Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework

Tanweer Alam

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

Abstract— The Internet of Things (IoT) devices have the capabilities to interact and communicate in 5G heterogeneous networks. They also have the capabilities to form a network with neighborhood devices without a centralized approach. This network is called the mobile ad hoc network (MANET). Through an infrastructure-less system of the Internet of Things environment, the MANET enables IoT nodes to interact with one another. Those IoT nodes could interactively connect, communicate as well as share knowledge between several nodes. The role of cloud throughout this structure is to store as well as interpret information through IoT nodes. The communication security has been introduced as one of the techniques to solve the data transmission security issue that could result in increased performance in cloud consumption and ubiquity. The purpose of this research is to establish a communication system among IoT nodes in an embedded Cloud and MANET structure. Aiming to create an efficient and secure approach for communication in Cloud-MANET-IoT integrated framework, this approach has been implemented and tested.

Index Terms—Cloud Computing; Internet of Things; Mobile Ad-Hoc Networks (MANET); Smart Devices; Wireless Communication.

I. INTRODUCTION

The IoT connected devices are devices that collaborate and communicate with each other or with other machine. They are expected to increase significantly to approximately 22 billion by 2025 [1]. As shown in Figure 1, the number of IoT connected devices are continuously increasing between 2015 and 2025, although the whole production of IoT devices would not hinge onto the populous of humanity. Although its popularity is increasingly exponentially, one of the most exhaustive issues these devices face is the surveillance and the monitoring of portable devices [2]. The concept of the internet of things could be defined as "an omnipotent as well as an ubiquitous structure, which further enables monitoring control of a physical planet through gathering, processing, as well evaluating data received from sensors". The IoT framework allows its subscribers to detonate an association to something like a network of computing resources in such a seamless fashion, in which subscribers could rapidly measure high or low requirements to insignificant communication from the supplier. Recently, mobile-based technology has been so popular as the number of connected devices has been rising exponentially day by day [3]. The connected devices are capable of transmitting information to any and all connected devices throughout the network [4]. Figure 2 shows the Cloud-MANET-IoT framework.
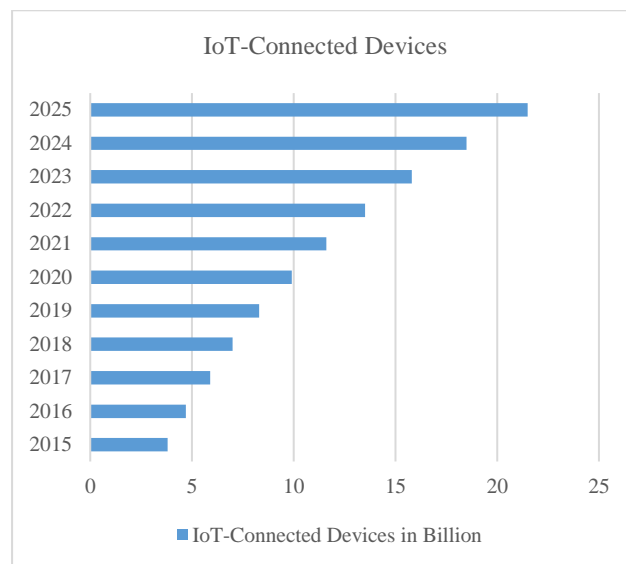

Figure 1: IoT device statistics between 2015-2025 [1]

Whenever a wireless device does not have adequate information, it communicates the query to its nearby devices. Communication networks protection is the most essential part, which is predicated on cryptography and encryption keys and provides security in intelligent interaction of ad-hoc networks [5]. Connected devices contribute to strengths, such as the context awareness, enhanced processing capabilities, and autonomy from power sources. In 2008, the development of the IoT begin by communicating physical things to the World Wide Web [6]. The sensory elements were linked to something like an intelligent repository with a bundle of intelligent data. The structure seems to have the image processing innovation for business as well as consumer verification of both the physical things, buildings, persons, sources, destinations, etc. Then, the IoT shifted from data-based technology to operable-based technology, i.e. IPv4 (man to machine) to IPv6 (machine to machine) [7]. It integrates detectors, connected devices as well as modules like Smart Grid. The growing numbers of detectors and sensor networks are connected to the World Wide Web. Machine-to-machine (M2M) interaction has been the main innovation to sustain sensor data transfer [8]. There are many techniques for transforming integrated M2M interaction paradigms into the proposed systems. In such a broader context, each of the prior end-users will have their issues about weaknesses in cloud services and obstacles that could deter them from accomplishing the goals. The following are the components of IoT: i) Identifiers (ii) Detectors (iii) Surveillance (iv) Calculations (v) Utilities (vi) Terminology, etc.
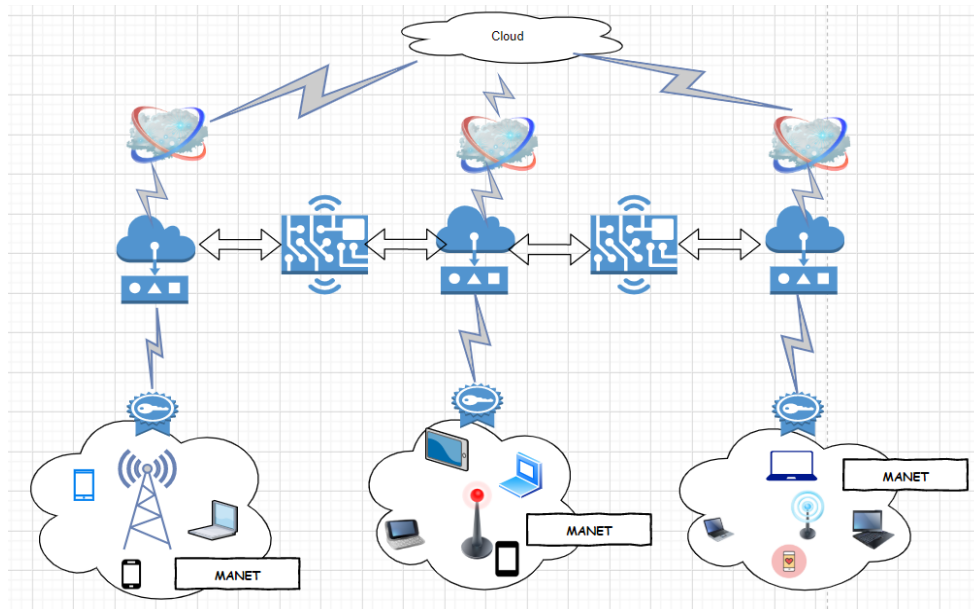
Figure 2: Cloud-MANET-IoT framework

There are three techniques that have contributed to the development of Cloud-MANET-IoT system. The ubiquitous computation is capable for smart physical things to perform the data transmission among physical devices. The IPv6 is utilizing pervasive computations that cover the area of proposed architecture as well as supporting machine-to-machine talking. IPv4 internet have a disadvantage that adds billions of smart appliances around each other; However, it is feasible in IPv6 internet as it enables the IoT to wirelessly connect billions of smart devices around the world [9]. Association in omnipresent computations used the specified mobility using sensor interconnection. Such techniques must be frequently improved to allow the advancement of smart devices internet including multi-sensor structures to store, calculate, evaluate and own mechanism abilities with smaller size or lower power consumptions [10].

The rest of the paper is organized as follows. Section II represents the related works, Section III represents the methodologies, Section IV represents the data transmission approach in Cloud-MANET-IoT framework, Section V shows the results and discussions and Section VI shows the conclusion.

II. RELATED WORKS

A decentralized based infrastructure is referred to as MANET. The IoT devices form MANET with nearby devices. The MANET is a set of many endpoints that transmit the information, which uses a peer-to-peer mechanism. Therefore, a specifically assigned device is independent of any existing framework, such as wireless devices as well as wireless networks. Although the self-created network is usually helpful to create MANET, the MANET connected with the Internet is significantly more attractive. The Internet is considered as the key part of the daily life of many people by providing an extensive scope of administration. Access points are being used to integrate the MANET and the connected outer spaces.

In the article [11], the authors discuss ways to minimize the limitations connected to IoT deployment and implementation in a smart city environment using a multi mediator scheme. Also, they developed the data transmission scheme in the

Vehicular Ad-Hoc Networks (VANET) for the traffic congestion in the smart cities [11].

In article [12], the authors proposed an efficient energy-aware routing scheme for cloud-based MANET in the 5G network. They obtained positive results and demonstrated better performance in terms of less energy consumption compared to previous studies [12].

In article [13], the authors proposed an approach to secure communication in mobile ad-hoc networks of Android devices. In this approach, they developed an algorithm for secure communication in the MANET of smart devices [13].

In article [14], the authors provided the solution of the data transfer securely among the smart devices and IoT based cloud services.

In article [15], the author described the roles of the Cloud-MANET framework in the Internet of Things. They developed an algorithm for secure communication among smart devices. They also compared the previous approaches and obtained positive results [15].

III. METHODOLOGIES

The research contribution ties a special wireless communication approach that uses cloud computing and MANET techniques in the internet of things. The following are the key challenges of the centralized system so that the proposed research is highly needed.
1. It is not simple to set up data from billions of detectors in such a centrally controlled structure of smart devices.
2. Handling computing resources in a wide network that can retrieve environmental data from either the centrally controlled structure is not easy.
3. It is very difficult to control detectors operating the same kind of information similarity and stored in the centrally controlled structure.

Nowadays, smart devices are becoming the requirements of our daily life. These devices could connect with each other. The time is not far away whereas in real-time millions of physical objects will relate to each other [16]. They will interact or send data as well as process their required information onto the cloud [17]. However, there seems to be

a lack of a scientific standardized security point of view on the architecture of IoT. Cloud computing has indeed been regarded as one of the most famous computing concepts. This also resulted from innovations in previous computing frameworks that integrate simultaneous computation, grid computation, distributed computation, and other computing frameworks [18]. Cloud computing offers its consumers with three important features of administration: SaaS, PaaS as well as IaaS. Software as a service (SaaS) is specifically intended for consumers that must use the software as part of their routine practices [19]. Platform as a Service (PaaS) is specifically intended for software developers that need technologies to establish their software or methodology. Infrastructure as a service (IaaS) is specifically intended for network designers that need development abilities, interaction, protection difficulties and cyberattacks to smart devices [20]. The author has identified some security issues or attacks in this article. The first threat is the interruption of action due to attacks [21]. Recently, existing attacks in a distributed system could be made accountable for serious security violations. The second challenge would be to reject provider threats. This is given as distinctive, numerous or easy attacks. A challenge occurs if it arrives in differentiating in both the unlawful packet as well as the legal packet [22].

Clearly, such attacks must provide moment cooperation, in which unexperienced cybercriminals could cause them because they only operate easy codes and techniques [23]. As just a matter of fact, packets can pass by the selected providers. Its restraint of these attacks could be attempted via emerging technologies. Any of these innovations seem to be the protection system for the intrusion [24].

The cloud-MANET-IoT layered structure (Figure 3) is a novel methodology in the connected device interaction throughout the Internet of Things that realizes as well as integrates neighboring devices without any centrally controlled technology. The current mobile network would not enable all smart devices to also be linked without centrally controlled technology even though they are very near to one another [25].

The suggested methodology would be very helpful in M2M networks because there are many machines close to one another in the M2M network. Developing the MANET framework integrated with IoT and Cloud could be very effective and beneficial for saving energy and speed performance. Cloud-based services in MANET designed for user-to-device connectivity might be a very valid solution to optimizing the strengths of the smart devices [26]. Consumers of devices will be using cloud storage services to explore devices, reduce valuable information in big data, and that can process videos, pictures, messages, and recordings [27]. Throughout this paper, the author is suggested a new structure to improve the ability of smart devices on the internet for MANET and cloud computing which could be helpful throughout the highly diverse 5G service.

The following procedure is used to connect a device with the Cloud-MANET-IoT framework.
   i. Register the IoT node in the clouds. The cloud server will generate the node id as well as login details.
   ii. Enter the node id and login details in the clouds.
   iii. Install the configuration file on the new connected device.
   iv. Start the MANET service on the IoT nodes using this file.
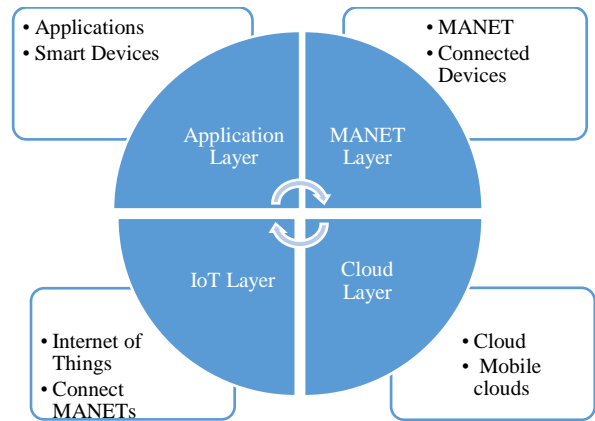

Figure 3: Cloud-MANET-IoT layers

This file is now connected with the mobile application.
   v. MANET has started.
   vi. Discover the neighborhood IoT devices within the MANET area as well as discover by device id.
   vii. Connection established.
   viii. Able to Communicate.

IV. DATA TRANSMISSION APPROACH IN CLOUD-MANET-IoT INTEGRATED FRAMEWORK

The Cloud-MANET-IoT structure is an integrated model of Cloud computing and MANET technologies in the internet of things. The MANET's capability varies depending on the mobility of its clusters as well as on the communication of resources like storage and power efficiency. Cloud services operators maintain communications infrastructure, warehouses, as well as mobile applications that sustain versatility, effectiveness, as well as usability. The following algorithm is used to compute the IoT node velocity in the Cloud-MANET-IoT framework.

Input: Total number of IoT nodes, transmission function value (t).
Output: Velocity of IoT node.
Initialization: Count=0, Velocity=0.
Step 1: Discover all IoT nodes in each direction of the selected IoT node.
Step 2: Find a Communication session using the formula.
Step 3: Calculate speed and directions.
Step 4: Calculate transmission function value (t).
Step 5: Find entropy per symbol.
Step 6: Find Transmission in bits/sec.
Step 7: Find velocity (V) in m/s.
Step 8: Counter=Counter+1;
if counter! = Number of devices then go to step 2 otherwise stop.

MANET mobile devices could interact with one another in the Cloud-MANET-IoT framework, but at least one smart device should be tied to wireless or Wi-Fi networks. All MANET smart devices will be independently enrolled in the cloud. The proposed system would be accessed in the disjointed style. Whenever a MANET is detected, cloud providers would trigger in real-time as well as provide services to MANET's devices. The smart devices submit a report to the cloud for a communication session. Cloud offers better interaction with smart devices. Communication life is defined as a mathematical function in equation (1) as follows.

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

The integral expression would be 0 whether the limit tends to be as high as 0. Since computation session life using the above deterministic function, every device involves computational the values of π and μ. Such two variables are connected to the link established between MANETs and cloud service which could be calculated and used the preceding function via connected devices, $e^{\mu(1/2)\sigma^2}$.

Whenever a smart device estimates the communication life among MANET and Cloud, this will efficiently transfer or receive information. A link would be triggered and there is high stabilization. They considered that when generating a cloud session, every smart device is guaranteed of creating the path around MANET and cloud. Using the Gauss-Markov utility system, the electronic devices could start moving from one area to the next area via the velocity of 20 meters per second. The next equations (2) and (3) can be used to measure the move of the smart device velocity inside the MANET scope.

$$\text{Speed(t)}=\delta Speed_{t-1} + (1-\delta)\overline{Speed} + \sqrt{(1-\delta^2)}\,Speed_{t-1}^G \tag{2}$$

$$\text{Direction(t)}=\delta Direction(t-1) + (1-\delta)\overline{Direction} + \sqrt{(1-\delta^2)Direction_{t-1}^G} \tag{3}$$

The δ is a random degree if computational velocity and the trajectory of the smart device in such a period (t). During the time interval [t_i, t_{i-1}], the transmission (t_k) of data (I_k) between the number of smart devices could be calculated. Within the MANET, the smart devices could start moving as well as connect directly the cloud storage service using the multifaceted function (*t*) in equation (4).

$$t = CS_n \times t_k \times I_k \tag{4}$$

where: k = 0,1,2,3.......∞ (+*ve*)

When electronic devices start moving outside of the MANET, after which k will be a negative number. Here, they recognize that somehow the transition of data takes place concurrently. We understand that the probability becomes proportional to the inverse data, $P_k \propto \frac{1}{I_k}$.

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

$$P_k(S_n \mid \varepsilon_k, I_k, t_k) = 1 - \int_{-\infty}^{\infty} M_q\left(\sqrt{\left(\frac{2\delta^2}{1-\delta^2}\right)}.\frac{S_n}{t_k}, \sqrt{\frac{S_n}{1-\delta^2}}.2\delta\right) \tag{5}$$

where: $\delta = 1$

So, we have divided the probability density function of all associations that used the entropy per symbol for all smart devices of 3-dimensional locations.

$$H_{\alpha,\delta,\epsilon} = \sum_{x=0}^{\infty}\sum_{y=0}^{\infty}\sum_{z=0}^{\infty}\left[P_{x_k}.P_{y_k}.P_{z_k}\log_3\frac{1}{P_{x_k}}.\frac{1}{P_{y_k}}.\frac{1}{P_{z_k}}\right]\alpha_{\beta^{-1}}.\varepsilon_2\left(\frac{\delta}{\alpha}, S_k, \gamma\right) \tag{6}$$

Here $\varepsilon_2(\frac{\delta}{\alpha}, S_k, \gamma)$ is the Chi-Square distribution method that is used for congruence. Now, we will measure all the probabilities, entropies for each direction as well as finally, create the transition matrix from the probabilities of all smart devices.
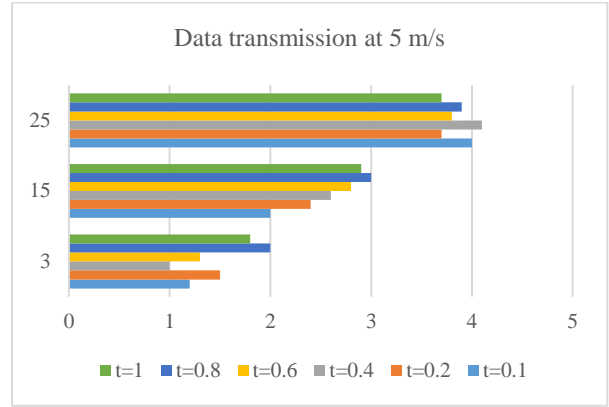

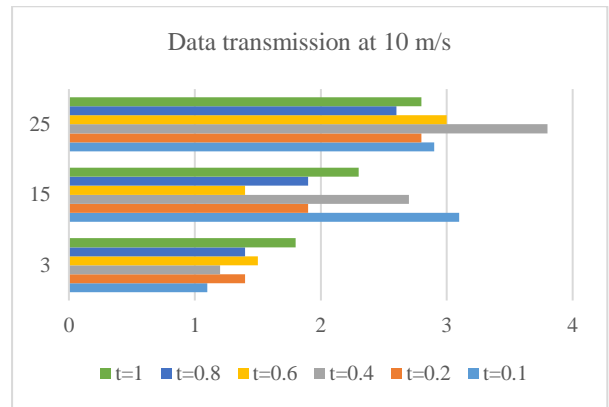Figure 4: Data transmission in Cloud-MANET at 5 m/s

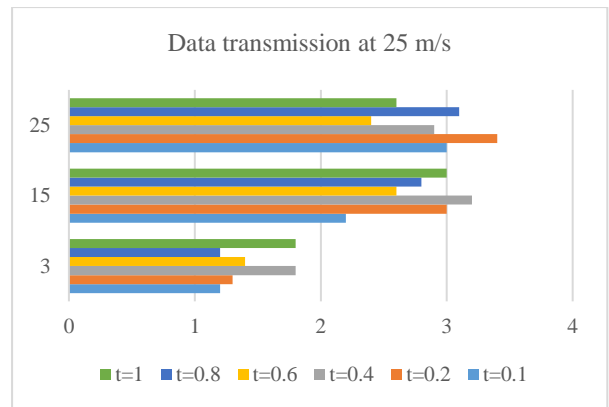Figure 5: Data transmission in Cloud-MANET at 10 m/s

Figure 6: Data transmission in Cloud-MANET at 25 m/s

Instead, we are going to calculate entropy per symbol line-wise said H_1, H_2, H_3 ......, H_K as per the transition matrix earlier calculated.

$$H=H_1.P_1 + H_2.P_2 + H_3.P_3 + ...H_K.P_K. \tag{7}$$

The authors have calculated the throughput of devices utilizing in the proposed model that used 5, 15 and 25 devices at 5 m/s, 10 m/s, and 25 m/s (Figure 4, 5 and 6). The data is gathered in Table 1, 2, and 3 at the time of testing.

The proposed framework was implemented in three ways. Firstly, all the connected devices were discovered throughout the self-created MANET network. Secondly, IoT devices communicate to the cloud and the thirdly, the IoT devices communicate with MANET devices, including the sessions and transmit data from one IoT device to the next that utilize cloud as a provider.

Table 1
Transmission in MANET of Smart Devices at 5 m/s

Devices	t=0.1	t=0.2	t=0.4	t=0.6	t=0.8	t=1
3	1.2	1.5	1	1.3	2	1.8
15	2	2.4	2.6	2.8	3	2.9
25	4	3.7	4.1	3.8	3.9	3.7

Table 2
Transmission in MANET of Smart Devices at 10 m/s

Devices	t=0.1	t=0.2	t=0.4	t=0.6	t=0.8	t=1
3	1.1	1.4	1.2	1.5	1.4	1.8
15	3.1	1.9	2.7	1.4	1.9	2.3
25	2.9	2.8	3.8	3	2.6	2.8

Table 3
Transmission in MANET of Smart Devices at 25 m/s

Devices	t=0.1	t=0.2	t=0.4	t=0.6	t=0.8	t=1
3	1.2	1.3	1.8	1.4	1.2	1.8
15	2.2	3	3.2	2.6	2.8	3
25	3	3.4	2.9	2.4	3.1	2.6

We tested the above approach on a different number of IoT smart devices. The methodology was operated on numerous MANETs and utilized the cloud as a provider. The study was performed using the smart device with the suggested formulation of the calculation as well as other existing methodologies that had been built in the same setup systems. The researchers realize that somehow the output of the proposed approach had been stronger than any of the other approaches.

V. RESULT AND DISCUSSION

For secure data transmission among IoT, nodes have been introduced in this research using a framework named Cloud-MANET-IoT. Two mobile apps, one for smart device communication and another for the administrator to monitor and control have been developed. Next, the framework was tested using these mobile apps on three Android devices. Two of them were supported by the 4G network and one was supported by 3G networks. Amazon Web Services (AWS has been used to execute the cloud services. The whole cloud service communicated to the MANETs and the applications were deployed on every device. The device was also enrolled on the cloud since the mobile applications were set up on the devices. The cloud would produce a device Id for each, and every device was approved in the cloud. Using cloud-based services, the devices were able to interact with some other devices within the area of the same MANET or any other MANET. Mobile apps would configure a smart IoT device.

When the smart IoT smart node starts, it was automatically connected to Amazon's cloud service and started to connect with another IoT node. The Amazon cloud produced database schema utilities to store information regarding devices, queries, communicated texts, and information about devices in the neighborhood.

VI. CONCLUSION

The Cloud-MANET-IoT framework has the ability to play an important role in diverse 5G communication. The framework have been developed to enhance interaction efficiency. It was found that the cloud framework was predicated on such a diversified structure, many precautions or security risks linked to disbursed concepts are acquired. Data transmission security issues or obstacles which depend on behind cloud computing were enticed. Moreover, many of these excessive risks has strengthened in most of the cloud framework. The security requirements as well as communication security problems between all connected devices throughout the cloud services were also analysed. The proposed framework has been constructed, implemented and tested.

REFERENCES

[1] Lueth, Knud Lasse. "State of the IoT 2018: Number of IoT devices now at 7B–Market accelerating." IoT Analytics (2018)

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] Saleem, Muhammad Asim, Zhou Shijie, and Abida Sharif. "Data transmission using IoT in vehicular ad-hoc networks in smart city congestion." Mobile Networks and Applications 24, no. 1 (2019): 248-258. DOI: https://doi.org/10.1007/s11036-018-1205-x

[12] Riasudheen, H., K. Selvamani, Saswati Mukherjee, and I. R. Divyasree. "An efficient energy-aware routing scheme for cloud-assisted MANETs in 5G." Ad Hoc Networks 97 (2020): 102021. DOI: https://doi.org/10.1016/j.adhoc.2019.102021

[13] 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

[14] Stepień, Krzysztof, Aneta Poniszewska-Marańda, and Witold Marańda. "Securing Connection and Data Transfer Between Devices and IoT Cloud Service." In Integrating Research and Practice in Software Engineering, pp. 83-96. Springer, Cham, 2020. DOI: https://doi.org/10.1007/978-3-030-26574-8_7

[15] 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

[16] 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

[17] 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

[18] 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)

[19] Alam, Tanweer, Parveen Kumar, and Prabhakar Singh. "Searching Mobile Nodes Using Modified Column Mobility Model", International Journal of Computer Science and Mobile Computing, (2014)

[20] 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

[21] Singh, Parbhakar, Parveen Kumar, and Tanweer Alam. "Generating Different Mobility Scenarios in Ad Hoc Networks.", International Journal of Electronics Communication and Computer Technology, 4(2), 2014

[22] Sharma, Abhilash, Tanweer Alam, and Dimpi Srivastava. "Ad Hoc Network Architecture Based on Mobile Ipv6 Development." Advances in Computer Vision and Information Technology (2008): 224

[23] 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

[24] M. Aljohani and T. Alam, "Design an M-learning framework for smart learning in ad hoc network of Android devices," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1- 5. DOI: https://doi.org/10.1109/ICCIC.2015.7435817

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

[26] 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

[27] Tanweer Alam, Abdulrahman A. Salem, Ahmad O. Alsharif, Abdulaziz M. Alhujaili, "Smart home automation towards the development of smart cities", APTIKOM Journal on Computer Science and Information Technologies, Vol 5, No 1, 2020. DOI: https://doi.org/10.11591/APTIKOM.J.CSIT.153.