANET Model

The smart device to smart device communication in the cloud-MANET framework of the internet of things is a novel methodology that discovers and connected nearby smart

devices with no centralized infrastructure. The proposed technique will be very useful in machine to machine (M2M) networks because, in the M2M network, there are several devices nearby to each other. The smart device users will use cloud service to discover the devices, minimize useful information in big data and can process videos, images, text, and audio. In the proposed framework, the smart device will consider as service nodes (Alam, 2016).

Motivation

The MANET is a very popular network to get connected anywhere at any time (Mahapatra, 2019). Cloud provides service for storing and accessing information. The integration of cloud and MANET provides the facilities to access cloud inside MANET of smart devices. In real-life situations, the group of smart device users wants to connect in a meeting at a place where no network services are present. These users may form MANET among smart devices. Also, they can use the cloud service only if one device has the internet in the group.

Research organization

The organization of the rest of the research paper is as follows: 1. The introduction presents a brief overview of this research paper. 2 – Literature Survey, 3 – Presents a brief overview of Cloud-based Mobile ad doc networks of Smart Devices, 4- Communication Security issues and challenges in cloud and Internet of Smart Devices, 5 presents the Cloud-MANET mobility model, 6 presents the results interpretation and 7the represents the conclusion of the research paper and future scope of the proposed research.

Research contributions

This research paper proposes the Cloud-MANET mobility model for communication among smart devices. All these items can be summed up in the following list:

1. Form a MANET
2. Access the ad hoc network in the range of Wi-Fi.
3. Register smart devices in the range of Mobile Ad Hoc Network.
4. Register smart devices in Cloud
4. Implement the Cloud-MANET model among all smart devices.
5. Start communication.

The smart device to smart device communication in the cloud-MANET framework is a novel methodology that discovers and connected nearby smart devices with no centralized infrastructure. The existing cellular network doesn’t allow to connect all smart devices without centralized infrastructure even if they are very near to each other. The proposed technique will be very useful in machine to machine (M2M) networks because, in the M2M network, there are several devices nearby to each other. So the implementation of the

MANET model in the smart device to smart device communication can be very efficient and useful to save power as well as the efficiency of spectrums. The cloud-based services in MANET modeling for the device to device communication can be a very useful approach to enhance the capabilities of smart devices. The smart device users will use cloud service to discover the devices, minimize useful information in big data and can process videos, images, text, and audio. In this article, I proposed a new middleware framework to enhance the capability of MANET and cloud computing on the internet of smart devices that can be useful in the 5G heterogeneous network.

LITERATURE SURVEY

In the 1980s, with the evolution of the internet, the foundation of an emerging grid computation was established (Foster, 2000). The foundation involved various principals which employ the internet in a way in which users are provisioned as resource nodes. A grid coordinates these resources nodes and dispenses takes to them thus the entire computation is viewed as a cumulative fashion. The principles paved the way for a novel computing paradigm which eventually carved today's distribution concepts. In the 1990s, the concept of virtualization was driven to the application tier (Hoffman, 2011). It followed by employing virtualized private network connections that share the same physical channel. In 2002 researchers published an article entitled "Connecting the Physical World with Pervasive Networks", in this article they address the challenges and opportunities of instrumenting the physical world with pervasive networks of sensor-rich, embedded computation (Estrin 2002). Cloud computing came as a consequence of the continued development of computing paradigms. The emergence of these technologies has established the appearance of (SaaS) software as a service which states that consumers are not required to purchase the software rather than paying according to their demand. In the mid of 2006, Amazon achieved a prominent milestone by testing elastic computing cloud (EC 2) which initialized the spark of cloud computing in it. However, the term cloud computing was not found until March 2007. The following year brought even more rapid development of the newly emerged paradigm. Furthermore, cloud computing infrastructure services have widened to include (SaaS) software as a service. In the mid of 2012, Oracle cloud has been introduced, where it supports different deployment models. It is provisioned as the first unified collection of its solutions which are under continuous developments. Nowadays, typing cloud computing in any search engine will result in a tremendous result. For example, it would result in more than 139,000,000 matches in Google. In 2009, (Evan Welbourne et al, 2009) published an article entitled "Building the Internet of Things Using RFID", in this paper authors presented RFID-based personal object and friend tracking services for the IoT that proposed tools can quickly enable. In 2010, (Gerd Kortuem et al., 2010) published an article on "Smart objects as building blocks for the internet of things", in this article they presented the development of a new flow-based programming paradigm for smart objects and the Internet of Things. In 2011, (Ahmed Rahmani et al, 2011) published an article on "Context-Based Network Estimation for EnergyEfficient Ubiquitous Wireless Connectivity", in this article they presented context-based network estimation to leverage the strengths and provide ubiquitous energy-efficient wireless connectivity. In the article researchers presented Wi-Fi-based sensors for the internet of things, they focused on measurement of the range performance.

In May 2014, (Jiang et al, 2014) published an article entitled "An IoT-Oriented Data Storage Framework in Cloud Computing Platform", they focused on data storage

framework that is not only enabling efficient storing of massive IoT data as well as integrating both structured and unstructured data. In this article, the authors are introduced to the IoT ecosystem and key technologies to support IoT communications (Rathee, 2019). In 2016, (Maria Rita Palattella et al, 2016) published an article entitled “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models”, in this article they presented 5G technologies for the IoT, by considering both the technological and standardization aspects.

CLOUD-BASED MOBILE AD-HOC NETWORKS OF SMART DEVICES

MANET

The Ad hoc network can connect all smart devices in the decentralized system. The mobile ad hoc network is a self-organizing collection of wireless mobile nodes that form a temporary network without the aid of a fixed networking infrastructure (Zhang, 2003) or centralized administration, as shown in the following figure 2.

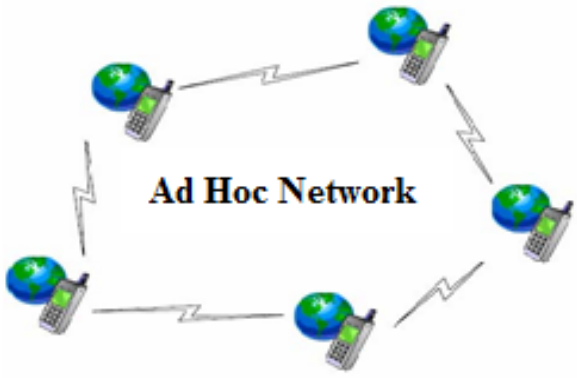

Figure 2: Ad Hoc Network

Messages requiring a destination outside this local neighborhood zone must be hopped or forwarded by these neighbors, which act as routers, to the appropriate target address.

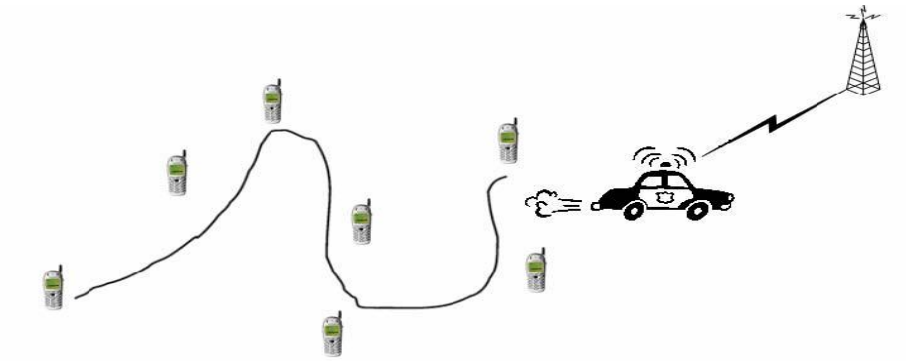

Figure 3: Controlling the movement of Nodes

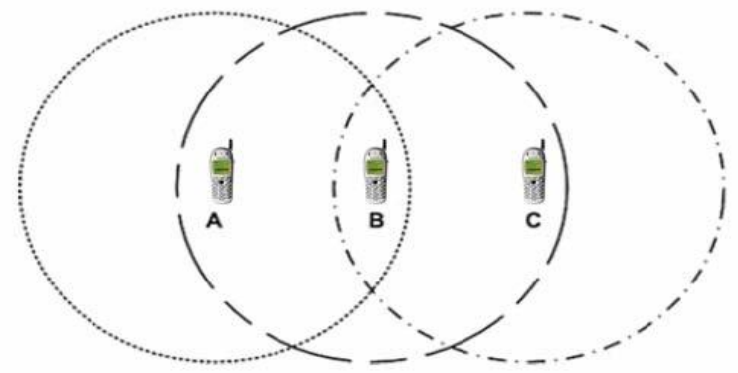

Figure 4: MANET with three nodes

Discovering the smart devices using probability-based model

Here in the probability-based model, we accept a thick portable MANET system. The smart devices are located on the 3D plane in directions x-axis, y-axis and z-axis accessible. The whole area is divided into cells over the wireless network. The area of all cells is fixed so that the android smart devices can travel within the range of cells. The smart device discovers the neighborhood devices in a binary digit within the same cell area. Verifiable information reserved by a smart device that discovers another device (Alam, 2018). The calculation of the ideal track in the Hidden Markov Model (HMM) is exorbitant particularly when the quantity of Android smart devices turns out to be expansive. Result interpretation shows that the movement of the target can only take place between neighboring cells. Besides, data is developed in a disseminated way utilizing a weighted normal of the angle and the move likelihood. The angle results from Android smart device versatility: an android smart device experiencing the objective spares the objective's area and sets the inclination.

Table 1: PBM statistics

	PBM
Average Path Length	8.0
Average Stretch Factor	2.2
Success Rate	96.5%

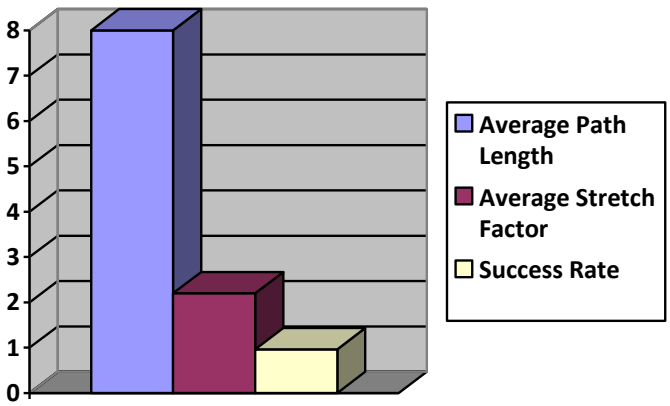

Figure 5: PBM statistics

Discovering the smart devices using hidden Markov model

For discovering the smart devices, the hidden Markov model is utilized in the 2Dimensional plane area. This model is connected to the working area and devices move inside the area and this model found neighborhood devices within the range. We form the transition matrix in the area of the wireless network, discover all the smart devices and put in the transition matrix (Alam, 2019). The following parameters are used for discovering smart devices. This model contains the following parameters.

Let $S=S_1, S_2 \ldots\ldots S_N$ where S=state, S_1 is the first state, S_2 is the second state and so on. Each cell depends on one state.

The transition matrix probability $P= P_{ij}(1 \leq i \leq N)$ where P_{ij} characterized to move likelihood from S_i to S_j.

Geometrically, P_{ij} is just significant if Si, S_j is neighborhood states. Now rearrange states to move up, down, left and right. Whatever is left components within the framework are all 0s. The following figure represents the transition matrix using the hidden Markov model.

A starting smart device in each cell represented by $\Pi = \Pi_i\ (1 \leq i \leq N)$.

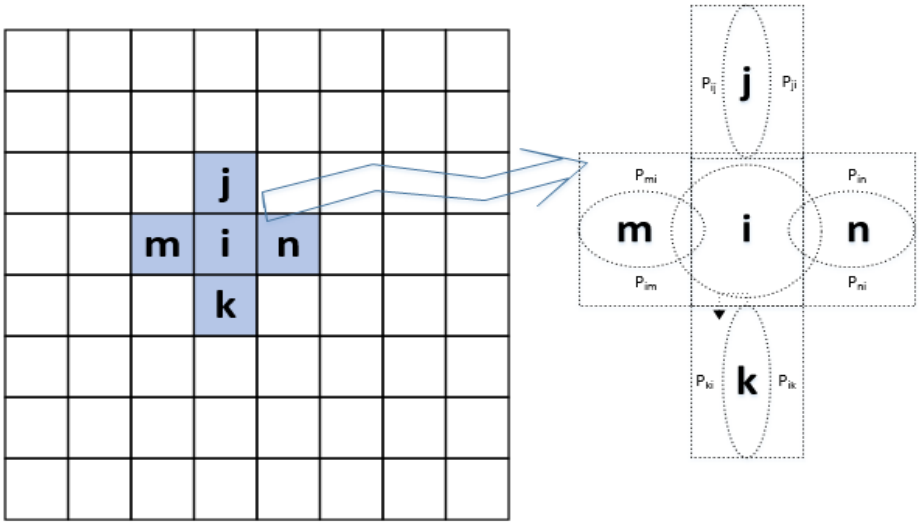

Figure 6: Discovering area by HMM model

The smart devices in the Ad-hoc network can be used to discover the signals using the Viterbi algorithm. Let $O_1, O_2, \ldots, O_n$ are the observation of discovering the devices. Every smart device sends a report of observations in meanwhile. This algorithm discovers the way at each step by maximizing the likelihood. This process is so expensive and time consuming for the rush of devices. The whole way can be accomplished by essentially joining the sub-track at every cell (Alam, 2019). Even though the HMM model has been utilized as a part of the target following applications, it adds a few requirements when connected to appropriate MANET. It depends on the device's previously founded probabilities of discovering. The Hidden Markov model depends on the state's probability.

The matrix represents the information in every cell. When the Android device enters a new cell, it removes previous data and updates the information with new data.

Table 2: PBM vz. HMM statistics

	PBM	HMM
Average Path Length	8	8.3
Average Stretch Factor	2.2	2.3
Success Rate	96.5%	95%

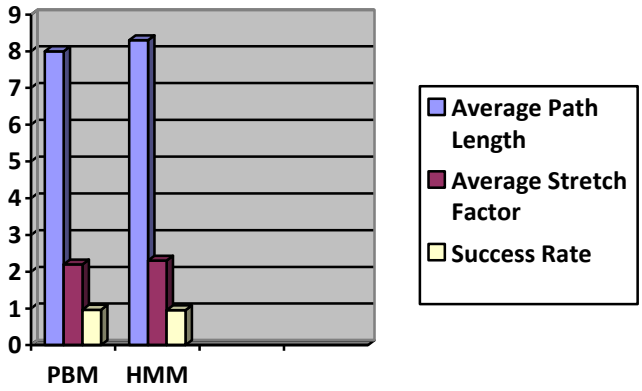

Figure 7: PBM vz. HMM Model statistics

Discovering the smart devices using gradient-based model

For discovering the smart devices, the gradient model works to find the devices and share the ideas to develop and send the information. This inclination is kept up not by correspondence among android smart devices, but rather exclusively by the android smart device versatility inborn in the MANET (Alam, 2018).

At the point when an android smart device recognizes the objective, the gradient value will set 1 also discover android smart devices in the region where the ad hoc network is established. The gradient data is the area that focuses on some time back. We utilize an exponential diminishing capacity to continue diminishing this quality at that Android smart device at the progression of time.

According to the physical law, the node distance is proportional to one upon the distance of the event, for example

$$\text{Node (distance)} \ \alpha \ 1/\text{event}^{\text{distance}}$$

The following formula represents the gradient over time.

More specifically, we construct the gradient with respect to time t as equation 1:

$$\text{Gradient (time)} \ \alpha \begin{cases} 1 & \text{time} = 0 \\ \text{event}^{-\text{time}} & 0 < \text{time} < \text{Totaltime} \\ 0 & \text{time} > = \text{Totaltime} \end{cases}$$

The gradient model finds the gradient distribution over time. If time=0 then the gradient value will be 1. If time is greater than the total time then the value of gradient will be 0. Otherwise, the gradient is proportional to one upon time power of the event.

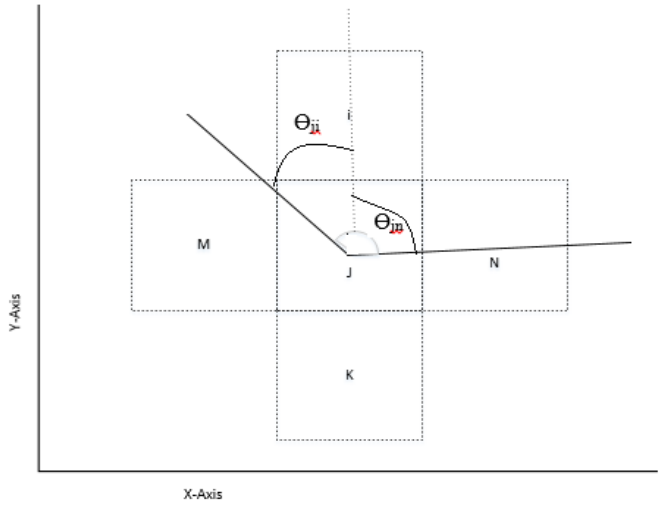

Figure 8: Motion in Gradient-based Model

Table 3: PBM, HMM vz. Gradient statistics

	PBM	HMM	Gradient
Average Path Length	8	8.3	15
Average Stretch Factor	2.2	2.3	3.91
Success Rate	96.5%	95%	89.5%

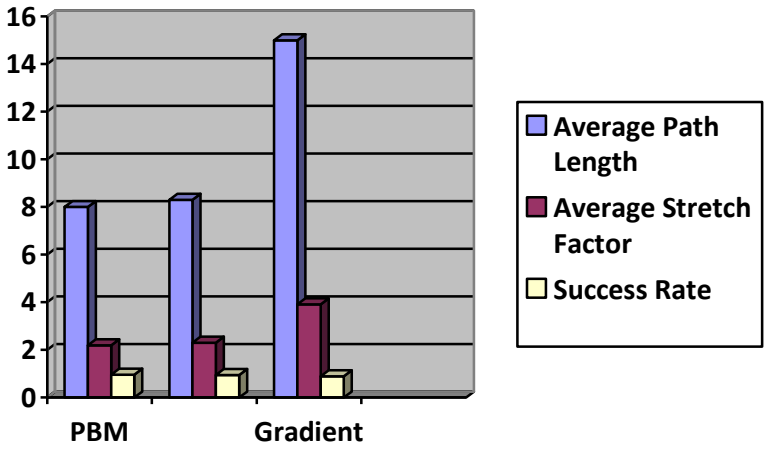

Figure 9: PBM, HMM and gradient Model statistics

So, the achievement rate of the PBM model is best in the examination of HMM and Gradient Model. So, we utilize the PBM model for outlining the Ad Hoc Network among android smart devices.

Put smart devices in the range of MANET

The smart devices are put within range of wireless MANET that considers coverage and connectivity of Wi-Fi ad hoc networks. Every android smart device is expected to have a settled Wi-Fi region and an altered correspondence range (Alam, 2018). The objective is to accomplish a certain reach scope and/or correspondence network prerequisite.

At first, the wi-fi Ad Hoc Network is in the dynamic state. If a region surpasses the required level of scope, excess brilliant Android smart devices will get themselves pointless and switch to the rest state. An ad hoc network is inactive all the time, when one device wants to make the connection with another device then it creates a connection with their neighborhood within the discovering area. A resting android smart device additionally occasionally awakens to enter into a ready state. The ready state detects the devices and comes back to the dynamic state.

Implement MANET among smart devices

The fundamental supposition of building the ad hoc network communication for communication among a group of android smart devices is that they can communicate securely within the range. So many researchers are moved in the field of communication among android devices without cellular network. Moreover, ad-hoc network communication on Android devices is progressively connected due to Google. Google provides an open-source for Android developers. It's a freely available code for developers to design and develop their applications as well as research projects using Android SDK. So, we focus here on the implementation of a wireless ad hoc network among a group of Android devices within the range of Wi-Fi.

The smart device to smart device communication in the cloud-MANET framework of the internet of things is a novel methodology that discovers and connected nearby smart devices with no centralized infrastructure. The existing cellular network doesn't allow to connect all smart devices without centralized infrastructure even if they are very near to each other.

The proposed technique will be very useful in machine to machine (M2M) networks because, in the M2M network, there are several devices nearby to each other. So the implementation of the MANET model in the smart device to smart device communication can be very efficient and useful to save power as well as the efficiency of spectrums. The cloud-based services in MANET modeling for the device to device communication can be a very useful approach to enhance the capabilities of smart devices.

The smart device users will use cloud service to discover the devices, minimize useful information in big data and can process videos, images, text, and audio. In this article, I proposed a new framework to enhance the capability of MANET and cloud computing on the internet of smart devices that can be useful in the 5G heterogeneous network. In the proposed framework, the smart device will consider as service nodes. This model also covers security and reliability as well as the vulnerability issue of communication.

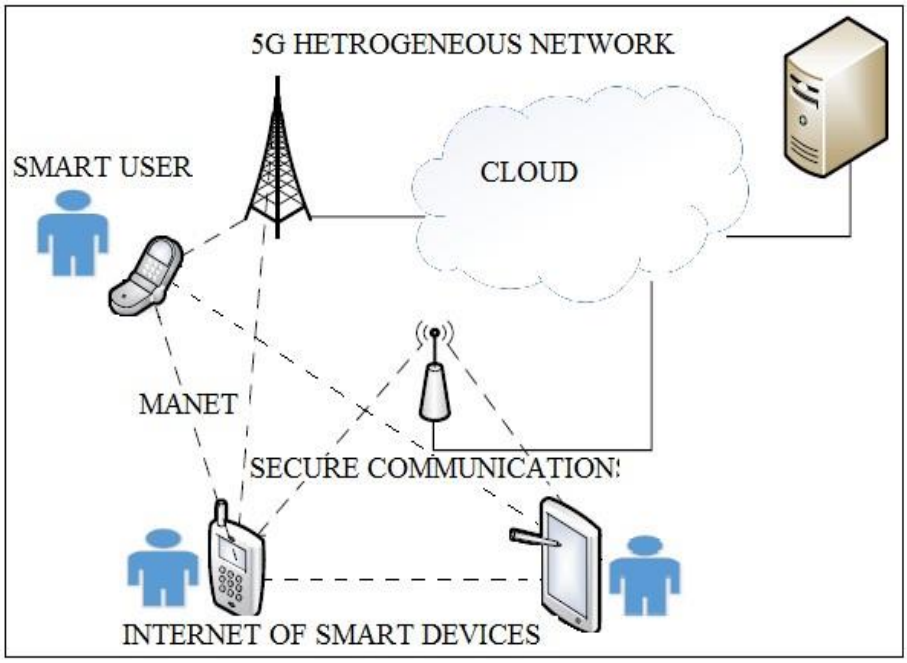

Figure 10: Cloud-MANET model in 5G heterogeneous networks

COMMUNICATION SECURITY ISSUES AND CHALLENGES IN CLOUD AND INTERNET OF SMART DEVICES

The communications security is a challenge when two or more smart devices want to communicate without listening to the shared data by the third party. The smart devices are electronic devices that are connected to other devices or networks through network protocols such as a smartphone, tablets, smartwatch, etc. Wireless mobile ad hoc networks facilitate users to communicate with each other in an infrastructure-less environment. Cloud computing enables the sharing of resources, storage, and services using mobile applications. This study is focused on secure communication among smart devices in the area of Cloud-MANET. In Cloud-MANET, the smart devices are dynamically joined and created a network on their own called MANET and they can access cloud service. But there are more challenges for secure communication in this own created network that access cloud service. In this paper, I proposed a key exchange algorithm for secure communication in the Cloud-MANET of smart devices. The key issues concerning this approach provide the security analysis for communication in a cloud-based ad hoc network. This algorithm works like a protocol among all connected smart devices and provides communication security so that the communication will be more secure among all smart devices in the proposed area. This algorithm is implemented as a mobile application and tested in the cloud-MANET of smart devices. The results are found positive and can be implemented in the framework of the internet of things in 5G heterogeneous networks.

The Mobile ad hoc network is a kind of wireless network that is self-organizing and auto connected in a decentralized system. Every node in MANET can be moved freely from one location to another in any direction. They can create a network with their neighbors' smart devices and forward data to another device like a router. The cloud-MANET framework of smart devices is composed of cloud computing and MANET. This framework can access and deliver cloud services to the MANET users through their smart devices where all computations, data handling, and resource management are performed. The smart devices can move from one location to another in the area of mobile ad hoc network and at least one smart device in MANET should be connected with the cloud in real-time. Various MANETs can connect with the same cloud, they can use cloud service in a real-time. Connecting the smart device of MANET to cloud needs integration with mobile apps. The MANET model of smart devices in local communication can work very well using the cloud, it is failed when it connects in exist wired networking framework. For working in wireless and wired infrastructure, an access point will be required like gateways. The communication process to connect a smart device with another device in the cloud-MANET framework, every smart device must be configured universally using routing IP address. Also, every device requires searching neighbor device as well as gateways that use its prefixed and assign the universally routing IP addresses. When these devices will connect using cloud services then the main issue is the security of communication. The question is arises here How are communication security in the public cloud and MANET model?. The proposed algorithm for secure communication in the cloud-MANET model is implemented and integrated with mobile apps. Java programming is used to develop a mobile app. This mobile app should be installed on every smart device of MANET infrastructure.

This convention will work in a Wi-Fi-based remote especially in the ad hoc network system. The performance results are shown in the figures with the comparison of the performance of existing popular algorithms for key exchanges includes AES, DES, DES3 and Blowfish algorithms through size, data and execution time. The proposed algorithm is implemented in C-Sharp.net technology like a mobile app and installed at smart devices also it is tested on three smart devices inside the range of MANET. The algorithm also works on different MANETs and use the cloud as a service. Table 4 shows the comparisons between existing and proposed algorithms. Figure 11 shows the comparative analysis of existing and proposed algorithms.

The experiment was conducted using the smart device with proposed algorithm implementation and another existing algorithm was installed on the same configuration devices. We notice the performance of the proposed algorithm was better than all existing algorithms. Figure 12 shows the performance analysis of the algorithms.

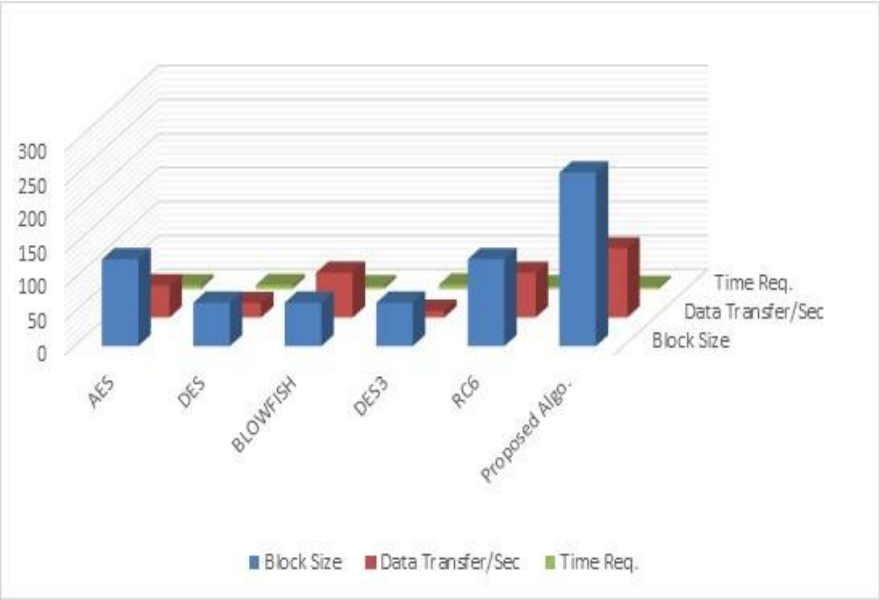

Figure 11: Comparative analysis of existing and proposed algorithms.

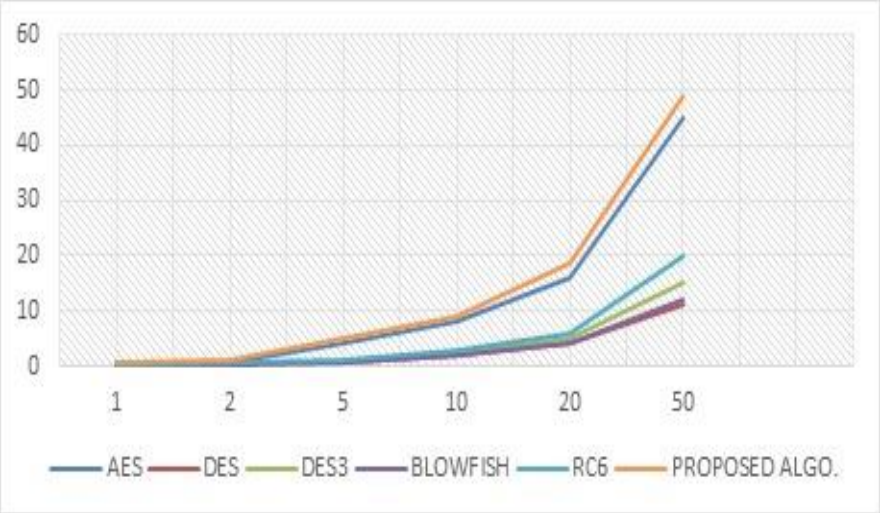

Figure 12: Algorithms performance in comparisons of block size and time is taken.

In the future, this algorithm may be integrated with Wi-Fi Direct protocol and implement it on smart devices. This algorithm can be used to take a meeting with colleges in a building or outside securely using smart devices. The experimental results of the proposed algorithm have a better performance than all existing algorithms. DES algorithm showed poor performance while RC6 showed very good performance. Our proposed framework can play very important roles in the framework of the Internet of Things where smart devices will communicate with each other securely.

CLOUD-MANET MOBILITY MODEL

The Cloud MANET mobility model is an integrated model of Cloud computing and MANET technologies. The functionality of MANET is depended on the mobility of its nodes and connectivity also resources such as storage and energy efficiency. In Cloud computing, cloud providers retain network infrastructure, storage facilities, and software applications that support flexibility, efficiency, and scalability. In the Cloud MANET mobility model, smart devices of MANET can communicate with each other but at least one smart device must be connected to cellular or Wi-Fi networks. All smart devices of MANET should be registered in the cloud individually. The proposed model will activate in disconnected mode. When a MANET is activated then cloud services will activate in real-time and provide services to the smart devices of MANET (Alam, 2016). The smart devices send a request to the cloud for a session of connectivity. Cloud provides the best connection to the smart device. The life of a connection is described as the probabilistic function as follows.

Session (life)) = $\left(\frac{\int_{life}^{\infty}\left(\left(\frac{1}{2}\right)-\left(\frac{1}{2}\right)erf\left(\log\left(\frac{u}{\mu}\right)\div\sqrt{2}\sigma\right)\right)du}{\left(\frac{1}{2}\right)-\left(\frac{1}{2}\right)erf\left(\log\left(\frac{life}{\mu}\right)\div\sqrt{2}\sigma\right)}\right)$

The expression in the integral will be 0 if the limit tends to ∞. After computing session life by using the above probabilistic function, every smart device requires computing the values of σ and μ.

These two parameters are related to the connection establishment among MANETs and Cloud service that can be measured through smart devices using the following function. $e\mu(1/2)\sigma^2$.

When a smart device estimates the connection life between MANET and Cloud, it will transfer or receive data securely. The connection will be activated, and stability will be high. We consider that every smart device is assured to establish the route between MANET and cloud when they create a session in the cloud. The smart devices can move through the maximum speed 20m/s from one location to another location by using the Gauss-Markov mobility model. The following formula is used to calculate the moving speed and direction of the smart device within a MANET range (Alam, 2020).

Speed^{t} $= \lambda Speed_{t-1} + (1-\lambda)\,\bar{Speed} + \sqrt{(1-\lambda^2)\,Speed_{t-1}^{G}}$

and

Direction$_s$ = λDirection$_{t-1}$ + (1 − λ) Direction^{-} + $\sqrt{(1-\lambda^2)\,Direction_{t-1}^{G}}$

The λ is used as a random degree when computing speed as well as the direction of smart device in a duration (t).

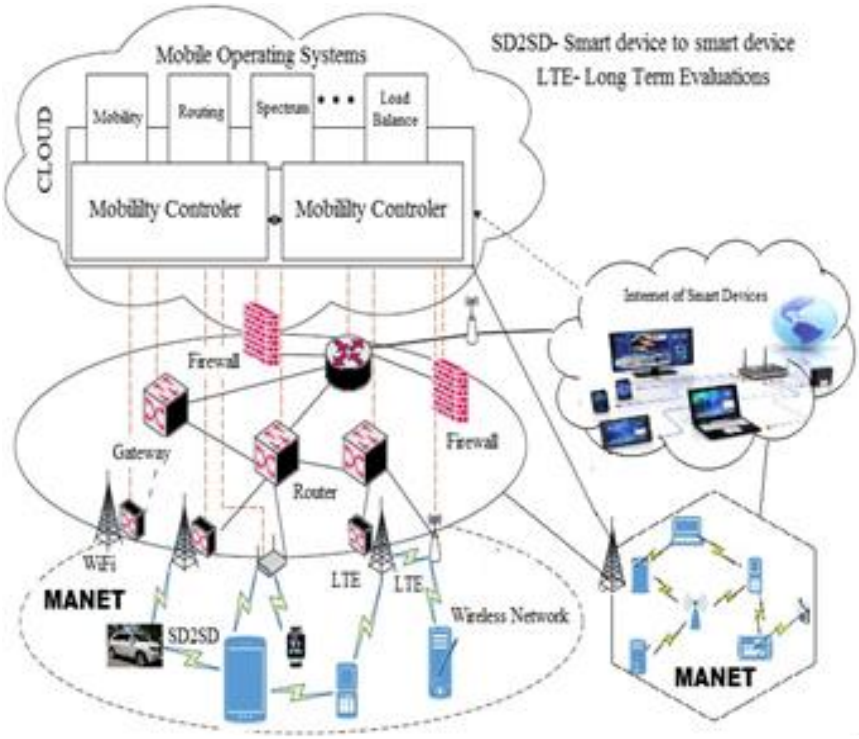

Figure 13: Working Process of Cloud MANET mobility model

The transmission (t_s) of information (I_k) among the number of smart devices (S_n) can be estimated during the time interval [t_i, t_{i-1}]. The smart devices can move within the MANET and access the cloud service using the multidimensional function (ε^k).

$\varepsilon k = CSn \times tk \times Ik$

where k=0,1,2,3.....∞(+ve).

If smart devices have moved outside the MANET then k will be a negative value. Here we consider that the transformation of information happens simultaneously. We know that the probability is proportional to the one divide by information.

$P^k \propto \frac{1}{I_k}$

The probability density function for transmission is calculated mathematically as follows.

$P_k(S_n \mid \varepsilon_k, I_k, t_k) = 1 - \int_{-\infty}^{\infty} M_Q\left(\sqrt{\frac{2\gamma^2}{1-\gamma^2} \times \frac{S_n}{t_k}}, \sqrt{\frac{S_n}{1-\gamma^2} \times 2\gamma}\right)$

Now we have divided the probability density function of all the connections using the entropy per symbol of all connected devices in 3-dimensional directions.

.

$$P_{X_k}.P_{Y_k}.P_{Z_k} \log_3 \frac{1}{P_{X_k}} \frac{1}{P_{Y_k}} \frac{1}{P_{Z_k}}$$

Here $\varepsilon_2\left(\frac{\delta}{\alpha}, S_k, \rho\right)$ is the Chi-Square distribution method that is used here for convergence. Now we will calculate all the probabilities, entropies in each direction and finally, we draw the transition matrix from the probabilities of all connected devices.

Now we will find entropy per symbol row-wise said H_1, H_2, H_3....., H_K according to the above transition matrix. After findings of H_1, H_2, H_3....., H_K we will found the whole entropy per symbol of the smart devices.

$H=H_1.P_1 + H_2.P_2 + H_3.P_3 + ...H_K.P_K.$
We have calculated the velocities of smart devices using the Gauss-Markov Mobility Model in the multidimensional area of MANET. We have tested on simulation using 5, 10 and 50 smart devices at 10 m/s, 20 m/s, and 50 m/s.

The proposed cloud MANET framework consists of three algorithms. The first algorithm is used to discover the smart devices within the range of MANET. The second algorithm focused on discovering the gateway point to connect to the cloud and the third algorithm is used to establish a connection, provide session and transfer data from one smart device to another using cloud as a service.

Table 4: Transmission in MANET of Smart devices at 10 m/s.

Devices	εk =0.1	εk =0.2	εk =0.4	εk =0.6	εk =0.8	εk =1
5	2.1	2.2	2.3	2.2	2.2	2.3
10	3.1	3.3	3.3	3.3	3.4	3.3
50	4.9	4.8	4.7	4.6	4.8	4.7

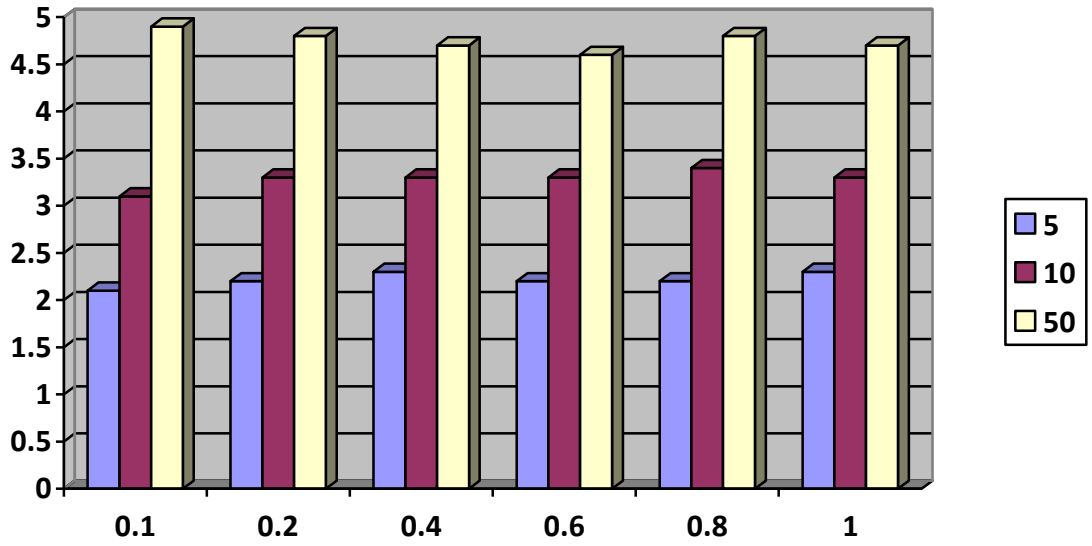

Figure 14. Transmission in Cloud-MANET at 50 m/s

The following algorithm is used to find the new position of the smart devices in MANET.
Get the position (X_1, Y_1) of smart devices in the ad-hoc network.
Get current Speed (s) of the smart moving device in the ad-hoc network.
The basic formula to get speed is as follows.
Speed (s)= distance (d)/time (t).
If time=t and angle is θ (positive) then we consider the new location of the smart device is as follows.
$X_2 = X_1 + s * t * \cos(\theta);$
$Y_2 = Y_1 + s * t * \sin(\theta);$
If theta is negative, then
$X_2 = X_1 - s * t * \cos(\theta);$
$Y_2 = Y_1 - s * t * \sin(\theta);$

4. Find the real Location of smart device.
Location L=get New Location (new Point(smart device Location)); Example:L = (x_1,y_1)
5. Find theoretical location
Location ref=get NewRef Location (new Point(smart device Location)); Example: ref=(x_2,y_2) 6. Find distance between L and ref.
Distance (d)=$\sqrt{(x_2 - x_1)^2 - (y_2 - y_1^2)}$
Find random location (X, Y) of smart device at thediagonal of triangle.
X=Math.random(d.getX());
Y=Math.random(d.getY());
Find the actual location of smart device according to thediagonal of triangle.
The device may be up or down from diagonal. If the device is upper than the diagonal then increase the value of X and Y as follows.

$X = X + \delta X;$
$Y = Y + \delta Y ;$

Otherwise

$X = X - \delta X;$
$Y = Y - \delta Y;$

9. Return new Location(X, Y)

The following algorithm will compute the velocity of smart devices in Cloud-MANET mobility model.
Input: Number of smart devices, transmission function value (ε_k).
Output: Velocities of smart devices.
Initialization: Counter=0, V=0.
Step 1: Find all probabilities of smart devices in each direction.
Step 2: Find entropy per symbol.
Step 3: Find Transmission in bits/sec.
Step 4: Find velocity (V) in m/s.
Step 5: Counter=Counter+1;
if counter < Number of devices go to step 2 otherwise stop.

The complexity of the algorithm is $O(n^2)$. The Proposed mobility model had been implemented using two mobile applications. These mobile applications are verified on three Samsung devices. One of them is supported by the 4G network and another two are supported by 3G networks. Amazon Web Services (AWS) are used for implementing cloud services. This cloud service will connect to the MANETs. Mobile apps should be installed on every smart device. After installing mobile apps to the devices, the device should be registered in the cloud. The cloud will generate a device id to every smart device who is registered to the cloud. A smart device can communicate with another smart device within the range of the same MANET or another MANET using cloud services.
The smart user will be activated by mobile apps. When he opened smart apps then he had connected with Amazon cloud service automatically and start to communicate with another device. The Amazon cloud provides relational database services for storing smart device information, requests, communicated messages, and neighborhood smart devices information.

The following procedure should be followed by smart devices.
1. Open mobile apps and register in the cloud. The cloud will provide device id and password.
2. Enter device id and password to login to the cloud.
3. Store WPA supplicant.conf on every smart device. This file is used to start MANET service on the smart devices. We had connected this file to our developed mobile apps.
4. Start MANET.
5. Searching neighborhood devices within the range of MANET or search through the device id.
6. Click on the searched device and start communication.

CONCLUSION AND FUTURE SCOPE

The Cloud MANET mobility model can play a most important role in 5G heterogeneous networking. We designed this model to enhance the efficiency and speed of communication. Since the cloud paradigm is based on a distributed architecture, then it is inherited some risks and vulnerabilities that are related to distributed paradigms. The communication security threats and challenges that rely on behind the lure of cloud computing. However, several of these risks have intensified over the cloud paradigm. We analyzed the security requirements and challenges for communication security among all smart devices in cloud computing environment. The proposed model has been developed in the form of a mobile app. The mobile app has started the service of MANET as well as connected with the cloud. We have used cloud service from Amazon. The proposed model of this study has been introduced in the ubiquitous system. The study showed successfully and expectation for a future scope in this area. After researching a lot of how MANET networks work and which are its advantages and disadvantages, I get to the conclusion that this kind of networks could help people in many situations, some of them in critical situations. But as far as Android doesn't support by itself the Ad-hoc mode it's not likely to think that some application could use this kind of networks for the general public. All the modifications I had to make to enable ad-hoc mode just for one device shows us that with most of the current market android smart devices would be totally impossible to do so. The main problem is that although Android is open source, no every single line of the code is really open to the developers. Most of the time the only part that is opened is just the main Android code, but all code related to a specific android smart device that is not part of Android itself, as drivers and specific manufacturers modules it's never released to the public and this make totally impossible for the developers to build some solution to enable Ad-hoc mode in most of the Android smart devices. In addition, although all the manufacturers release all needed code, it's not likely for regular people to make all this process of rooting and flashing a custom kernel and a custom recovery just to install some app. Because of this the only way of really implementing MANET networks in smartphones would be if Google adds support from default Android and final user don't' need to modify anything of their smartphones, just download some applications form the market and run it. Although it's true that MANET networks had high power consumptions and it could be a reasonable point from Google for not supporting Ad-hoc mode, I'm sure that a better alternative than disabling it could be found. For example, it could just active Ad-hoc mode when there is no connectivity from the regular network or let the user decide, knowing the high consume it would have if they want to have Ad-hoc enabled or not. To

sum up, MANET networks on smartphones could be a really useful utility in many daily life situations, but as long as Google doesn't implement native support to them it's not likely to think that they are going to expand to the final user and have a real utilization among them.

REFERENCES

A. J. Yuste, A. Trivino, E. Casilari, and F. D. Trujillo. Adaptive gateway discovery for mobile ad hoc networks based on the characterization of the link lifetime. IET communications, 5(15):2241– 2249, 2011.

Alam T, Benaida M. "The Role of Cloud-MANET Framework in the Internet of Things (IoT)", International Journal of Online Engineering (iJOE). Vol. 14(12), pp. 97-111. DOI: https://doi.org/10.3991/ijoe.v14i12.8338

Alam T, Benaida M. CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). 2018 Nov 1;12(6):74-84. DOI: https://doi.org/10.3991/ijim.v12i6.6776

Alam, T. Cloud Computing and Its Role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI) 2020, 1, 108-115. DOI: https://doi.org/10.34306/itsdi.v1i2.103

Alam, T., Salem, A.A., Alsharif, A.O. and Alhejaili, A.M., 2020. Smart Home Automation Towards the Development of Smart Cities. APTIKOM Journal on Computer Science and Information Technologies, 5(1).

Alam, Tanweer, and B. K. Sharma. "A New Optimistic Mobility Model for Mobile Ad Hoc Networks." International Journal of Computer Applications 8.3 (2010): 1-4. DOI: https://doi.org/10.5120/1196-1687

Alam, Tanweer, and Mohammed Aljohani. "An approach to secure communication in mobile ad-hoc networks of Android devices." In 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015. DOI: https://doi.org/10.1109/iciibms.2015.7439466

Alam, Tanweer, and Mohammed Aljohani. "Design a new middleware for communication in ad hoc network of android smart devices." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, p. 38. ACM, 2016. DOI: https://doi.org/10.1145/2905055.2905244

Alam, Tanweer, and Mohammed Aljohani. "Design and implementation of an Ad Hoc Network among Android smart devices." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1322-1327. IEEE, 2015. DOI: https://doi.org/10.1109/ICGCIoT.2015.7380671

Alam, Tanweer, Arun Pratap Srivastava, Sandeep Gupta, and Raj Gaurang Tiwari. "Scanning the Node Using Modified Column Mobility Model." Computer Vision and Information Technology: Advances and Applications 455 (2010).

Alam, Tanweer, Parveen Kumar, and Prabhakar Singh. "SEARCHING MOBILE NODES USING MODIFIED COLUMN MOBILITY MODEL.", International Journal of Computer Science and Mobile Computing, (2014).

Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538.

Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94

Alam, Tanweer. "Tactile Internet and its Contribution in the Development of Smart Cities." arXiv preprint arXiv:1906.08554 (2019).

Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.

Aljohani, Mohammed, and Tanweer Alam. "An algorithm for accessing traffic database using wireless technologies." In Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on, pp. 1-4. IEEE, 2015. DOI: https://doi.org/10.1109/iccic.2015.7435818

Aljohani, Mohammed, and Tanweer Alam. "Real Time Face Detection in Ad Hoc Network of Android Smart Devices", Advances in Computational Intelligence: Proceed-ings of International Conference on Computational Intelligence 2015. Springer Singa-pore, 2017. DOI: https://doi.org/10.1007/978-981-10-2525-9_24.

Baha Rababah, Tanweer Alam, Rasit Eskicioglu, "Next Generation Internet of Things Architecture Towards Distributed Intelligence: Reviews, Applications, and Research Challenges", Journal of Telecommunication, Electronic and Computer Engineering, Vol 12, No 2, 2020.

Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., & Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. Sensors, 19(20), 4444.

Estrin, Deborah, David Culler, Kris Pister, and Gaurav Sukhatme. "Connecting the physical world with pervasive networks." IEEE pervasive computing 1, no. 1 (2002): 59-69.

Foster, Ian. "Internet computing and the emerging grid." Nature (2000): 1-4. DOI: https://doi.org/10.1038/nature28024

Hoffmann, Marco, and Markus Staufer. "Network virtualization for future mobile networks: General architecture and applications." In 2011 IEEE international conference on communications workshops (ICC), pp. 1-5. IEEE, 2011.

Jain, R., Jain, N., & Nayyar, A. (2020). Security and Privacy in Social Networks: Data and Structural Anonymity. In Handbook of Computer Networks and Cyber Security (pp. 265-293). Springer, Cham.

Jiang, L., Da Xu, L., Cai, H., Jiang, Z., Bu, F. and Xu, B., 2014. An IoT-oriented data storage framework in cloud computing platform. IEEE Transactions on Industrial Informatics, 10(2), pp.1443-1451.

Kortuem, Gerd, Fahim Kawsar, Vasughi Sundramoorthy, and Daniel Fitton. "Smart objects as building blocks for the internet of things." IEEE Internet Computing 14, no. 1 (2009): 44-51.

Mahapatra, B., Patnaik, S., & Nayyar, A. (2019). Effect of Multiple-Agent Deployment in MANET. Recent Patents on Computer Science, 12(3), 180-190.

Nayyar, A. (2019). Handbook of Cloud Computing: Basic to Advance research on the concepts and design of Cloud Computing. BPB Publications.

Palattella, Maria Rita, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. "Internet of things in the 5G era: Enablers, architecture, and business models." IEEE Journal on Selected Areas in Communications 34, no. 3 (2016): 510-527.

Q. Zhang and D. P. Agrawal. Dynamic probabilistic broadcasting in mobile ad hoc networks. In Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, volume 5, pages 2860–2864 Vol.5, Oct 2003.

Rahmati, Ahmad, and Lin Zhong. "Context-based network estimation for energy-efficient ubiquitous wireless connectivity." IEEE Transactions on Mobile Computing 10, no. 1 (2010): 54-66.

Rathee, D., Ahuja, K., & Nayyar, A. (2019). Sustainable future IoT services with touch-enabled handheld devices. Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions, 131.

Singh, P., Gupta, P., Jyoti, K., & Nayyar, A. (2019). Research on auto-scaling of web applications in cloud: survey, trends and future directions. Scalable Computing: Practice and Experience, 20(2), 399-432.

Singh, S. P., Nayyar, A., Kumar, R., & Sharma, A. (2019). Fog computing: from architecture to edge computing and big data processing. The Journal of Supercomputing, 75(4), 2070-2105.

Solanki, A., & Nayyar, A. (2019). Green internet of things (G-IoT): ICT technologies, principles, applications, projects, and challenges. In Handbook of Research on Big Data and the IoT (pp. 379-405). IGI Global.

Statista Report, (2020), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

T. Alam "Design a blockchain-based middleware layer in the Internet of Things Architecture," JOIV : International Journal on Informatics Visualization, vol. 4, no. 1, Feb. 2020. https://doi.org/10.30630/joiv.4.1.334

Tanweer Alam and Mohammed Aljohani, “Decision Support System for Real-Time People Counting in a Crowded Environment”, International Journal of Electronics and Information Engineering, Vol. 12(1), 2020.

Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111.

Tanweer Alam, “5G-Enabled Tactile Internet for smart cities: vision, recent developments, and challenges”, JURNAL INFORMATIKA, Vol. 13, No 2, July 2019, pp. 1-10, DOI: 10.26555/jifo.v13i2.a13426

Tanweer Alam, “A Middleware Framework between Mobility and IoT Using IEEE 802.15.4e Sensor Networks”, Jurnal Online Informatika, Vol 4, No 2 (2019). DOI: https://doi.org/10.15575/join.v4i2.487

Tanweer Alam, “Blockchain and its Role in the Internet of Things (IoT)”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 5(1), pp. 151-157, 2019. DOI: https://doi.org/10.32628/CSEIT195137

Tanweer Alam, “Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT integrated Framework”, Journal of Telecommunication, Electronic and Computer Engineering (JTEC), Vol. 12 No. 1, 2020.

Tanweer Alam, “Internet of Things: A Secure Cloud-Based MANET Mobility Model”, International Journal of Network Security, Vol. 22(3), 2020.

Tanweer Alam, “IoT-Fog: A Communication Framework using Blockchain in the Internet of Things”, International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-6, 2019.

Tanweer Alam, “Middleware implementation in MANET of Android Devices”, International Journal of Electronics and Information Engineering, Vol. 12(2), 2020.

Tanweer Alam, Baha Rababah, "Convergence of MANET in Communication among Smart Devices in IoT", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.9, No.2, pp. 1-10, 2019. DOI: 10.5815/ijwmt.2019.02.01

Tanweer Alam, Yazeed Mohammed Alharbi, Firas Adel Abusallama, Ahmad Osama Hakeem, “Smart Campus Mobile Application Toward the Development of Smart Cities”, International Journal of Applied Sciences and Smart Technologies, Vol. 2 (1), 2020.

Welbourne, Evan, Leilani Battle, Garret Cole, Kayla Gould, Kyle Rector, Samuel Raymer, Magdalena Balazinska, and Gaetano Borriello. "Building the internet of things using RFID: the RFID ecosystem experience." IEEE Internet computing 13, no. 3 (2009): 48-55.