# An Assessment on the State of Art of Internet of Things (IoT)

**Sarabjeet Singh Sethi, Dinesh Kumar, Lalit Kumar Lata**
Department of Electronics & Communication Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur -302017 (INDIA)
***Email: sarabjeet.singh@skit.ac.in, dinesh.kumar@skit.ac.in, lalit.lata2008@gmail.com***
Received 03.02.2023 received in revised form 13.03.2023, accepted 24.03.2023
***DOI:*** *https://dx.doi.org/10.47904/IJSKIT.13.1.2023.23-28*

***Abstract*- In essence, the Internet of Things (IoT) is a network that connects computers, electronic and mechanical goods, people, and other entities that have been given unique identities (UIDs) and the capacity to exchange data across human-to-human and computer-to-human connections. Another feature of the IoT devices is linked together in a manner akin to that of humans as well as computers, in the midst of IP addresses (Internet Protocol Addresses) that are assignable and capable of transmitting data to other artificial things or through networks. This paper describes the utilization of IoT in the cloud, fog, IoT technologies with applications and security. Finally, discussion is done to the unanswered questions for both existing and upcoming IoT research.**

**Keywords–** IoT technologies, cloud computing, fog computing, IoT security and privacy.

## 1. INTRODUCTION

Noteworthy advancements in artificial intelligence and a precursor to a revolution in the globe today, the IoT, is developing [1]. As seen in Fig. 1, IoT is a vast network of connected gadgets. The linked devices carry out predefined tasks, gather data, and exchange operational data [2]. The ecology of IoT is made up of smart gadgets with online access that utilize integrated systems like CPUs, sensors, and communication equipment put together to assemble, communicate, and respond on the information collected [3]. IoT devices expose the sensed data gathered via an IoT gateway or any other edge devices which periodically converse amid other linked devices and behave in response to the information they obtain from one another. The explicit connection, networking along with employed communication protocols leveraging these web-enabled gadgets depend greatly on the IoT based applications that are employed with them. The IoT is a collection of networked devices, including sensors, automobile antennas, and other devices [4]. Due to the huge volumes of data, it creates and analyses, IoT is a primary driver of big data analytics activities [5]. The Internet of Things (IoT) is a manifestation of an interconnected system of devices capable of obtaining and exchanging data. These network devices often connect with one another over internet protocol (IP). The Internet of Everything (IoE) is a subset of the Internet of items (IoT) that encompasses people, processes, data, and items in network connections. The Internet of Nano Things (IoNT) is the next phase, a Nano Technology that allows communication between nanoscale objects. The Internet of Mission-crucial Things (IoMCT) is utilised in crucial missions such as search and rescue, battlefields, and so on. The Internet of Mobile Things (IoMT) is used to connect devices that have built-in mobile sensors [6].

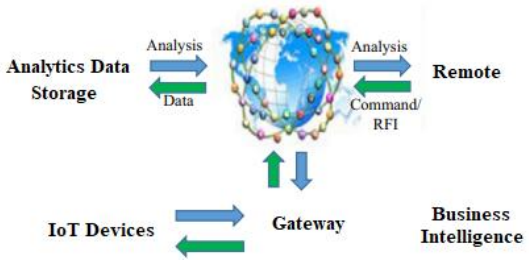


**Figure 1: IoT network attributed to multiple devices. [2]**

Fig. 2 provides an illustration of IoT data collecting through data processing. An application of IoT towards cloud computing as well as fog is covered in the paper. The limitations of prior attempts and the challenges that lay ahead are also discussed. Identification and analyses are done to a number of outstanding issues that need to be dealt with the correct deployment and operation of IoT for cloud and fog computing.


**Figure 2: IoT data collection to data processing.**

This paper, which is based on an IoT survey in addition to evaluation in numerous domains, is separated into six sections. IoT technology and cloud IoT are the topics of sections two and three, respectively. Section four concentrates on IoT usage in fog in a similar manner. The privacy and security of IoT form the basis of Section 5. Section 6 presents the unanswered research questions in this field.

2. Technologies for IoT

Outlining the technology that will regulate the enormous number of inventions and discoveries that will be made in the future is a challenging undertaking. However, it can be demonstrated by breaking down the massive stack into the four

components that make up the Internet of Things [7, 8].

- Computer hardware
- Software gadget
- Mode of communication
- Platform

### *2.1 Computer hardware*

These make up the system's physical structure; they are the elements referred to in the IoT name as "things" [9]. They serve as the link between the physical world and the digital one. They can be seen in a variety of places, such as a phone sensor or a self-driving automobile [10]. IoT hardware is any physical connected item that can be made "smart" by adding a chip, sensor, or board for signal control. These tools are extensively utilized to collect data on their corresponding fields. In order to make the gadgets smart, several sensors and microprocessors are placed inside of them. However, a little issue arises which could be resolved in the coming years, namely higher cost of procure, which necessitates a sizable sum of money [11, 12]. The device's compatibility with the newly developed sensors, which may become less accurate with time, is another issue [13, 14].

### *2.2 Software gadget*

The software device is the next phase in the creation of the IoT [15]. It serves as the IoT system's brain; hence the adjective "smart" may be employed [16]. This division is responsible for cloud communication and data implementation. It is in charge of collecting system data, integrating devices, and analyzing data on the cloud using IoT software. By transforming the data into application-level formats that the user can perceive, it also makes it possible for the user to engage with the system. (DAS) Data acquisition system converts analogue data from devices into digital streams by carrying out all logical, analytical, and theoretical procedures. The IT edge repeats the same set of activities after the information has been processed before it is entered the information center to improve its accuracy and in formativeness.

### *2.3 Mode of Communication*

It serves as the IoT system's third foundation [17]. The communication stage, which is in charge of supplying the path for transmission of the recently formed intelligent hardware devices, comes after the setup for the hardware as well as software components is finished, moreover made ready. First, we must select the data transmission path from a variety of options on the market. These options include satellite controlling, Bluetooth, or Wi-Fi LAN. All communication chipset has a unique cloud structure and configuration that governs not merely the distribution method but also the fashion whereby the devices interact. An illustration of a ladder without steps illustrates the impact of communication in the IoT [18].

### *2.4 Platform*

The fourth and last Internet of Things system is where all the data mentioned above is stored after being gathered and processed. From this point on, the user is given the facts in an approachable format. The purpose of the data is categorized and divided in this part. The information is classified and kept on several shelves [19]. Various businesses in the marketplace offer platforms relying on the features along with the layout platform [20]. The options may change depending in terms of budget and necessity. Numerous businesses offer platforms that may be loaded on a device using additional storage or cloud storage.

## 3. CLOUD IOT

A whole collection of gadgets for combining, processing, storing, and dividing data both at the edge and in the cloud are the Google Cloud IoT [21]. For all users' IoT needs, the platform includes flexible, fully managed cloud services, as well as an integrated development stack for edge/on-premises solutions with AI capabilities [22, 23]. In Fig. 3 [24], the Cloud IoT scenario is depicted. IoT has advanced along with the more prevalent data age. With billions of connected equipment and gadgets, Cloud service for the Internet of Things offers the finest compatibility amid inexpensive sensors within, indicating much greater accessibility [25].

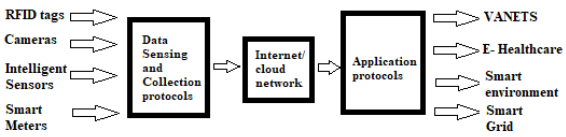


**Figure 3: Cloud IoT scenario [24].**

### *3.1 Salesforce IoT Cloud*

The Salesforce.com IoT cloud is set up with plans to store and manage IoT data [26]. Thunder, described by Salesforce.com has indeed been defined as an "incredibly diverse consistent event planning engine." [27]," manages IoT Cloud. The system is designed to collect the massive amounts of data produced by devices, websites, assistant's sensors, applications, clients to begin working for developing replies. IoT Cloud may also give business clients a far more comprehensive and integrated picture of their customers without the need for specialist knowledge or the assistance of a data investigator [28]. According to Dylan Steele [29], the IoT Cloud will accumulate furthermore pile up the data that is produced by linked devices, while also keeping that data easily accessible in terms of improving user experience. During the event, Steele noted that one benefit of the IoT Cloud is that it makes it easier for corporate clients to gather information. Less

specialized customers are no longer need to rely on information specialists to profit from the knowledge.

### *3.2 Cloud Computing and IoT for the Future Internet*

The question of how the gadgets would remain connected throughout still stands. The cloud network offered by web of things supervision contains the proper reaction. More significant IoT cloud usage has acted as a catalyst for the development and dissemination of flexible IoT applications and success tactics. IoT and cloud/fog computing are now two inextricably linked forthcoming web revolutions, each advancing the other [30].

### *3.3 Problems with the cloud:*

**Ownership of data:** Does the user or the cloud provider own "the data" once the user store it during an organization's cloud administration? For IoT applications that use private data, this may be absolutely necessary [31].

**Potential collisions:** The IoT application function if the connection is interrupted or the cloud service itself breaks [32]. Short incompatibility will not be a big issue for some IoT applications, like reasonable farming, but it may be catastrophic for others. There is no need to worry about using health or security programs continuously for hours or even just a few seconds.

**Latency:** Transmitted data to the cloud and getting commands heading to the devices both cost money [33]. Ensuring IoT applications, as these milliseconds are vital in areas like wellbeing and security. Self-sufficient vehicles make a decent example. The user doesn't have to go to the automobile to deal with the cloud if a collision is imminent before choosing to switch off the methods.

## 4. FOG IOT

"Fog computing is a dispersed computing structure or technique in which computer resources are distributed across a source of data in addition to cloud or supplementary files centre [34, 35]," according to the definition given above. The technology that is most suited to handle IoT is fog computing [36]. Fog computing, sometimes referred to as a fog or cloud networks, takes happen at a decentralized location between data sources and the cloud at the logical and effective point [37]. Similar fog computing, edge computing offers the advantages and functionality of the cloud wherever information is produced as well as handled. Where data has to be evaluated quickly and with a large number of policies, fog is employed. The tactics are quite far from the environment, and the gadget equipment is exposed to harsh circumstances.

Fog nodes offer temporary storage, the capacity to process data before it is transferred to the cloud, and quick, accurate decisions. IoT devices, additional fog nodes, the cloud, routers, encircled servers, changes, video shadowing cameras, etc. are all connected via the network [38]. Every fog node has its own cumulative fog node and may be deployed anywhere within the network [39].

Fog nodes are constantly giving to people who accumulate any type of record. The automated controller reads signals from Internet of Things devices throughout the process of data transfer through a fog computing structure in an IoT atmosphere [40]. The system program required in order to automate IoT devices is launched by the controller (reader). Set the platform drivers to a data governor system standard OPC or to alternative gateway measures. This data is converted into a contract that an Internet service provider, such as MQTT or HTTP, can comprehend. The data is then simplified and delivered to the cloud or IoT gateway following the conversion. These endpoints either gather comprehensive data for more information or send data to the cloud for widespread public use.

## 5. IOT SECURITY & PRIVACY

Because users do not know what data is gathered and how it is utilized, they are gradually giving up their privacy without even realizing it, which makes the Internet of Things the most hazardous technology [41]. As a result, there may be no genuine way to fix a damaged consumer's privacy. Fig. 4 [42] provides an illustration of IoT security and privacy. This keeps data's integrity intact and prevents hackers from looking through it. Strong passwords or time-based authentication signatures must be used for any communication with your IoT devices [43]. The use of antivirus software can provide an important layer of defense against outbreaks.

For IoT gadgets to function more efficiently, hardware, software, and connection must be secure [44]. Without security in IoT, it is possible to hack robots that have artificial intelligence and link anything to them [45]. Once the hackers have taken over the machine, the user will not be able to use it again unless it is linked to some anti-virus software.

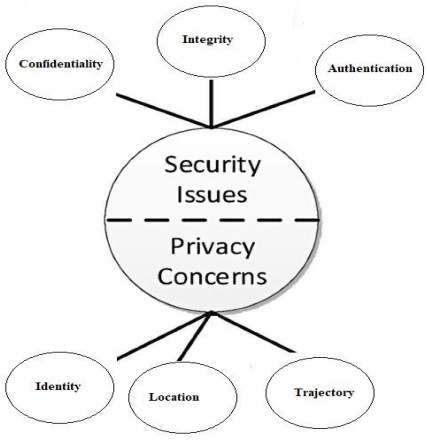


**Figure 4: Security and Privacy of IoT [42].**

Caution must be taken to safeguard the system from hackers that are more skilled than and can take over an object's functioning while stealing the user's digital data. Following are certain risks associated and ways to secure data

- Risk 1: Storage of Personal Data
- Risk 2: Non-Existent Commitment to Updates and Security
- Ways to Secure Your Data in IoT
  1. Understand the Benefts of Connecting to the Internet
  2. Use the Secondary Network
  3. Keep Changing Your Passwords
  4. Do not Enable Universal Plug and Play Functions
- Privacy Risk

Because IoT devices are networked with various equipment and programming, there is a clear risk of sensitive data flowing via unauthorised control. All devices send the client's data, such as name, address, date of birth, health card data, credit card information, and much more, without encryption. Whilst there are some security and protection concern with IoT, it offers value to our lives by enabling us to deal with our daily routine tasks remotely and organically, and, more importantly, it is a significant benefit for businesses.

## 6. OPEN RESEARCH ISSUES

This paper's primary goal is to offer an overview of IoT areas along with research challenges. The challenges and future directions for the research effort that are mentioned in this paper's preceding sections are covered in this part.

- **Technologies for IoT:** Since it is possible to convert supply chain management, home automation, and healthcare technology, the question of what technology will be converted to IoT remains a challenge in this study field. Few people are worried about auto cars and health systems since if a sensor fails, a lot of damage would result [46]. System hardware for a certain topic is particularly problematic since neither researchers nor organizations recognize any specified hardware or software. The majority of Internet of Things (IoT) apps were accessed via smart phones, and during mobility, both the cell and the communication channel are altered. This results in a delay when sending instructions to the Internet of Things system specific actions, which is a major issue [47].

- **Cloud IoT:** Big data generated by IoT devices is transferred to the cloud for processing, delaying findings and actions as a result of the cloud's slow communication with the IoT device [48]. Data transmission and reception delays are also being brought on by the distance between IoT devices and the cloud. Another major issue is that even a basic IoT system has to store log files, transaction data, and data connected to applications. As a result, buying cloud storage drives up the price of cloud IoT systems.

- **Fog IoT:** Sensitive monitoring data is continually generated by IoT sensors and sent to the cloud for analysis and response to distorted circumstances, however the cloud is located remote from the IoT system. Huge volumes of information must be sent and analyzed slowly from IoT devices to the cloud, which is bad for use in real-time applications. Fog computing allows for the procedure at the IoT sensor edge, but the flow of data is problematic owing to insufficient security, trustworthy and un trusted nodes, and other factors [49, 50]. This is a weighty issue with fog IoT since the fog does not offer substantial data storage, such as the cloud, and cannot be saved for an extended period of time [51].

- **IoT Applications:** Many researchers and companies launched IoT applications, but the quality of the user experience (QoE) was not yet anticipated to boost the quality of the service (QoS) [52, 53]. Application developers and service providers would both benefit from the inclusion of QoE in IoT apps as it will help them create applications that better meet user demands [54]. Some of the top IoT applications are:
  - Smart Urban Citie
  - Wearables
  - Smart Retail
  - Digital Health
  - Smart Farming
  - Smart Supply Chain
  - Industrial Internet
  - Smart Home System
  - Smarts Water System

## 7. CONCLUSIONS

This paper looked at IoT related technologies including the cloud and fog. IoT security and privacy is also provided. IoT security as well as privacy is crucial for protecting information and preventing loss. For upcoming research directions, unresolved concerns are also explored. It is discovered that sensors are crucial parts of the Internet of Things system; if sensors malfunction while monitoring the environment, operating a car, or in health applications, substantial harm will result. Detailed background presented in this paper provides the information, explanations of essential concepts, examples of various IoT technologies, and suggestions for their use in upcoming developments.

## 8. REFERENCES

[1] Thumeera WR, Gosine RG, James LA, Mann GKI, de Silva O, Warrian PJ (2020) The internet of things in the oil and gas industry: a systematic review. IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8654-8673.

[2] Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2
[3] Medhat GM, Aneiba A, Basurra S, Batty O, Elmisery AM, Kovalchuk Y, Rehman MHU (2019) Internet of things and data mining: from applications to techniques and systems. Wiley Interdiscip Rev Data Min Knowl Disc 9(3): e1292.
[4] Hossein MN, Taleb T, Arouk O (2016) Low-altitude unmanned aerial vehicles-based internet of things services: comprehensive survey and future perspectives. IEEE Internet Things J 3(6):899–922.
[5] Marjani M, Nasaruddin F, Gani A, Karim A, Hashem IAT, Siddiqa A, Yaqoob I (2017) Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access 5:5247–5261.
[6] Srinivasan, C.R. & Bodduna, Rajesh & Saikalyan, P. & Premsagar, K. & Yadav, Eadala Sarath. (2019). A review on the different types of internet of things (IoT). Journal of Advanced Research in Dynamical and Control Systems. 11. 154-158.
[7] Giancarlo F, Savaglio C, Palau CE, de Puga JS, Ganzha M, Paprzycki M, Montesinos M, Liotta A, Llop M (2018) Towards multi-layer interoperability of heterogeneous IoT platforms: the INTER-IoT approach. Integration, interconnection, and interoperability of IoT systems. Cham: Springer, pp 199–232.
[8] https://camrojud.com/how-iot-works-4-main-components-ofiot-system/. Accessed 6 Jun 2020.
[9] Gwani SM, Sequeiros JBF, Correia AFPP, Freire M, Inacio PRM (2017) IoT hardware development platforms: past, present, and future. Internet Things-Chall Adv Appl 101 133.
[10] Petrov V, Samuylov A, Begishev V, Moltchanov D, Andreev S, Samouylov K, Koucheryavy Y (2017) Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT). IEEE Internet Things J 5(5):3710–3723.
[11] Julia J (2017) Internet of things-based Deadbolt lock latch strike location smart sensor. U.S. Patent Application 14/804,146. Filed 26 Jan 2017.
[12] Adegbija T, Rogacs A, Patel C, Gordon-Ross A (2017) Microprocessor optimizations for the internet of things: a survey. IEEE Trans Comput Aid des Integr Circ Syst 37(1):7–20.
[13] Tsai C-W, Lai C-F, Vasilakos AV (2014) Future internet of things: open issues and challenges. Wireless Netw 20(8):2201–2217.
[14] Efremov S, Pilipenko N, Voskov L (2015) An integrated approach to common problems in the internet of things. Procedia Eng 100:1215–1223.
[15] Fatmasari RL, Ozcelebi T, Lukkien J (2018) Understanding IoT systems: a life cycle approach. Procedia Comput Sci 130:1057–1062.
[16] Qian Z, Wang R, Chen Q, Liu Y, Qin W (2010) Iot gateway: bridging wireless sensor networks into internet of things. In: 2010 IEEE/IFIP international conference on embedded and ubiquitous computing. IEEE, pp 347–352.
[17] Hamrioui S, Lorenz P (2017) Bio inspired routing algorithm and efficient communications within IoT. IEEE Netw 31(5):74–79.
[18] Das Almeida RJ, Brito V, Palma LB, Barata J (2017) Approach to adapt a legacy manufacturing system into the IoT paradigm. Int J Interact Mob Technol iJIM 11(5).
[19] Mohieddine B, Abdaoui A, Ahmad SHM, Touati F, Kadri A (2018) A modular IoT platform for real-time indoor air quality monitoring. Sensors 18(2):581.
[20] Hamdan H, Rajab H, Cinkler T, Lengyel L (2018) Survey of platforms for massive IoT. In: 2018 IEEE international conference on future IoT technologies. IEEE, pp 1–8.
[21] Rashid N, Ahmed Z, Ahmad Z, Shaikh N, Laghari A, Kumar K (2020) Cloud computing applications: a review. EAI Endor Trans Cloud Syst 6(17).
[22] Mahalle PN, Shinde GR, Deshpande AV (2021) The convergence of internet of things and cloud for smart computing. CRC Press.
[23] Ali LA, He H, Khan A, Kumar N, Kharel R (2018) Quality of experience framework for cloud computing (QoC). IEEE Access 6:64876–64890.
[24] Stergiou C, Psannis KE, Kim B-G, Gupta B (2018) Secure integration of IoT and cloud computing. Futur Gener Comput Syst 78:964–975.
[25] Pacheco PG, Prazeres C (2019) Web of things data visualization: from devices to web via fog and cloud computing. In: 2019 IEEE 28th international conference on enabling technologies: infrastructure for collaborative enterprises (WETICE). IEEE, pp 140–145.
[26] Gregory BE, Chao J (2020) Recovery strategy for a stream processing system. U.S. Patent Application 16/793, 936. Filed 11 Jun 2020.
[27] Hosuk L-M (2018) Stealing thunder: cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness? No. 2/18. ECIPE Occasional Paper.
[28] Gunaseelan JSK, Ellappan V (2017) IOT agriculture to improve food and farming technology. In: 2017 conference on emerging devices and smart systems (ICEDSS). IEEE, pp 260–266.
[29] https://venturebeat.com/2015/09/15/salesforce-launches-iotcloud-to-let-business-users act-on-big-data/. Accessed 24 Nov 2020.
[30] Jeet KM, Riaz S, Mushtaq A (2020) Cyber-physical cloud computing systems and internet of everything. In: Principles of internet of things (IoT) ecosystem: insight paradigm. Cham: Springer, pp 201–227.
[31] Ali LA, He H, Memon KA, Laghari RA, Halepoto IA, Khan A (2019) Quality of experience (QoE) in cloud gaming models: a review Multiagent Grid Syste 5(3):289–304.
[32] Farshad F, Farahani B (2020) Architecting IoT Cloud. Intel internet things. Cham: Springer, pp 173–241.
[33] Ali LA, He H, Shafiq M, Khan A (2016) Assessing effect of cloud distance on end user's quality of experience (QoE). In: 2016 2nd IEEE international conference on computer and communications (ICCC). IEEE, pp 500–505.
[34] Vishal K, Laghari AA, Karim S, Shakir M, Brohi AA (2019) Comparison of fog computing and cloud computing. Int J Math Sci Comput (IJMSC) 5(1):31–41.
[35] Adeel A, Deng Z, Memon KA, Laghari AA, Mohammadani KH (2019) A dynamic application-partitioning algorithm with improved offloading mechanism for fog cloud networks. Future Internet 11(7):141.
[36] Puliafito C, Mingozzi E, Longo F, Puliafito A, Rana O (2019) Fog computing for the internet of things: a survey. ACM Trans Internet Technol (TOIT) 19(2):1–41.
[37] Hina M, Lei LH, Laghari AA, Karim S (2020) Quality of Experience and quality of service of gaming services in fog computing. In: Proceedings of the 2020 4th international conference on management engineering, software engineering and service sciences. pp 225–228.
[38] Mohit T, Davy A (2017) Resource aware placement of IoT application modules in fog cloud computing paradigm. In: 2017 IFIP/ IEEE symposium on integrated network and service management (IM). IEEE, pp 1222–1228.
[39] Ali LA, Jumani AK, Laghari RA (2021) Review and state of art of fog computing. Arch Comput Method Eng 1–13.
[40] Amir MR, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P (2018) Exploiting smart e-Health gateways at the edge of healthcare internet-of-things: a fog computing approach. Futur Gener Comput Syst 78:641–658.
[41] Bryan FC, Foltz L (2020) Mobile users' information privacy concerns instrument and IoT. Inf Comput Security.
[42] Prabhjot S (2018) Cross-layer design for internet of things (IOT)- issues and possible solutions. Dep Syst Comput Eng 1–10.
[43] Vidya R, Prema KV (2019) Light-weight hashing method for user authentication in internet-of-things. Ad Hoc Netw 89:97–106.
[44] Mfanasibili N, Ngoepe M (2020) A framework for data security, privacy, and trust in "consumer internet of things"

assemblages in South Africa. Secur Priv e122.
[45] Christopher R, Toft J (2019) Finding vulnerabilities in IoT devices: ethical hacking of electronic locks.
[46] Guilin Z, Xing L (2020) Reliability analysis of IoT systems with competitions from cascading probabilistic function dependence. Reliab Eng Syst Saf 106812.
[47] An C, Celimuge W (2020) Traffic big data assisted V2X communications toward smart transportation. Wirel Netw 26(3):1601–1610
[48] Paolo F, Flammini A, Sisinni E, Rinaldi S, Brandão D, Rocha MS (2018) Delay estimation of industrial IoT applications based on messaging protocols. IEEE Trans Instr Measur 67(9):2188–2199.
[49] Zhang P, Zhou M, Fortino G (2018) Security and trust issues in Fog computing: a survey. Futur Gener Comput Syst 88:16–27.
[50] Gu K, Na W, Yin B, Jia W (2019) Secure data query framework for cloud and fog computing. IEEE Trans Netw Serv Manag 17(1):332–345.
[51] Shikhar V, Kawamoto Y, Fadlullah ZM, Nishiyama H, Kato N (2017) A survey on network methodologies for real-time analytics of massive IoT data and open research issues. IEEE Commun Surv Tut 19(3):1457–1477.
[52] Ali LA, He H, Shafq M, Khan A (2019) Application of quality of experience in networked services: review, trend and perspectives. Syst Pract Act Res 32(5):501–519.
[53] Redowan M, Srirama SN, Ramamohanarao K, Buyya R (2019) Quality of experience (QoE)-aware placement of applications in Fog computing environments. J Parallel Distrib Comput 132:190–203.
[54] Ali LA, Memon KA, Soomro MB, Laghari RA, Kumar V (2020) Quality of experience (QoE) assessment of games on workstations and mobile. Entertain Comput 100362.