CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices

https://doi.org/10.3991/ijim.v12i6.6776

Tanweer Alam(✉), Mohamed Benaida
Islamic University of Madinah, Saudi Arabia
tanweer03@iu.edu.sa

Abstract—The internet of smart devices is a network of intelligent gadgets with sensors, programs, Wi-Fi and communication network connections. These devices store the data in cloud and process data outside the device using the proposed Cloud-Internet communication framework. These devices can communicate with other devices using the proposed framework. However, there are many challenges for communication security among the internet of smart devices. The Cloud can store the device data with security, reliability, privacy and service availability. The communication Security has been raised as one of the most critical issues of cloud computing where resolving such an issue would result in a constant growth in the use and popularity of cloud computing. Our purpose of this study is to create a framework for providing the communication security among smart devices network for the internet of things using cloud computing. Our main contribution links a new study for providing communication security for the internet of smart devices using the cloud-Internet framework. This study can be helpful for communication security problem in the framework of the Internet of Things. The proposed study generates a new framework for solving the issue of communication security among internet of smart devices.

Keywords—Internet of Things, Cloud Computing, Communication Security, Smart Devices, Wireless Communications.

1 Introduction

The Internet of things (IoT) is growing exponentially in the area of telecommunication. It is expected that by 2020, the development of the internet of smart devices connected together exponentially with 50 billion smart devices [1]. This development will not depend on mankind's population, but the reality that the units we utilize consistently [2]. The reality of interconnected things is cooperating man to machines and machine to another machine. They will be talking with each other. However, monitoring and tracking of the movable device are one of the most comprehensive issues [3]. 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. According to the study in the last few years, the smart device technologies are becoming popular. It is exploring very fast [4]. The smart devices are able to transmit data in a wireless network to all active devices [5]. If a smart device doesn't have full information for transferring the requests then it can connect the neighbor devices and forward that request to the neighbor device. The communications security is the most important aspect that is based on encryption and decryption key technology to provide secure data communication among smart devices. The smart devices have functionalities such as context-aware computing, computational powers and energy-source independence [6]. The growth of the internet of things initially started in 2008 by connecting the physical objects to the internet. The physical objects are connected with a smart database that has a collection of smart data [7]. The framework has the image recognition technology for identifying the physical object, buildings, people, 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 to machines) to IPV6 (machine to machines). It combines sensors, smart devices and interfaces like Smart Grid. The M2M communications are the novel methodology for transferring information among sensors-based devices [8]. The various tools are available for M2M communication among devices [9]. In a wider respect, each of the previous consumers has their concerns over cloud computing vulnerabilities and challenges which might prevent them from their objectives [10, 11].

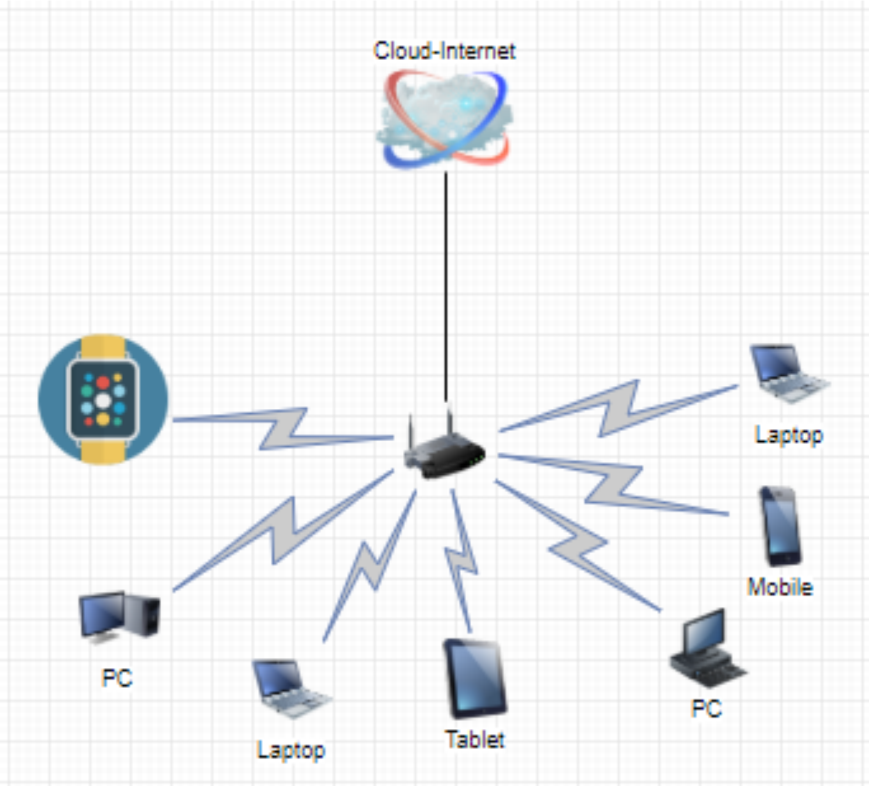

Fig. 1. Internet of Smart Devices

The objective of this study is to create a framework for providing the communication security among smart devices network for the internet of things using cloud computing. Our main contribution links a new study for providing communication security for the internet of smart devices using cloud and internet framework. This study can be helpful for communication security problem in the framework of the Internet of Things. Our study will generate a new framework for solving the issue of communication security among internet of smart devices.

This paper is organized into the sections. Section 1 is the Introduction, Section 2 is the literature Survey, Section 3 is "Technologies contributed to the growth of the Internet of smart devices", section 4 is "Communication Security Challenges and Threats", section 5 is "Cloud-Internet Communication Security Framework" and the last section is the conclusion.

2 Literature Survey

In 1994, Tristan Richardson et.al. were presented an article on X windows systems, X protocol for securing the communication between client and server [12]. In the article [13], the authors represented System Software for Ubiquitous Computing for the integration of different kinds of network, also create a connection among the devices in different types of network. In 2002 D. Estrin et.al. were published an article on connecting the Physical World with Pervasive Networks, in this article they address the communication in physical world using embedded technologies [14].

The cloud computing came as a consequence of continues development of computing paradigms [15]. In 2009, Evan Welbourne et al. were published an article on RFID-based services for the IoT [16]. In 2010, Gerd Kortuem et al. were presented the development of a new flow-based programming paradigm for smart objects and the Internet of Things [17]. In 2011, Ahmed Rahmati et al. were published an article on the context-based network estimation and provide ubiquitous energy efficient wireless connectivity [18]. In the article [19] researchers presented Wi-Fi based sensors for the internet of things, they focused on measurement the range performance.

In May 2014, Lihong Jiang et al published an article on data storage in IoT and integration of both structured and unstructured data [20]. In the article [21], introduced the IoT ecosystem and key technologies to support IoT communications. In 2016, Maria Rita Palattella et al 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 [22].

3 Technologies contributed to the growth of the Internet of smart devices

There are three technologies that contributed to the internet of things growths.

i) The ubiquitous computation that has the capacity of intelligent physical objects that execute on the computation framework.

ii) Internet Protocol (IPV6) using ubiquitous computing that covers the area of network and support talking of machine to machine [23]. IPv4 internet has a drawback to adding billions of smart gadgets together, but it is possible in IPv6 internet because it enables internet of things to connect billions of smart gadgets together securely.
iii) Connection using ubiquitous computing that uses the fixed cell network or mobility with using sensor connectivity [24].

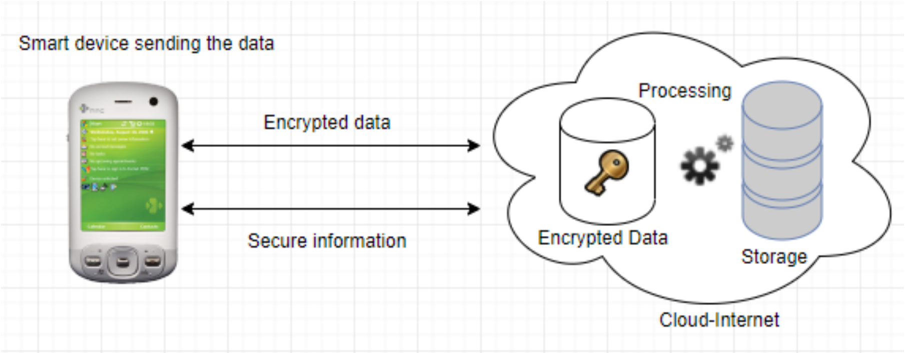

Fig. 2. Idea behind the proposed framework

These technologies must be enhanced and progressive so that it allows the progress of internet of smart devices including multi-sensor framework to store, computation, analyze and process capability with smaller in size and lowest energies required [25]. The main contribution of this article is solely on the communication security viewpoint among smart gadgets in the area of the internet of things. The security idea depends on three main points in the designing of the internet of things architecture.

1. It is not easy to manage data getting from millions of sensors in a centralized framework of smart devices collection.
2. It is not easy to manage and schedule network resources [26] in a large network that can collect environment information from the centralized framework.
3. It is very hard to manage sensors that execute the same kind of data parallel and store on the centralized framework.

Most researcher move to the growth of internet of things using the advancement of wireless sensor technology with satellites, mobility, gadgets industrialize, computation and storage in cloud etc. [27,28,29] this technology provide the opportunities for reducing the operation cost and people physical work [30,31]. The distribution of intelligent capacity is called fog computation. Fog computation is an architecture that is designed for processing the information by smart devices to the centralized cloud system. Computation, storage, and networking resources are the building blocks of both the Cloud and the Fog computing [32]. Cloud computing has been regarded as one of the most popularized computing paradigms [33]. It came likewise an outcome for developments done past computing paradigms which incorporate parallel computing, grid computing, disseminated computing also other computing paradigms [34,35,36]. Cloud computing gives its customers three essential administration models: SaaS, PaaS, and IaaS [38]. Software as a service (SaaS) is the service that is mainly intended to end users who need to use the software as a part of their daily activities [39]. 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 [40]. Nowadays increasing numbers of sensors and sensor networks are being connected to the Internet and the World Wide Web [41].

4 Communication Security Challenges And Threats

The communication security challenges and threats for communicating in cloud perspective internet of smart devices are the most important aspect. 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. This can be illustrated in the case of Adobe systems, where it cooperates databases were hacked and data was stolen. It was reported that around 130 million consumer records got leaked. Therefore, the cloud provider must step up preventive measures to diminish the severity of these attacks. The second challenge is Denial of service attacks. It is provisioned as unique, frequent and simple attacks. Their characteristics make them unpredictable and difficult to be intercepted.

5 Cloud-Internet Communication Security Framework

For the most part speaking, security will be a limitless issue to take care of viewpoint about perspective. Different gatherings included inside the cloud standard bring different destinations. Therefore, they might differ their worries in regard to threats and vulnerabilities in the cloud environment. Moreover, these worries might be eased or intensified depending on the implemented deployment model. In the realism of the internet, security has been perceived as a prominent inhibitor of embracing the cloud paradigm. Since the cloud environment is a distributed architecture, which its resource storage and management may lay in any 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 perspective and objective. It has been determined that there are three dominant parties which participate in the cloud environment.

- Service providers: Their concerns may intensify over public and hybrid cloud where issues related to unauthorized access and cyber-attacks may jeopardize the service availability.
- Service consumers: Their concerns may focus on issues related to data privacy and quality of service. Besides, their concerns regard service availability and interoperability.
- Service regulators: Their concerns may focus on issues related to service.

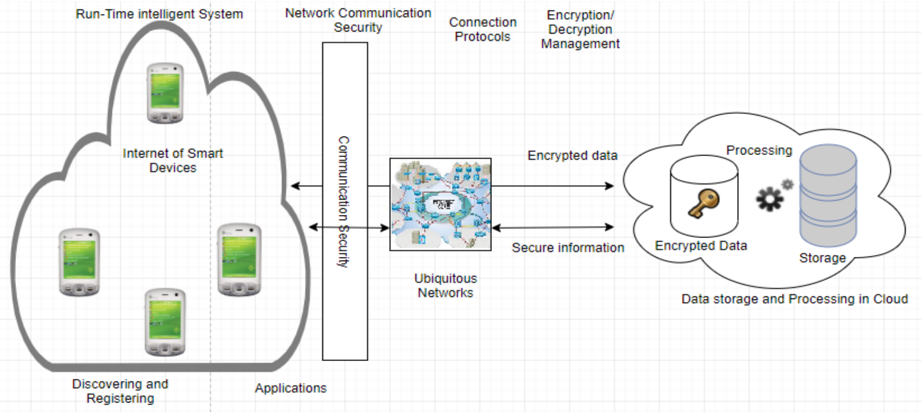
Run-Time intelligent System
Network Communication Security
Connection Protocols
Encryption/ Decryption Management
Internet of Smart Devices
Communication Security
Encrypted data
Processing
Encrypted Data
Storage
Secure information
Ubiquitous Networks
Data storage and Processing in Cloud
Discovering and Registering
Applications

Fig. 3. Cloud-Internet Communication security Framework

Standard violations. Thus issues related to interoperability would affect them greatly. It is fair to say that all previously mentioned party concerns might be correlated and associated with other parties.

In cloud computing, several deployment models can be deployed on the previously mentioned service models. These various deployment models can be utilized based on their distribution nature which depends on cloud service location as follows:

i) Public cloud: All services are been provided in a public environment where consumers can access a pool of resources which are managed by a hosted organization. Due to its nature, this type of environment may raise critical concerns over security problems.
ii) Private cloud: Services are been provided by a third party vendor which separates it from public access. Consequently, it is safer than the previous development model due to the fact that it prevents unauthorized access.
iii) Community cloud: Services are been provided to a specified community where all members have an equal right of accessing the shared resources.
iv) Hybrid cloud: Services are provided as combustion of more than one cloud (public cloud, private cloud, and community cloud). It could inherit any type of vulnerability or risk that resides within the previously mentioned parties.

There are various initiatives which try to establish standardization projects. Broadly speaking, these projects primarily empathized on standardizing four prominent cloud interoperability use cases which are the following:

i) User authentication: it can be standardized according to OpenID or protocols depend on Oath.
ii) Workload migration: it can be standardized based on VM image file formats.
iii) Data migration: it can be standardized by addressing APIs differences.
iv) Workload management: it can be standardized by unifying workload management standards across various providers.

The proposed framework has four layers, the first is the presentation layer acts on the smart device side. The second layer is the communication security layer that provides communication security in the network using encryption/decryption management. The third layer is the ubiquitous network layer. The fourth layer is the Cloud layer. This layer is the key layer in this framework. The cloud collects the encrypted data, process data, and store in the cloud. The information can be sent to the smart device in encrypted form.

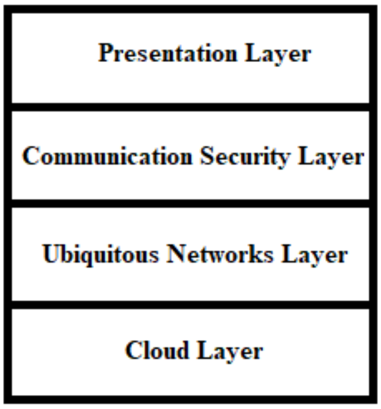

Fig. 4. Layers in the proposed framework

The proposed framework shows the framework elements with their functionality. This is a complex architecture. So that it is divided into several parts in each layer. The communication security layer is responsible to collect and aggregate data with encryption techniques also identify, classify, filter and process the data packets and send to the ubiquitous network. The packets are securely transferred to the cloud. The cloud received the light weighted packets in an encrypted format. It processes the packets and store in a cloud. This layer uses the programming with intelligence to process data packets received from the smart devices that are on the border of the coverage area. The communication security layer in the proposed framework applies the algorithm to monitor the attacks using deep learning or Petri Nets or artificial intelligence models. This layer also has the latest viruses or attacks information. It can be updated online automatically to adopt the new threat definitions.

6 Conclusion

The communication security threats and challenges that rely on behind the lure of cloud computing. Since the cloud paradigm is based on a distributed architecture, then it is inherited some risks and vulnerabilities that are related to distributed paradigms. However, several of these risks have intensified over the cloud paradigm. In this article, the issues related to the causes of information unavailability been discussed. To overcome it, a cloud provider and consumers should agree on the service level agreement.

While the causes of interoperability have been discussed. The article primarily focused on communication security, one of these threats related to service disruption which can result due to attacks such as denial of service attacks, service hijackings, and VM-level attacks. We analyzed the security requirements and challenges for communication security among all smart devices in cloud computing environment. The fundamental functions of this study have been introduced to the ubiquitous network layer. The study showed successfully and expectation for a future scope in this area. The proposed framework has been presented a layered architecture for secure communication among internet of smart devices. We explained the possible layers and techniques used in the framework.

7 References

[1] https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data

[2] Alam, T. & Aljohani, M., 2015. An approach to secure communication in mobile ad-hoc networks of Android devices. 2015 International Conference on Intelligent In-formatics and Biomedical Sciences (ICIIBMS). https://doi.org/10.1109/ICIIBMS.2015.7439466

[3] Alam, T. & Aljohani, M., 2015. Design and implementation of an Ad Hoc Network among Android smart devices. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). https://doi.org/10.1109/ICGCIoT.2015.7380671

[4] Aljohani, M. & Alam, T., 2015. An algorithm for accessing traffic database using wire-less technologies. 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). https://doi.org/10.1109/ICCIC.2015.7435818

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

[6] Perera, C., Zaslavsky, A., Christen, P. and Georgakopoulos, D., 2014. Context aware computing for the internet of things: A survey. IEEE communications surveys & tu-torials, 16(1), pp.414-454. https://doi.org/10.1109/SURV.2013.042313.00197

[7] Khan, M., Silva, B.N. and Han, K., 2017. A web of things-based emerging sensor net-work architecture for smart control systems. Sensors, 17(2), p.332. https://doi.org/10.3390/s17020332

[8] Bilal, M., 2017. A Review of Internet of Things Architecture, Technologies and Anal-ysis Smartphone-based Attacks Against 3D printers. arXiv preprint arXiv:1708.04560.

[9] Lien, S.Y., Chen, K.C. and Lin, Y., 2011. Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. IEEE Communications Maga-zine, 49(4).

[10] Evans, Dave. "The internet of things: How the next evolution of the internet is chang-ing everything." CISCO white paper 1.2011 (2011): 1-11.

[11] M. Hasan, E. Hossain, and D. Niyato. Random access for machine-to-machine com-munication in LTE-advanced networks: issues and approaches. IEEE Communica-tions Magazine, 51(6):86–93, June 2013. https://doi.org/10.1109/MCOM.2013.6525600

[12] Richardson, T., Bennett, F., Mapp, G. and Hopper, A., 1994. Teleporting in an X win-dow system environment. Olivetti Research Limited.

[13] Kindberg, T. and Fox, A., 2002. System software for ubiquitous computing. IEEE per-vasive computing, 1(1), pp.70-81. https://doi.org/10.1109/MPRV.2002.993146

[14] Estrin, D., Culler, D., Pister, K. and Sukhatme, G., 2002. Connecting the physical world with pervasive networks. IEEE pervasive computing, 1(1), pp.59-69. https://doi.org/10.1109/MPRV.2002.993145

[15] Sultan, N., 2010. Cloud computing for education: A new dawn?. International Jour-nal of Information Management, 30(2), pp.109-116. https://doi.org/10.1016/j.ijinfomgt.2009.09.004

[16] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M. and Borriello, G., 2009. Building the internet of things using RFID: the RFID ecosys-tem experience. IEEE Internet computing, 13(3). https://doi.org/10.1109/MIC.2009.52

[17] Kortuem, G., Kawsar, F., Sundramoorthy, V. and Fitton, D., 2010. Smart objects as building blocks for the internet of things. IEEE Internet Computing, 14(1), pp.44-51. https://doi.org/10.1109/MIC.2009.143

[18] Rahmati, A. and Zhong, L., 2011. Context-based network estimation for energy-efficient ubiquitous wireless connectivity. IEEE Transactions on Mobile Compu-ting, 10(1), pp.54-66. https://doi.org/10.1109/TMC.2010.139

[19] Swan, M., 2012. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor and Actuator Networks, 1(3), pp.217-253. https://doi.org/10.3390/jsan1030217

[20] 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 In-formatics, 10(2), pp.1443-1451. https://doi.org/10.1109/TII.2014.2306384

[21] Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. Computer networks, 54(15), pp.2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[22] Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. and Ladid, L., 2016. Internet of things in the 5G era: Enablers, architecture, and business mod-els. IEEE Journal on Selected Areas in Communications, 34(3), pp.510-527. https://doi.org/10.1109/JSAC.2016.2525418

[23] Bandyopadhyay, D. and Sen, J., 2011. Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), pp.49-69. https://doi.org/10.1007/s11277-011-0288-5

[24] Satyanarayanan, M., 2001. Pervasive computing: Vision and challenges. IEEE Per-sonal communications, 8(4), pp.10-17. https://doi.org/10.1109/98.943998

[25] Vermesan, O. and Friess, P. eds., 2013. Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.

[26] Santacana, E., Rackliffe, G., Tang, L. and Feng, X., 2010. Getting smart. IEEE Power and Energy Magazine, 8(2), pp.41-48. https://doi.org/10.1109/MPE.2009.935557

[27] Abdulhamid, S. M., Abd Latiff, M. S., & Ismaila, I. (2014). Tasks scheduling technique using league championship algorithm for makespan minimization in IAAS cloud. ARPN Journal of Engineering and Applied Sciences, 9(12), 2528 - 2533.

[28] Abdulhamid, S. I. M., Abd Latiff, M. S., Madni, S. H. H. and Abdullahi, M. (2016). Fault Tolerance Aware Scheduling Technique for Cloud Computing Environment Us-ing Dynamic Clustering Algorithm. Neural Computing and Applications. 1-15.

[29] Madni, S. H. H., Latiff, M. S. A., Coulibaly, Y. and Abdulhamid, S. I. M. (2016). Recent Advancements in Resource Allocation Techniques for Cloud Computing Environ-ment: A Systematic Review. Cluster Computing. 1-45.

[30] Abdulhamid, S. M., Latiff, M. S. A. and Bashir, M. B. (2014). On-Demand Grid Provisioning Using Cloud Infrastructures and Related Virtualization Tools: A Survey and Taxonomy. International Journal of Advanced Studies in Computer Science and En-gineering IJASCSE. 3(1), 49 - 59.

[31] Abdulhamid, S. M., Latiff, M. S. A., Abdul-saalam G. and Madni, S. H. H. (2016). Se-cure Scientific Applications Scheduling Technique for Cloud Computing Environ-ment Using Global League Championship Algorithm. PlosOne. DOI: 10.1371/journal.pone.0158102. https://doi.org/10.1371/journal.pone.0158102

[32] Madni, S. H. H., Latiff, M. S. A., Abdullahi, M., & Usman, M. J. (2017). Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing envi-ronment. PloS one, 12(5), e0176321 https://doi.org/10.1371/journal.pone.0176321

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

[34] Alam, T. & Aljohani, M., 2016. "Design a New Middleware for Communication in Ad Hoc Network of Android Smart Devices". Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strate-gies – ICTCS, 2016. http://dx.doi.org/10.1145/2905055.2905244. https://doi.org/10.1145/2905055.2905244

[35] Abhilash, Tanweer Alam, and Dimpi Srivastava. "Ad Hoc Network Architecture Based on Mobile IPV6 Development.", Advances in Computer Vision and Infor-mation Technology (2008): 224.

[36] Aljohani, M. & Alam, T., 2016. Real Time Face Detection in Ad Hoc Network of An-droid Smart Devices. Advances in Computational Intelligence, pp.245–255. https://doi.org/10.1007/978-981-10-2525-9_24

[37] Alam, Tanweer. (2017) "Fuzzy control based mobility framework for evaluating mo-bility models in MANET of smart devices", ARPN Journal of Engineering and Ap-plied Sciences. Vol 12(15), pp. 4526-4538

[38] Alam, T., Srivastava, A. P., Gupta, S., & Tiwari, R. G. (2010). "Scanning the Node Us-ing Modified Column Mobility Model.", Computer Vision and Information Technol-ogy: Advances and Applications, 455.

[39] Alam, T. & Sharma, B.K., 2010. "A New Optimistic Mobility Model for Mobile Ad Hoc Networks.", International Journal of Computer Applications, 8(3), pp.1–4. Available at: http://dx.doi.org/10.5120/1196-1687. https://doi.org/10.5120/1196-1687

[40] 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.

[41] Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engi-neering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111

8 Authors

Tanweer Alam is with the Department of computer science, Islamic University of Madinah since 2013. He is awarded by Ph.D. (Computer Science and Engineering), M.Phil. (Computer Science), MTech (Information Technology), MCA (Computer Applications) and M.Sc. (mathematics). His area of research including Mobile Ad Hoc Network (MANET), Smart Objects, Internet of Things, Cloud Computing and wireless networking. He is a single author of twelve books. He is the member of various associations such as International Association of Computer Science and Information Technology (IACSIT), International Association of Engineers, Internet Society (ISOC), Computer Science Teachers Association (CSTA), Indian Society of Technical Education (ISTE) etc. His Scopus Author Id is 57189067051 and Researcher Id is M-7780-2017.

Mohamed Benaida is an Assistant Professor in the Islamic University of Madinah faculty of computer science and information systems and received his Bachelor of Science in Computer Science and information systems at Salford University and a Masters in Computer Aided Product Development and Engineering Management, and he received his PhD in usability from Salford University (United Kingdom). His main area of research interest is Human Computer Interaction includes; Usability, language and web design and Internet of Things (e-mail: md.benaida@gmail.com).

Article submitted February 14, 2017. Resubmitted July 17, 2017. Final acceptance August 21, 2018. Final version published as submitted by the authors.