

# Internet of things: review, architecture and applications

Tanweer Alam

Faculty of Computer and Information Technology, Islamic University of Madinah, Medina, Saudi Arabia

---

## Article Info

### Article history:

Received March 7, 2021

Revised Jan 28, 2022

Accepted Feb 9, 2022

---

### Keywords:

Cloud computing

Internet of things

Mobile Ad-Hoc networks

Smart devices

Wireless communication

---

## ABSTRACT

Devices linked to the internet of things (IoT) may communicate with one another in several settings. Furthermore, rather of relying on an existing centralized system, users may develop their own network by using wireless capabilities. This kind of network is known as a wireless mobile ad hoc network. The mobile ad-hoc network (MANET) enables IoT devices to connect with one another in an unstructured networked environment. IoT devices may connect, establish linkages, and share data on a continuous basis. In this system, the cloud's purpose is to store and analyze data acquired from IoT devices. One of the most significant challenges in cloud computing has been identified as information security, and its resolution will result in an even bigger increase in cloud computing usage and popularity in the future. Finally, the goal of this project is to create a framework for facilitating communication between IoT devices in a Cloud and MANET context. Our major contribution is a ground-breaking research initiative that combines cloud computing with the MANET and connects the internet of things. This research might be used to the IoT in the future.

*This is an open access article under the [CC BY-SA](#) license.*



---

## Corresponding Author:

Tanweer Alam

Department of Computer Science, Islamic University of Madinah

Abo Bakr Al Siddiq, Al Jamiah, Medina 42351, Saudi Arabia

Email: tanweer03@iu.edu.sa

---

## 1. INTRODUCTION

A worldwide network for the knowledge society, the internet of things (IoT) is a network that connects (physical and virtual) things across digital networks that is currently under development and makes use of existing and new interoperable communication and information platforms. The IoT is a network that connects all of humanity's devices to the rest of the world through the Internet. Among the IoT's many applications are remote connection, mobile sensor networks, computer systems, 2G/3G/4G, GSM/GPRS, RFID/Wi-Fi/GPRS, GPS, microcontrollers, and microprocessors, among others. As "Internet of Things" facilitators, they're well-known in the industry [1]. Approximately 75 billion smart devices will be connected to the internet by 2025 [2]. Figure 1 depicts the proliferation of IoT devices from 2015 to 2025.

This evolutionary method enables users to swiftly scale up or down their requirements with minimum involvement from the service provider. The use of mobile technology has increased in popularity over the last many years [3], [4]. The number of smart devices available on the market is increasing at an alarming pace [5]. Smart devices have the ability to communicate data to any other active devices connected to a wireless network [6], [7]. When a smart device does not have enough information to selectively transmit a request, it broadcasts the request to all of its neighbors [8], [9]. It is the most important characteristic of ad hoc networks [10] of smart communication devices [11] to ensure their security, which is achieved via the use of encryption and decryption keys. Smart gadgets offer a variety of benefits, including context awareness, increased computational power, and independence from a single energy source [12].

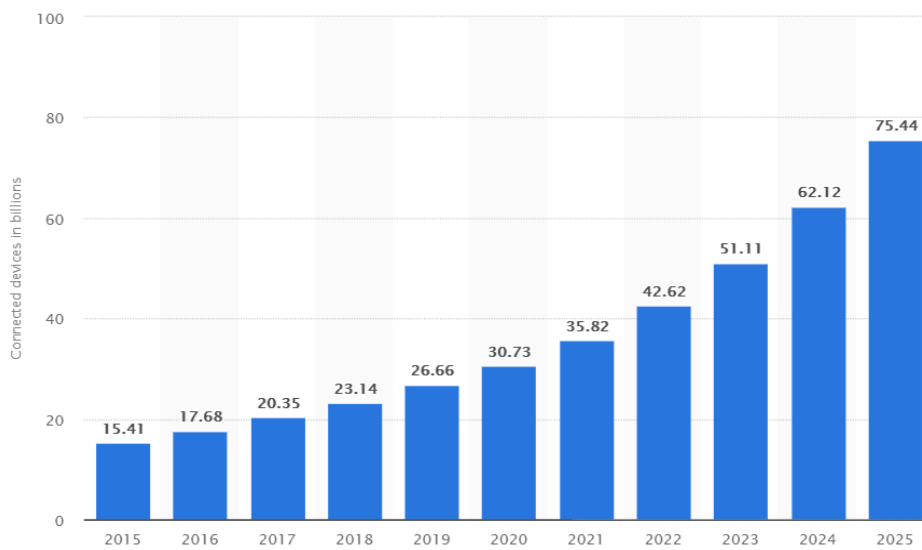


Figure 1. IoT devices growth between 2015-2025

As far as IoT is concerned, everything can be linked to the worldwide communication and information network. IoT is able to deliver stuff-related services within the limitations of objects, such as protection of privacy and conceptual continuity among physical objects and their corresponding electronic activities. With the attempt to deliver things-related resources under the limitations of life, all technology in the physical world and the knowledge environment must adjust. IoT devices are diverse based on various mobile platforms and infrastructure. These can communicate with other devices or service platforms over various platforms. The state of the devices changes continuously, e.g., resting and wake up, linked and/or disconnected, and the scope of the equipment, involving position and velocity. In addition, the number of devices will change continuously. The number of devices that need to be handled and interact with each other would be at least significantly greater than the devices connected to the current Network. The management of the data generated and their analysis for application purposes would be even more important.

## 2. LITERATURE REVIEW

When physical objects were first linked together, it signaled a new phase in the development of the internet of things, which started in 2008. The physical goods are connected to a smart database that contains intelligent data [13]. For companies and customers, the framework makes use of image recognition technology to distinguish real-world items, such as buildings and people [14]. It also recognizes brands and locations, among other things. At this point, the IoT is migrating from information-based technology to operational-based technology, i.e. from IPV4 (machine-to-machine) to IPV6 (internet of things) networking (machine-to-machine). A smart grid [15] is a system that includes sensors, smart devices, and interfaces to provide energy and other services. A rising number of sensors and sensor networks [16] are now able to communicate with one another over the Internet and the World Wide Web. Machine-to-machine (M2M) communication [17] is the core technology for data transfer among sensors and is the most widely used. An increasing variety of tools are being developed to assist in the conversion of embedded machine-to-machine communication concepts into operational systems [18]. In a larger sense, each of the previous clients is worried about the risks and challenges associated with cloud computing that might prevent them from achieving their objectives [19].

Figure 2 shows the framework of IoT. The following are the components of the internet of things: i) Identifiers [20], ii) Sensors [21], iii) Communications [22], iv) Computations, v) Services, vi) Semantics. Three technologies have contributed to the expansion of the internet of things. Using the ubiquitous computing architecture [23] intelligent physical entities are capable of executing on the platform. In addition to supporting machine-to-machine communication [24], [25] the internet protocol (IPv6) is based on ubiquitous computing and enables ubiquitous computing. When it comes to connecting billions of smart devices, the IPv4 internet has its limitations [26]. On the other hand, the IPv6 internet enables billions of smart devices to be securely linked [27]-[37].

These technologies should be updated on a regular basis in order to facilitate the evolution of the internet of smart devices. This includes multi-sensor frameworks that can be used to store, compute, analyze, and process data while using the least amount of space and energy. Most significantly, this study develops a unique secure communication paradigm for the IoT that makes use of cloud computing and mobile ad-hoc network (MANET) technology [38] as its foundation. It is based on three primary criteria that the communication security concept is implemented in the design of the IoT architecture [39].

- a. In a distributed system, it is difficult to manage data from millions of sensors in a centralized framework for smart device collecting.
- b. Controlling the resources of a big network capable of collecting environmental data from one central location is difficult.
- b. To handle sensors that examine the same data simultaneously in a centralized framework is quite tough.

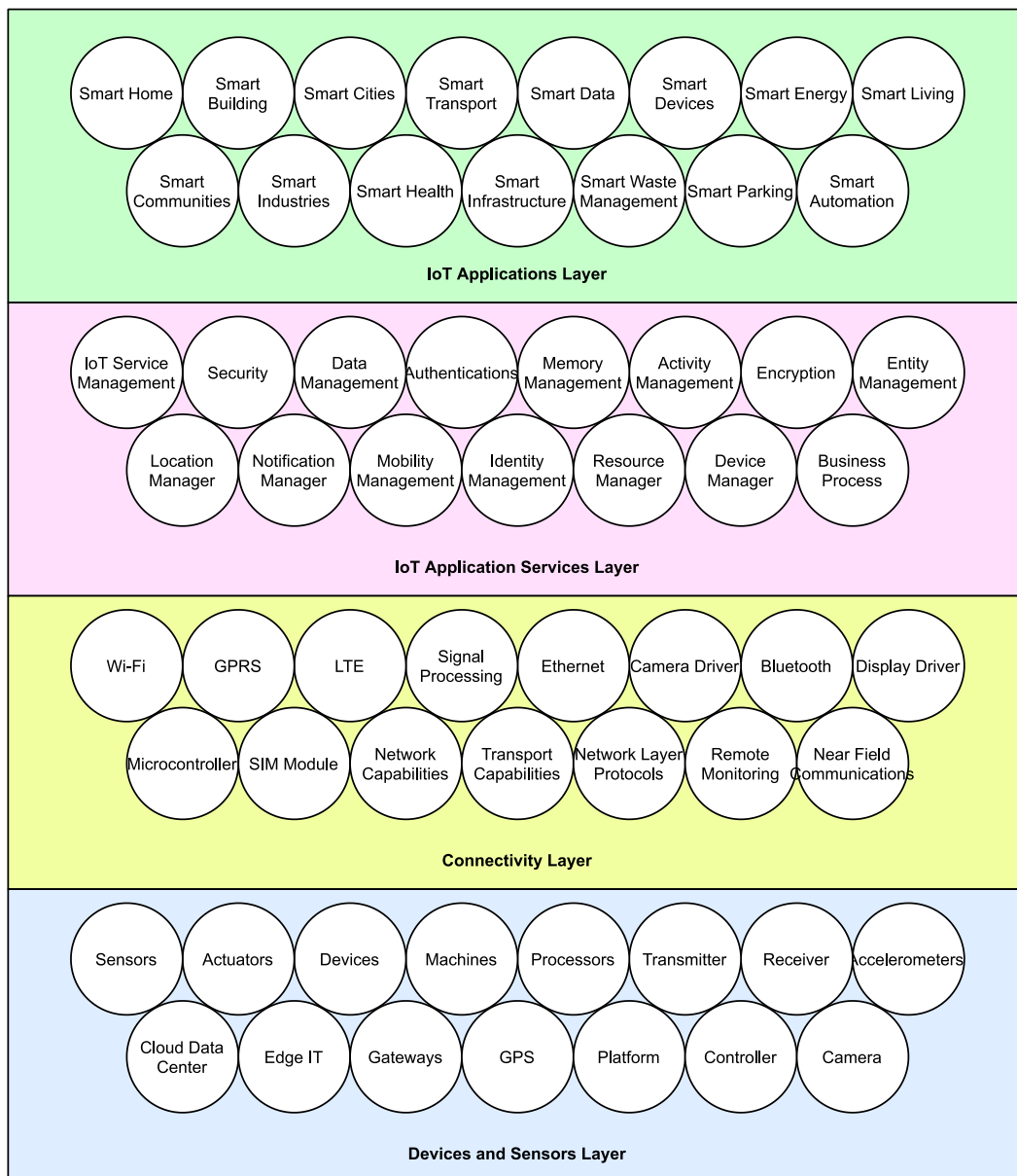


Figure 2. IoT framework

A computer paradigm known as cloud computing is widely used nowadays. Parallel computation, grid computation, distributed computation, and various computing paradigms, among others, have all contributed to this breakthrough. Three major cloud computing administration models are a software as a

service (SaaS), platform as service (PaaS), and infrastructure as a service (IaaS) [40]. End users that use software for their day-to-day operations and are ready to pay a monthly subscription price make up the primary market for software as a service (SaaS). Application developers are the key benefactors of platform-as-a-service since they require platforms on which to build software or applications. Infrastructure as a service (IaaS) is a kind of cloud computing service that is mainly aimed towards network architects that want infrastructure services. The internet of smart devices [41] is the most important component of cloud communication security challenges and hazards. A number of security challenges and hazards were explored in this article, including In the first instance, service disruption as a consequence of an attack is a concern. External attacks on the cloud have lately been attributed to a number of high-profile security breaches. As a consequence, cloud service providers must step up their efforts to prevent cyberattacks in order to mitigate the severity of these attacks. The second problem is the use of denial of service (DoS) attacks. In order to be effective, it must be unique, frequent, and simple to execute. When it comes to distinguishing between illegal and legitimate packets, there is an issue to contend with. These attacks, of course, need temporal coordination, which might be accomplished by inexperienced hackers utilizing simple programs and instruments. This will result in a deluge of packets being directed towards the targeted service provider, which will cause it to become inaccessible. In order to cope with the mitigation of such hazards, many technologies may be used [42].

### 3. RESEARCH METHOD

The intrusion detection system is an example of this sort of technological advancement. In the face of persistent dangers, it proves to be an effective piece of software. A hybrid intrusion detection system that can survive a broad variety of attacks is currently being developed [43]. Service hijacking is the third issue to be concerned about. Since service hijacking is a serious issue that threatens service confidentiality, integrity, and availability, it's important to bring it to the public's notice. Software weaknesses and specialized tools are routinely used by hackers to get access to passwords and usernames. Attackers will have total access to the cloud service, making it vulnerable to compromise. Some of these attacks may be avoided by limiting the transmission of personal information like passwords and usernames. The next degree of difficulty and danger is posed by attacks on the virtual machine (VM) itself. VM technologies are required by cloud service providers since the cloud environment is built on virtualization. A hypervisor is one of these tools, and it's in charge of running and maintaining virtual computers on a network. For service providers, the first step in using hypervisors should be a comprehensive assessment of all the potential issues. As the last step, cloud service providers must extensively analyze their security models. Cloud multitenancy is the next step. The cloud environment enhances client satisfaction by using shared resources. Multi-tenancy is used by cloud service providers to make the idea of sharing a reality [44], [45]. As a software architecture, it ensures that all of the available resources are used to their fullest degree.

To recognize and link adjacent smart devices, the cloud-MANET architecture of the IoT uses smart device-to-smart device communication. Since there is no need for a centralized infrastructure, cloud-MANET architecture is the way to go for the internet of things. The present cellular network cannot link smart devices without a central infrastructure, regardless of how close they are in proximity. The recommended solution will be particularly effective in the machine-to-machine (M2M) networks because of the large number of devices that are in close proximity to one another. According to this, it is possible to save energy, utilize frequencies, and maximize utilization efficiency by employing the MANET paradigm in smart device-to-smart-device communications. As a means of enhancing the capabilities of smart devices, MANET models may use cloud-based services for communication between devices. For example, cloud-based services will be used by smart device users to identify devices, decrease useable data in large amounts of data (such as videos and photographs), and analyze movies, images, and text, among others. It is my hope that the architecture I propose in this study will be useful in a 5G heterogeneous network for improving MANET and cloud computing capabilities on the internet of smart devices. Devices like smartphones and tablets would be considered service nodes in this design. This strategy also covers the security, reliability, and vulnerability of the communication system [46], [47].

### 4. SMART DEVICE COMMUNICATION FRAMEWORK

The smart device communication architecture incorporates a number of different levels of Internet of Things-supporting technologies. Using this method, you may demonstrate how different technologies communicate with one another while also showing the interoperability, flexibility, and compatibility of IoT implementations in diverse situations.

#### 4.1. Application layer

The application layer of the standard IoT framework is supposed to be the top layer. Consumers' needs are met by each layer, which delivers services that are tailored to their needs. The major purpose of this layer is to bridge the gap that exists between users and programs. In addition, it brings together the industry to deliver high-level smart application-type applications such as emergency control, safety control, and transfer as well as property, health, and environmental management [48]. It also brings together the industry to deliver strategic management for all smart-type solutions [49].

#### 4.2. Service support and application support layer

Many features appear in the second tier, which is comprised of service management and application support, such as IoT supply chain management, which includes business process modeling and business process execution, system structure features, which include business structure and system improvisation, and digital enterprise features, which include VE resolution and VE system, to name a few.

#### 4.3. Network communication layer

The purpose of such a layer would be to collect important evidence in the form of electrical impulses from the sensing layer and transmit it to the middleware layer processing systems over wireless networks such as Wi-Fi, wireless, WiMAX, Zigbee, GSM, 3G, and other similar technologies. Media transport protocols such as IPv4, IPv6, MQTT, DDS, and others are used to convey data.

#### 4.4. Smart device/sensor layer

This layer is made up of smart devices that are connected to the detectors. These detectors bridge the gap between the digital and physical worlds, allowing for the collection and analysis of data in real time. Sensors are available in a variety of forms and sizes, and they have a wide range of uses. This kind of sensor might be used to measure a variety of factors such as temperatures, air pollution levels, velocity, moisture, stress levels, wind speeds, motion, and energy, to name a few. In certain situations, they may also possess an awareness aptitude that enables them to measure a number of different quantities at once. The sensor is capable of computing the physical object and converting it into a signal that can be understood by a tool. The job of transmitters is divided into many categories.

Due to the large number of smart items that will be connected to the Internet, each one will require a unique address in order to connect and share data. The following phases are involved in the communication between smart devices in the IoT architecture: i) Addressing and identifiers: Because billions of smart items will be connected to the Internet, each one will require a unique address in order to connect and share data. To do this, a vast address space, as well as a unique address for each smart device, are necessary [50]; ii) Low-power transmission: Data transfer between devices, particularly wireless connections, is an energy-intensive activity that requires low power transmission. An interaction mechanism with minimal power consumption is thus needed; iii) The use of effective communication mechanisms in conjunction with memory-limited dynamic routing; iv) Improved reaction time and flawless synchronization [51]; v) The adaptability of smart devices.

### 5. APPLICATIONS

Many of the everyday life apps that we are already familiar with are intelligent, enabling them to communicate with one another and exchange vital information among themselves. As a consequence, a diverse range of ground-breaking applications will be developed. There is little question that this new technology, in conjunction with some automated technologies, will increase the overall quality of our lives. For example, google car, which seeks to provide real-time driving experiences for vehicles while also providing information on traffic conditions, the environment, and other information exchanges, all of which are heavily related to the internet of things, is already on the market [52], [53].

#### 5.1. Smart home

Home automation used to be considered a science fiction notion. It was alarming until people learned the genuine benefits of home automation, at which time the notion began to appeal to a wider variety of individuals. Home automation encompasses a wide range of functions such as door and window controls, air conditioner controls, multimedia controls, lighting controls, stove controls, and so on. A smart house is defined as the capacity to control one's home from a distance utilizing various technologies such as GSM, Wi-Fi, Bluetooth, Zigbee, and so on. Smart homes are becoming more popular [54].

## 5.2. Internet of vehicles (IoV)

It is comprised of a collection of applications that analyze and exchange data in order to reduce traffic congestion, enhance traffic management, limit environmental effects, and increase revenue for businesses and public transit. In order to share data between high-speed automobiles, it is necessary to use cutting-edge technology that includes sensors, the internet, wireless connections, and protocols. The IoT should be capable of processing real-time data efficiently. The conventional data processing and communication system, on the other hand, has a number of challenges, including connection and coverage, communication and energy costs, congestion, coordination and execution, and the notification of traffic incidents [55].

## 5.3. Smart agriculture intelligent machinery

Precision agricultural equipment cultivation, precise fertilizer and pesticide application, robotic welding, precision parallel grain harvesting, and yield management are all made possible by this technology, as are precision parallel grain harvesting and yield management. A real-time judgment and correction are made by the machine based on data collected from GPS, geographic information system (GIS), and on-board sensors. The onboard sensors assess a variety of characteristics, including plant biomass, chlorophyll content, soil nitrogen level, and other factors. When spraying pesticides, for example, the system may make use of sensor and GIS data to adjust the boom height, nozzle flow, and droplet size as needed. GIS data is downloaded by farming, fertilizing, and harvesting equipment in order to assist them in planning their operations.

## 5.4. Smart mines

Equipment used in the building and mining, farming, and logging industries is one of the fastest-growing segments of IoT. In mining equipment, the IoT offers application potential. It's quite risky to work around such massive equipment. It's possible that a worker might die if they don't take precautions. For example, the usage of location sensors, cameras, and radio frequency locating devices (RFLDs) shows how IoT technology might help improve safety in this setting.

## 5.5. Smart clinics

Smart clinics would be outfitted with smart portable wearing RFID bands that patients would be provided with upon admission. This would allow doctors and nurses to track patients' cardiac output as well as their blood pressure, temperature, and other symptoms as they entered and left the clinic. Several emergency scenarios, such as heart failure, are now available on the market that may be transported to the survival kit, allowing physicians to closely monitor the patients and refer them to the clinic as needed.

## 6. CONCLUSION

When 5G heterogeneous networking is deployed, this architecture has the potential to play a significant role in the IoT framework. This study might help in the creation of smart gadgets that communicate more efficiently and quickly. Because the cloud paradigm is built on a distributed architecture, it inherits some of the risks and vulnerabilities associated with decentralized design. The risks and issues related to communication security are veiled behind the allure of cloud computing. However, as the cloud paradigm evolved, the quantity and severity of these hazards increased. The author explored the security needs and obstacles for communication security across all smart devices, as well as the advantages of cloud computing, within the context of cloud computing. This study was a success, and there is room for further research in this field.

## REFERENCES





- [1] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 6122–6131, 2016.
- [2] Statista, "Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025," *Technology and Telecommunications*. pp. 1–5, 2016, [Online]. Available: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.
- [3] A. J. Yuste, E. Casilari, A. Triviño, and F. D. Trujillo, "Adaptive gateway discovery for mobile ad hoc networks based on the characterisation of the link lifetime," *IET Communications*, vol. 5, no. 15, pp. 2241–2249, Oct. 2011, doi: 10.1049/iet-com.2010.0692.
- [4] T. Alam, "Middleware implementation in MANET of android devices," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3638977.
- [5] T. Alam and M. Aljohani, "Decision support system for real-time people counting in a crowded environment," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3639076.
- [6] T. Alam, "Internet of things: A secure cloud-based MANET mobility model," *International Journal of Network Security*, vol. 22,

- no. 3, p. 7, 2020, doi: 10.6633/IJNS.202005\_22(3).17.
- [7] T. Alam, Y. M. Alharbi, F. A. Abusallama, and A. O. Hakeem, "Smart campus mobile application toward the development of smart cities," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3638973.
- [8] T. Alam, "A middleware framework between mobility and IoT using IEEE 802.15.4e sensor networks," *Jurnal Online Informatika*, vol. 4, no. 2, p. 90, Feb. 2020, doi: 10.15575/join.v4i2.487.
- [9] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, Feb. 2020, doi: 10.34306/itsdi.v1i2.103.
- [10] 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, doi: 10.30630/joiv.4.1.334.
- [11] T. Alam, "Efficient and secure data transmission approach in cloud-MANET-IoT integrated framework," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 12, no. 1, p. 6, 2020, doi: 10.36227/techrxiv.12657194.
- [12] T. Alam and M. Benaïda, "The role of cloud-MANET framework in the internet of things (IoT)," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 14, no. 12, p. 97, Dec. 2018, doi: 10.3991/ijoe.v14i12.8338.
- [13] T. Alam, "Middleware implementation in cloud-MANET mobility model for internet of smart devices," *SSRN Electronic Journal*, 2017, doi: 10.2139/ssrn.3638980.
- [14] T. Alam and M. Benaïda, "Benaïda M. CICS: Cloud-internet communication security framework for the internet of smart devices," *International Journal of Interactive Mobile Technologies (IJIM)*, vol. 12, no. 6, p. 74, Oct. 2018, doi: 10.3991/ijim.v12i6.6776.
- [15] T. Alam and B. Rababah, "Convergence of MANET in communication among smart devices in IoT," *International Journal of Wireless and Microwave Technologies*, vol. 9, no. 2, pp. 1–10, Mar. 2019, doi: 10.5815/ijwmt.2019.02.01.
- [16] T. Alam, "IoT-fog: A communication Framework using blockchain in the internet of things," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 7, no. 6, pp. 1–5, 2019, doi: 10.36227/techrxiv.12657200.
- [17] T. Alam, "Blockchain and its role in the internet of things (IoT)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 151–157, Jan. 2019, doi: 10.32628/CSEIT195137.
- [18] T. Alam, "A reliable framework for communication in internet of smart devices using IEEE 802.15.4," *ARNP Journal of Engineering and Applied Sciences*, p. 10, 2018.
- [19] T. 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)*, vol. 3, no. 5, pp. 450–456, 2018.
- [20] T. Alam and M. Aljohani, "Design and implementation of an Ad Hoc Network among android smart devices," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Oct. 2015, pp. 1322–1327, doi: 10.1109/ICGCIoT.2015.7380671.
- [21] T. Alam and M. 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)*, Nov. 2015, pp. 371–375, doi: 10.1109/ICIIBMS.2015.7439466.
- [22] M. Aljohani and T. Alam, "An algorithm for accessing traffic database using wireless technologies," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Dec. 2015, pp. 1–4, doi: 10.1109/ICCIC.2015.7435818.
- [23] T. Alam and M. 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 - ICTCS '16*, 2016, pp. 1–6, doi: 10.1145/2905055.2905244.
- [24] T. Alam, "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices," *ARNP Journal of Engineering and Applied Sciences*, p. 10, 2017.
- [25] T. Alam, S. Srivastava, Arun Pratap Gupta, and R. G. Tiwari, *Scanning the node using modified column mobility model*. R. R. Manza, 2010.
- [26] T. Alam, P. Kumar, and P. Singh, "Searching mobile nodes using modified column mobility model," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 1, pp. 513–518, 2014.
- [27] T. Alam and B. K. Sharma, "A new optimistic mobility model for mobile ad hoc networks," *International Journal of Computer Applications*, vol. 8, no. 3, pp. 1–4, Oct. 2010, doi: 10.5120/1196-1687.
- [28] P. Singh, P. Kumar, and T. Alam, "Generating different mobility scenarios in ad hoc networks," *International Journal of Electronics Communication and Computer Technology (IJECCCT)*, vol. 4, no. 1, pp. 1–3, 2014.
- [29] A. Sharma, T. Alam, and D. Srivastava, *Ad hoc network architecture based on mobile Ipv6 development*. K. V. Kale, 2008.
- [30] M. Aljohani and T. Alam, "Real time face detection in ad hoc network of android smart devices," in *Advances in computational intelligence*, 2017, pp. 245–255.
- [31] M. Aljohani and T. Alam, "Design an M-learning framework for smart learning in ad hoc network of Android devices," in *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Dec. 2015, pp. 1–5, doi: 10.1109/ICCIC.2015.7435817.
- [32] T. Alam, "Tactile internet and its contribution in the development of smart cities," *International Journal of Electronics and Information Engineering*, vol. 12, no. 3, pp. 112–118, 2020, doi: 10.6636%2fijeie.202009\_12(3).02.
- [33] T. Alam, "5G-enabled tactile internet for smart cities: vision, recent developments, and challenges," *Jurnal Informatika*, vol. 13, no. 2, p. 1, Jul. 2019, doi: 10.26555/jifo.v13i2.a13426.
- [34] T. Alam, A. A. Salem, A. O. Alsharif, and A. M. Alhejaili, "Smart home automation towards the development of smart cities," *APTİKOM Journal on Computer Science and Information Technologies*, vol. 5, no. 1, pp. 13–20, Mar. 2020, doi: 10.34306/csit.v5i1.119.
- [35] B. Rababah, T. Alam, and R. Eskicioglu, "Next generation internet of things architecture towards distributed intelligence: reviews, applications, and research challenges," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 12, no. 2, p. 9, 2020, doi: 10.36227/techrxiv.12657182.
- [36] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, Mar. 2015, doi: 10.5120/19787-1571.
- [37] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
- [38] M. Bilal, "A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3D printers," *arXiv preprint arXiv:1708.04560*, p. 21, 2017.
- [39] T. Alam, A. Ullah, and M. Benaïda, "Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems," *Journal of Ambient Intelligence and Humanized Computing*, Jan. 2022, doi: 10.1007/s12652-021-03663-2.
- [40] D. Durairaj, T. K. Venkatasamy, A. Mehbodniya, S. Umar, and T. Alam, "Intrusion detection and mitigation of attacks in

- microgrid using enhanced deep belief network,” *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, pp. 1–23, Jan. 2022, doi: 10.1080/15567036.2021.2023237.
- [41] T. Alam, M. Tajammul, and R. Gupta, “Towards the sustainable development of smart cities through cloud computing,” in *AI and IoT for Smart City Applications*, 2022, pp. 199–222.
- [42] T. Alam, “IBchain: Internet of things and blockchain integration approach for secure communication in smart cities,” *Informatica*, vol. 45, no. 3, Sep. 2021, doi: 10.31449/inf.v45i3.3573.
- [43] T. Alam, “Blockchain cities: the futuristic cities driven by Blockchain, big data and internet of things,” *GeoJournal*, Sep. 2021, doi: 10.1007/s10708-021-10508-0.
- [44] T. Alam, “Cloud-based IoT applications and their roles in smart cities,” *Smart Cities*, vol. 4, no. 3, pp. 1196–1219, Sep. 2021, doi: 10.3390/smartcities4030064.
- [45] T. Alam, A. A. Hadi, and R. Q. S. Najam, “Designing and implementing the people tracking system in the crowded environment using mobile application for smart cities,” *International Journal of System Assurance Engineering and Management*, vol. 13, no. 1, pp. 11–33, Feb. 2022, doi: 10.1007/s13198-021-01277-7.
- [46] T. Alam, “A survey on the use of blockchain for the internet of things,” *International Journal of Electronics and Information Engineering*, vol. 13, no. 3, p. 12, 2021, doi: 10.22541/au.163519364.41044814/v1.
- [47] T. Alam and M. Erqsous, “he real-time alert system for prayers at smart masjid,” *Scientific Journal of Informatics*, vol. 7, no. 2, pp. 166–172, 2021.
- [48] T. Alam, “Performance evaluation of blockchains in the internet of things,” *Computer Science and Information Technologies*, vol. 1, no. 3, pp. 93–97, Nov. 2020, doi: 10.11591/csit.v1i3.p93-97.
- [49] T. Alam, B. Rababah, A. Ali, and S. Qamar, “Distributed intelligence at the edge on IoT networks,” *Annals of Emerging Technologies in Computing*, vol. 4, no. 5, pp. 1–18, Dec. 2020, doi: 10.33166/AETiC.2020.05.001.
- [50] T. Alam, M. A. Khan, N. K. Gharaibeh, and M. K. Gharaibeh, “Big data for smart cities: A case study of neom city, saudi arabia,” in *Smart cities: a data analytics perspective*, 2021, pp. 215–230.
- [51] T. Alam, “Federated learning approach for privacy-preserving on the D2D communication in IoT,” in *International Conference on Emerging Technologies and Intelligent Systems*, 2022, pp. 369–380.
- [52] T. Alam, “Blockchain-based big data analytics approach for smart cities,” *Electrical and Computer Engineering*, pp. 45–61, 2020, doi: 10.31219/osf.io/hd5n3.
- [53] T. Alam, S. Qamar, A. Dixit, and M. Benaïda, “Genetic algorithm: reviews, implementations, and applications,” *International Journal of Engineering Pedagogy*, p. 19, 2020, doi: 10.36227/techrxiv.12657173.v1.
- [54] T. Alam, “IoT-fog-blockchain framework,” *International Journal of Fog Computing*, vol. 3, no. 2, pp. 1–20, Jul. 2020, doi: 10.4018/IJFC.2020070101.
- [55] T. Alam, “mHealth communication framework using blockchain and IoT technologies,” *International Journal of Scientific & Technology Research*, vol. 9, no. 6, p. 7, 2020, doi: 10.22541/au.159223908.81270387.

## BIOGRAPHIES OF AUTHORS



**Tanweer Alam**     is working in Islamic University of Madinah as a Professor (Associate). His academic qualification is Ph.D., MPhil, MTech, MCA, MSc. His research area includes Blockchain, Internet of Things and Wireless Communications. His profile was published in Who's who in the world- 2013. He has membership of IACSIT, IA Engg, ISOC, Computer Science Teachers Association etc. He is a single author of twelve books. His books are included in the curriculum of several universities. He can be contacted at email: tanweer03@iu.edu.sa.