

Comparative study among constrained application protocol extensible messaging and presence protocol of IoT

Abdal Motalib Misbah Alshrif, Ashraf A. Gouda, Mohammed Abdel Razek

Department of Mathematics and Computer Science, Faculty of Science, Al-Azhar University, Nasr City, Egypt

Article Info

Article history:

Received Oct 18, 2021

Revised May 30, 2022

Accepted Jun 9, 2022

Keywords:

CoAP

IoT

MQTT

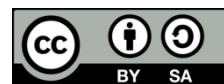
Protocols

XMPP

ABSTRACT

Many specialists are now looking for ways for commercial development and the introduction of technology and internet applications, especially since many homes in smart and developed cities need a great degree of fitness and electrical control. Now, days the internet of things shows a most important potential for commercial development in certain sectors. Therefore, this paper came with the aim of revealing a large variety of constantly evolving protocols for the internet of thing network design in particular three of these are constrained protocols such as message queuing telemetry transfer, application protocol message protocol extended, and message queuing telemetry transfer. To achieve this, the researcher used and followed the qualitative approach that relies on survey tools and theoretical presentation. Among the results obtained that: message queuing telemetry transfer is the best protocol among the three types as it has a high degree of reliability using supportive service quality levels and characterized by the use of neutral packets. The information may also contain binary or text content and has a superior transmission mechanism with efficiencies such as one-to-one, many-to-many or one-to-nothing. In addition, and for ease he uses easy-to-state strategies.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Abdal Motalib Misbah Alshrif

Department of Mathematics and Computer Science, Faculty of Science, Al-Azhar University

Nasr City, Cairo 11884, Egypt

Email: motalib.shrif@gmail.com

1. INTRODUCTION

The internet of things (IoT) is an essential technology today, it is an internet integrated of integrated devices or computers, mechanical and virtual machines, items, people, or animals which might be equipped with exclusive identifiers and ability of transporting built information over the community with not require building person-to-person or person-to-laptop communication [1], [2] An issue in IoT may be someone with a heart display implant, animals in a farm with a biochip bouquet, and car which are having sensors in order to alert the driving force whilst tire stability integrated is low or another herbal or guy-made item which is able to be allocated with IP protocol and is capable of transferring records over a network [2]. And it is noted that IoT has a special mechanic of work as an IoT surround built integrated involves integrated built integrated-enabled smart gadgets that utilize embedded structures, internet integrated sensors, processors, and communicate hardware, to accumulate, send and work on internet collected by them from their environments [3]. Devices of IoT share the sensor internet they gather through connect integrated to a gateway or other facet device internet fact is either sent to cloud in order to be analyzed or being analyzed regionally. Every so often, those gadgets communicate with different associated devices and work on the statistics which they get from each other [4]. Devices do most of the paintings without integrated intervention of human, although

humans can internet have built integrated with devices integrated, to nominate them, supply them built instructions integrated or get admission to the built information [5].

Networking integrated, connectivity, and verbal exchange protocols utilized with these built integrated-enabled devices broadly integrated rely on specific IoT packages deployed [5]. IoT may also make utilization of artificial integrated intelligence (AI) and Mach built integrated building to resource integrated abuilding statistics internet integrated approaches simpler and extra dynamic [6].

One of the big problems in IoT application is that it needs a huge number of sensors and gates that are deployed and interconnected, so that these sensors in new environments and smart cities can receive the physical environments and send data to the receiving gate. So, protocols are needed that can precisely select the application type. This type is identified with security, fault tolerance, performance, and interoperability. So, statement can be formulated in the main question "what is the best IoT Protocols in the theoretical level of the IoT network design?"

2. METHOD

The researcher follows the qualitative approach that depends on the survey of a group of scientific studies published in books and scientific journals, then the researcher followed the comparative approach in order to make comparisons between the four types and highlight the advantages and disadvantages of each protocol and then draw the results and discussion. Following MIT Professor Neil Gerstenfeld's book, it didn't utilize precise item, just furnished a bright and obvious vision of the IoT internet integrated headed [5].

Kevin Ashton, who are a co-founder of the car-identity middle at the Institute of Massachusetts of generation (MIT), first cited the building internet integrated [7]. The integration was to convey radio frequency identification (RFID) to eye of senior management of P&G's, Ashton named his presentation "internet integrated" to internet the new fashion of 1999: the built internet integrated. IoT has consisted of the wireless technology merging, micro electromechanical systems (MEMSes), micro services and internet [8]. The merging has improved the silos among built-information era and operational technology. It enables shapeless system-generated built-information for investigating the enhancements [5]. Even though Ashton's became the first mention of the IoT, the ideas of the connected devices have been around forming the Seventies, beneath the Nicknames embedded on the internet and pervasive computing [9].

The first equipment of internet, built instance, become a Coke device at university of Carnegie Mellon integrated early in 1980s. The use of the web, programmers should test the fame of match internet and internet whether there might be a cold rebuilt-ink built-in integrated them, need to they internet to make the journey to the integrated [10].

IoT advanced from machine-to-machine (M2M) conversation, IoT is only sensor in network (one of million smart small devices that help in connecting people [11]. M2M means a connecting tool to cloud, which manages and collect the data. When taking M2M to its following stage, IoT is said to be a sensor community of billions of smart devices that joint systems, humans, and other applications to gather data and share it. According to its basis, M2M gives the connectivity which allows IoT [12].

The IoT factors is also the natural protraction of the supervisory manage and internet conquest (SCADA), a software application packages category for procedure manages, integrated of facts from distant places to control the equipment and the conditions. SCADA systems consist of software program additives and hardware [13]. The hardware collects and feeds-built information right into the laptop which has software of SCADA built-in [14], [15]. The SCADA evolution is that past due-era SCADA structures evolved built-into the first technology IoT structures [10].

3. ARCHITECTURE OF IOT

3.1. Three-layer construction

This architecture contains three layers [3], [5]: Perception, Network, and Application layers [16] i) Perception layer involves sensors to sense and gather information from its ecosystem. It perceives and identifies smart things and other parameters in the environment, ii) Network layers connect devices with servers and smart things. They have features that transmit and process sensor data [17], and iii) Application layer provides users with application-specific services [18]. It identifies the various applications such as smart health and smart homes [12]. Figure 1 show the most main architecture of three-layers.

3.2. Five-layer architecture

Figure 2 shows the five-layers architecture contains belief, processing, transport, utility, and layers of business. The function of this layer is like perception and application layers [19]. As follows, the three layers are defined [13]. The delivery layer transmits the data from one layer called notion to another called processing and contrariwise across 4G, RFID, LAN, WIFI, or Bluetooth [20].

Middleware layer is another name-processing layer. This layer houses, evaluates, and processes huge sums of data resulted from delivery layer [21]. It might use and present a several set of facilities to reduce layers. It utilizes several tools simultaneously with cloud computing and databases [22]. The business layer runs the complete IoT gadget, which includes packages, enterprise and profit models, and user's privateness [23]. The layer of business is out of this paper's scope. As a result, we do now not discuss it in addition [24].

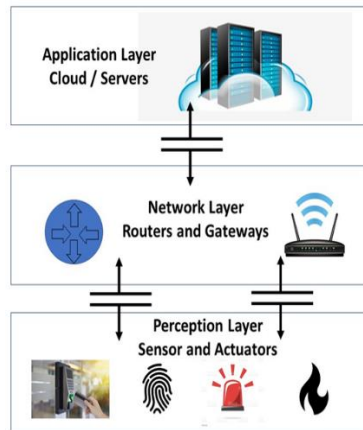


Figure 1. Three-layer IoT architecture

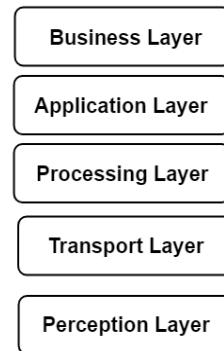


Figure 2. Five-layer IoT architecture

3.3. Conceptual architectures of IoT

The conceptual architectures concept of IoT consists of the real world, the information world, and the links between these two worlds. The real world builds a pervasive, mobile, community-computing environment consisting of sum of physical objects such as sensors, and devices. Each of which may have diverse computing capabilities. The world of information is made up of a set of virtual objects designated (or aggregated from) physical objects. The organization of societies scattered across the real world. The information can be managed through a community collaboration model or a member collaboration model. IoT infrastructure can be a platform for the network of things. Or a network of organisms for scattered communities.

Nowadays a fundamental transformation resulted from Industry 4.0 leads manufacturing processes through the interaction of the overall business systems [25]. Industry 4.0 continues playing an important role for several industrial businesses. Its reference book remains gradually being implemented in different areas to drive technologists on in what way their systems communicate with others. Enterprises take also experimented with various reference book constructions for Industry 4.0. However, there is no full sense of the current structures Industry 4.0 [26].

3.4. IoT protocols

IoT conventions are a critical piece of the IoT invention mound without them, outfit would be delivered futile as the IoT conventions empower it to trade information in an systematized and significant manner. Out of these moved bits of information, helpful data can be removed for the end customer and gratefulness to it, the entire association turns out to be monetarily salutary, particularly regarding IoT contrivance the directors [13].

When agitating the Internet of Things, we generally consider correspondence [27]. Collaboration between detectors, widgets, doors, workers, and customer apps is the core brand that makes the Internet of Things the way it is. Still, what empowers so important shrewd stuff to talk, and associate are the IoT conventions that can be viewed as cants that the IoT gear utilizes to conduct [14].

Anusha *et al*, [6]. manage the multitudinous data protocols extensible messaging and presence protocol (XMPP), constrained application protocol (CoAP), advanced message queuing protocol (AMQP), message queuing telemetry transport (MQTT), data distribution service (DDS) and message queuing telemetry transport-sensor node (MQTT-SN) in the conception of the IoT. Authors purpose a comparison between the capability of each information protocol and contrary records protocols with reference to criteria of performance like packet loss price, bandwidth input, communication length, and quiescence. Every protocol's overall performance is estimated according to the mileage. Except, XMPP as it has advanced

performance issues due to its extensible markup language (XML) stanza grounded completely transmitting for incontinently communicating packages over the internet [27].

Bandyopadhyay *et al.*, [7] intention to decide which protocol is lesser proper for unique app regions with defined bias by means of assessing CoAP and XMPP. Android O/S and Intel X86 structures are employed to perform protocol's opinions. The technologies of software for the perpetration are "LabCorp" library for CoAP and "Mosquito" task for MQTT [27]. Also, Wireshark is employed for assaying the network point callers. Protocols are being compared in the terms of consumption of power, bandwidth operation, and reliability. Harmonious with the consequences, CoAP is better than MQTT with reference to optimize power application.

Chen *et al.*, [8] carry out an Inclusive check in order to estimate performances of CoAP, MQTT, DDS and a custom UDP-primarily according to protocol in scientific operation of monitoring by means of addressing the quiescence, bandwidth consumption and packet loss criteria on a real-time data that's amassed from cases. Also, they make clear how the protocols carry out their functions underneath a limited, low satisfactory Wi-Fi network [28]. Tackle technologies are Raspberry Pi version 2, Arduino Uno modification three and home windows laptop ASUS ZenBook. The technologies of software program for perpetration are "Californium CoAP" for CoAP server and client), "Hive MQ" for MQTT sever perpetration, "Mosquito" for broker and MQTT guests (each subscriber and publisher), "OpenDDS" for DDS server and purchaser. Protocols' Performances are anatomized with "TBF", "NetEM" and "Wireshark" equipment. Overall performance issues induce that both TCP- based completely protocols (DDS and MQTT) are more dependable than UDP- primarily based protocols (custom-UDP and CoAP) in low great Wi-Fi networks. However, TCP- based completely protocols have lesser quiescence than UDP-based completely protocols in the equal network situation. Further, DDS performs advanced than MQTT in situations of poor network [28].

Thangavel *et al.*, [9] examine and estimate the performances of protocols of MQTT and according to packet- loss, retransmitting dispatches defer, data transferred in step with communication. Authors particularly concentrate on the transmission of records between the detectors on the knot of the gateway to the returned- end server for CoAP or broking for MQTT [29]. A pc as a server, a BeagleBoard- xM for the perpetration of middleware and a netbook for huge position community (WAN) impersonator are employed as the tackle- technologies. The software program technology is "Wanem" (the wide location community emulator) to switch messages, "Mosquito" assignment for MQTT dealer, "libcoap" library for CoAP and "Wireshark" in order to measure the metrics [30]. Results induce that communication of MQTT have lower detainments than CoAP for drop packet loss. On the different hand, MQTT has better detainments than CoAP for better packet loss [31]. Also, CoAP has much lower callers while communication length is lower and packet loss figure is much lower [32].

4. CRITICAL ANALYSIS

While current Internet frame is uninhibitedly accessible and applicable for any IoT contrivance, it regularly demonstrates exorbitantly weighty and power-burning-through for most IoT application cases. Established by the IETF Constrained peaceful surroundings working gathering and dispatched in 2013, constrained application protocol (CoAP) was intended to interpret the HTTP model with the thing that it veritably well may be employed in prohibitive contrivance and association conditions [15].

4.1. Constrained application protocol (COAP)

Intended to introduce the requirements of HTTP-based IoT frameworks, CoAP depends on the user datagram protocol (UDP) for building up secure correspondence among endpoints. By taking into consideration multicasting and broadcasting, UDP can send information to numerous hosts while holding correspondence speed and low data transmission use, which makes it a decent counterpart for remote organizations ordinarily utilized in asset obliged M2M conditions. Something else that CoAP imparts to HTTP is the Restful design that upholds a solicitation/reaction cooperation model between application endpoints. Additionally, CoAP receives the essential HTTP get, post, put and erase strategies, on account of which vagueness can be kept away from at the hour of communication between customers, as shown in Figure 3.

CoAP highlights Service Quality that is utilized to control the messages sent and imprint them as 'confirmable' or 'non conformable' likewise which demonstrates whether the beneficiary should return an 'ack' or not. Other fascinating highlights of CoAP are that it upholds content arrangement and asset disclosure system. Aside from moving IoT information, CoAP use datagram transport layer security (DTLS) for the safe trade of messages in the vehicle layer. CoAP completely addresses the necessities of an incredibly light convention to satisfy the needs of battery-worked or low-energy gadgets. With everything considered, CoAP is a decent match with regards to the existing web administration based IoT frameworks [33].

4.2. Message queuing telemetry transport (MQTT)

Presumably the most generally embraced standard in the Industrial IoT to date, Message Queuing Telemetry Transport is a lightweight distribution/membership type (pub/sub) informing convention, as can be seen in intended for battery-controlled gadgets, MQTT's design is basic and lightweight, giving low force utilization to gadgets. Chipping away at top of TCP/IP convention, it has been particularly intended for inconsistent correspondence networks to react to the issue of the developing number of little estimated modest low-power protests that showed up in the organization in the New Year's [34], see Figure 4.

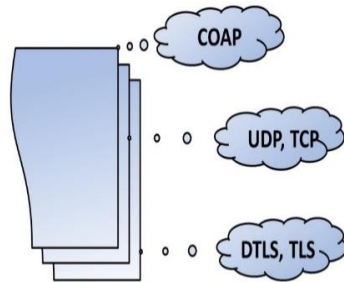


Figure 3. IoT Standards and protocols guide protocols of the Internet of Things

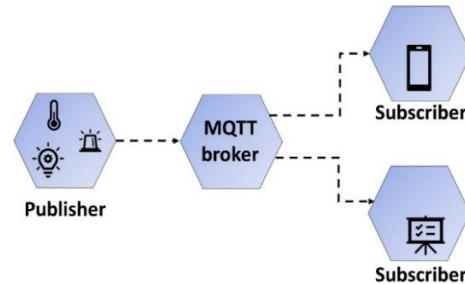


Figure 4. MQTT architecture

MQTT depends on supporter, distributor, and dealer model. Inside the model, the distributor's undertaking is to gather the information and send data to endorsers through the intercession layer which is the agent. The part of the merchant, then again, is to guarantee security through cross-checking the distributors' and supporters' authorization [35]. MQTT offers three methods of accomplishing this (Service Quality), on account of that the distributor has the likelihood to characterize the nature of its message: (i) QoS0 (At most once): The most un-dependable mode yet in addition the quickest. The distribution is sent however affirmation isn't gotten, (ii) QoS1 (At least once): Ensures that the message is conveyed in any event once, however copies might be gotten. (iii) QoS2 (Exactly once): The most dependable mode while the most data transfer capacity burning-through. Copies are controlled to guarantee that the message is conveyed just a single time. Having discovered large width of application in such IoT gadgets as electric meters, vehicles, finders, and modern or sterile gear, MQTT reacts well to the accompanying necessities [17], [36] (i) Minimum data transmission use, (i) Operation over remote organizations, (i) Low energy utilization, (i) Good dependability if vital and (i) Little handling and memory assets.

Despite its attributes, MQTT can be hazardous for some prohibitive gadgets, because of the reality of the messages' transmission over TCP and overseeing long subject names, as shown in Figure 5. That is tackled with MQTT-SN variation that utilizes UDP and supports point name ordering. Be that as it may, notwithstanding its wide selection, MQTT does not uphold a very much characterized information portrayal and gadget the board structure model, which delivers the execution of its information the executives and gadget the executives' abilities completely stage or merchant explicit [37].

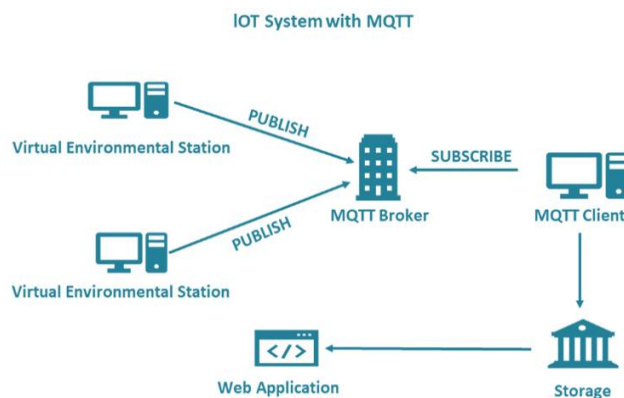


Figure 5. MQTT with IoT system

4.3. Extensible messaging and presence protocol (XMPP)

Created in 1999 by the Jabber open-source local area and initially implied for constant informing, this correspondence IoT convention for message-arranged middleware depends on the XML language. It considers ongoing trade of organized however extensible information between at least two organization customers [17], [38]. Since its initiation, XMPP has been generally applied as a correspondence’s convention. Over the long run and with the rise of a lightweight XMPP particular: XMPP-IoT, it has proceeded to be utilized with regards to the IoT. Being an open local area upheld standard, XMPP IoT’s qualities are tending to and adaptability capacities, that makes it ideal for customer arranged IoT organizations [39].

Among the downsides of utilizing XMPP in IoT correspondence, it ought to be noticed that it offers neither Service Quality nor start to finish encryption. Because of these impediments, among others, it is anticipated which its application inside IoT will remain approximately associated with the business, as the convention certainly will not turn into a standard utilized day-in outing for the reasons for information trade and the executives of asset compelled gadgets, similarly as MQTT or LwM2M are. Table 1 shows a comparison between IoT protocols. In Figure 6, we can see that The XMPP protocol used between XMPP client and XMPP server for communication is depicted [39].

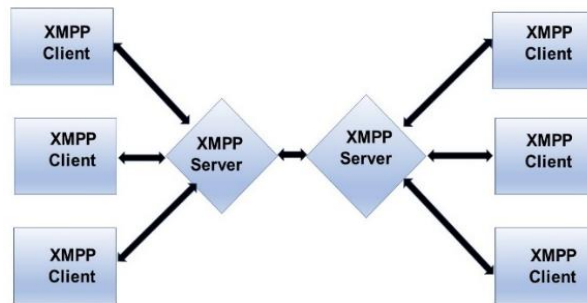


Figure 6. XMPP protocol used between XMPP client and XMPP server for communication

Table 1. Comparison between IoT protocols

Protocol	Advantages	Disadvantages
COAP	Operates fast advertisement by means of transferring small packets with UDP subcaste. Asynchronous discussion is supplied. Person-to-Person communication does not want to the intermediate server among customers. Aalso, numerous-to- numerous verbal exchanges is supported [42]. DTLS presents privacy, safety, and integrity with the aid of approving cracking and securing. Applicable volition designed for defined items [43]-[45].	Dispatches are unreliable thus, ACK (acknowledgement) packets are dispatched to affirm the communication arrives [40], [41]. But it does now not show actually whether those dispatches are decrypted successfully or absolutely. It follows up the criteria. It's named the most unstandardized protocol among different protocols [11].
MQTT	Offerings trustability of dispatches by using supporting QoS categories. Successfully makes use of bandwidth thru packet agnostic. The information can also cover double or textual content. Submit instrument takes capabilities like 1-to-1, numerous-to- numerous or one-to-none. Also, this way provides bi-way connections [47]. Develop easy strategies used for communicate. Asynchronous communication amongst nodes. Communications can put up every time [45].	The protocol such as TCP calls for redundant discussion bents in discrepancy to UDP [46]. Broker has constrained ability for verbal exchange. All nodes are associated to agent. Accordingly, the advertisement breakdowns while the broking is a disappointment [48].
XMPP	It is far flexible several hosting servers which offer continued advertisement. It provides advertisement among patron-patron, MVP server web architecture. The presence index gives lesser options to the messaging. It provides extra redundant verbal exchange and contains TCP protocol [11].	The server has restricted capability for verbal exchange [49]. The authorization takes plenty time at the same time as customers request get admission to the server [50]. The use of XML Stanzas in conversation reasons delays.

5. RESULTS AND DISCUSSION SECTION

The security is provided by COAP datagram transport layer security with the help of cryptographic authorization and security [51]. Still, the dispatches are not dependable. Thus, ACK (acknowledgment) packets are transferred to confirm the appearance of the communication. However, it now does not actually show whether these dispatches were successfully or absolutely deciphered. It is still invariant. It was chosen from the most non-standard protocols among the colorful protocols. XMPP is a good type as multiple servers are highly scalable and adaptable offering seamless communication and supports manifest between payee-tenant, server-server-server but the server's ability to verbally exchange is limited, and delegation takes a long time at the same time clients are requesting access to the server [48].

MQTT is the stylish protocol among the three types as it has a high degree of trust ability using probative service quality situations, which uses neutral packets. The information may also contain binary or text content and has a superior transmission mechanism with efficiencies such as one-to-one, many-to-many or one-to-no Thing. In addition, he uses easy-to-state strategies.

6. CONCLUSION

This paper demonstrates a comparison study among IoTs protocols. The features and components of the study are principally needed for the IoT gadgets to gather environmental records in accurate time. The comparative study presents the overall performance criteria of XMPP protocol, CoAP, and MQTT. They compare them based on some performance criteria. It covers the differences of these protocols in an actual verbal exchange surroundings. The packet time is used to find the preface time, packet transport pace criteria to decide the differences in the detention in the actual time communication. The results of the compression present that MQTT shows a considerable performance in the time of transmission than different protocols. However, CoAP presents a respectable transition like UDP-primarily grounded protocol. Furthermore, there are a considerable response in MQTT over CoAP. Overall, the performance of MQTT is better than others because of several issues. These issues contain massive bandwidth and other packets. These packets are actuality switch to drop magnitude. At the same time, the COAP presents much lower integrated. The comparison shows that XMPP has reasons extra quiescence when it is compared with the other protocols. This quiescence is happened because it has a decelerating structure like XML stanza. Our work in the future will measure provided protocols to cover unique situations. The suggested situations include high collision fee, low bandwidth, and make bigger the surroundings to gather environmental non-stop records from distinct places.

REFERENCES




- [1] O. Vermesan *et al.*, *Internet of things strategic research roadmap*, vol. 1. 2011.
- [2] I. Peña-López, "The internet of things," *Economist (United Kingdom)*, 2015. [Online]. Available: <https://www.comminit.com/global/content/itu-internet-reports-2005-internet-things> (accessed Apr. 12, 2021).
- [3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.
- [4] C. Sun, "Application of RFID technology for logistics on internet of things," *AASRI Procedia*, vol. 1, pp. 106–111, 2012, doi: 10.1016/j.aasri.2012.06.019.
- [5] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," *Ad Hoc Networks*, vol. 28, pp. 68–90, May 2015, doi: 10.1016/j.adhoc.2014.12.006.
- [6] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.
- [7] O. Said and M. Masud, "Towards internet of things: Survey and future vision," *Int. J. Comput. Networks*, vol. 5, no. 1, pp. 1–17, 2013, [Online]. Available: <http://www.cscjournals.org/csc/manuscript/Journals/IJCN/volume5/Issue1/IJCN-265.pdf>
- [8] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Aug. 2010, pp. V5-484-V5-487. doi: 10.1109/ICACTE.2010.5579493.
- [9] M. Anusha, E. S. Babu, L. S. M. Reddy, A. V. Krishna, and B. Bhagyasree, "Performance analysis of data protocols of internet of things: A qualitative review," *Int. J. Pure Appl. Math.*, vol. 115, no. 6 Special Issue, 2017.
- [10] S. Bandyopadhyay and A. Bhattacharyya, "Lightweight internet protocols for web enablement of sensors using constrained gateway devices," in *2013 International Conference on Computing, Networking and Communications (ICNC)*, Jan. 2013, pp. 334–340. doi: 10.1109/ICNC.2013.6504105.
- [11] Y. Chen and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," in *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, Apr. 2016, pp. 1–7. doi: 10.1109/MoWNeT.2016.7496622.
- [12] D. Thangavel, X. Ma, A. Valera, H.-X. Tan, and C. K.-Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Apr. 2014, pp. 1–6. doi: 10.1109/ISSNIP.2014.6827678.
- [13] R. Lombreglia, "The internet of things," *Boston Globe*. Retrieved October 22, 2010. [Online]. Available: http://www.boston.com/news/globe/ideas/articles/2005/2007/2031/the_internet_of_things (accessed Jul. 31, 2005).

- [14] K. Michalakakis and G. Caridakis, "IoT contextual factors on healthcare," 2017, pp. 189–200. doi: 10.1007/978-3-319-57348-9_16.
- [15] M. L. Smith and K. M. A. Reilly, Eds., "Transparency and development: Ethical consumption through web 2.0 and the internet of things," in *Open Development*, The MIT Press, 2014. doi: 10.7551/mitpress/9724.003.0007.
- [16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
- [17] M. Gigli and S. Koo, "Internet of things: Services and applications categorization," *Adv. Internet Things*, vol. 01, no. 02, pp. 27–31, 2011, doi: 10.4236/ait.2011.12004.
- [18] "The internet of things," Geneva, 2005. [Online]. Available: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>
- [19] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan. 2006, doi: 10.1109/MPRV.2006.2.
- [20] B. Li and J. Yu, "Research and application on the smart home based on component technologies and internet of things," *Procedia Eng.*, vol. 15, pp. 2087–2092, 2011, doi: 10.1016/j.proeng.2011.08.390.
- [21] F. Razzak, "Spamming the internet of things: A possibility and its probable solution," *Procedia Comput. Sci.*, vol. 10, pp. 658–665, 2012, doi: 10.1016/j.procs.2012.06.084.
- [22] S. W and L. L, "Analysis of the development route of IoT in china," *PerkingChina Sci. Technol. Inf.*, vol. 2, no. 2, pp. 330–331, 2009.
- [23] D. Moeinfar, H. Shamsi, and F. Nafar, "Design and Implementation of a Low-Power Active RFID for Container Tracking at 2.4 GHz Frequency," *Adv. Internet Things*, vol. 02, no. 02, pp. 13–22, 2012, doi: 10.4236/ait.2012.22003.
- [24] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.
- [25] E. Trunzer *et al.*, "System architectures for industrie 4.0 applications," *Prod. Eng.*, vol. 13, no. 3–4, pp. 247–257, Jun. 2019, doi: 10.1007/s11740-019-00902-6.
- [26] K. Schweichhart, "Reference architectural model industrie 4.0 (RAMI 4.0)," 2018. [On;ine]. Available: https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4_0_rami_4_0.pdf
- [27] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
- [28] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," 2019, pp. 27–51. doi: 10.1007/978-3-030-04203-5_3.
- [29] J. Saqlain, "IoT and 5G: History evolution and its architecture their compatibility and future," Subtitle Metropolia University of Applied Sciences, 2018.
- [30] A. Ravulavaru, "Enterprise internet of things handbook: Build end-to-end IoT solutions using popular IoT platforms," 2018.
- [31] E. Irmak and M. Bozdal, "Internet of things (IoT): the most up-to-date challenges, architectures, emerging trends and potential opportunities," *Int. J. Comput. Appl.*, vol. 179, no. 40, 2018.
- [32] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, Nov. 2014, pp. 1–8. doi: 10.1109/ICSEMR.2014.7043637.
- [33] M. Ullah, P. H. J. Nardelli, A. Wolff, and K. Smolander, "Twenty-one key factors to choose an IoT platform: theoretical framework and its applications," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10111–10119, Oct. 2020, doi: 10.1109/IJOT.2020.3000056.
- [34] R. Duan, X. Chen, and T. Xing, "A QoS architecture for IOT," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, Oct. 2011, pp. 717–720. doi: 10.1109/Things/CPSCom.2011.125.
- [35] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: taxonomy, challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, Aug. 2021, doi: 10.3390/su13169463.
- [36] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Aug. 2010, pp. V5-484-V5-487. doi: 10.1109/ICACTE.2010.5579493.
- [37] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the IOT architecture and gateway technology," in *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, Aug. 2015, pp. 196–199. doi: 10.1109/DCABES.2015.56.
- [38] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb. 2017, pp. 477–480. doi: 10.1109/I-SMAC.2017.8058395.
- [39] N. M. Kumar and P. K. Mallick, "The internet of things: insights into the building blocks, component interactions, and architecture layers," *Procedia Comput. Sci.*, vol. 132, pp. 109–117, 2018, doi: 10.1016/j.procs.2018.05.170.
- [40] S. Zamfir, T. Balan, I. Iliescu, and F. Sandu, "A security analysis on standard IoT protocols," in *2016 International Conference on Applied and Theoretical Electricity (ICATE)*, Oct. 2016, pp. 1–6. doi: 10.1109/ICATE.2016.7754665.
- [41] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Mar. 2016, pp. 1–7. doi: 10.1109/ICBDSC.2016.7460363.
- [42] I. Lee, "The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model," *Internet of Things*, vol. 7, p. 100078, Sep. 2019, doi: 10.1016/j.iot.2019.100078.
- [43] H. Muccini and M. T. Moghaddam, "IoT architectural styles," 2018, pp. 68–85. doi: 10.1007/978-3-030-00761-4_5.
- [44] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *J. Netw. Comput. Appl.*, vol. 169, p. 102763, Nov. 2020, doi: 10.1016/j.jnca.2020.102763.
- [45] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb. 2017, pp. 492–496. doi: 10.1109/I-SMAC.2017.8058399.
- [46] A. Kondoro, I. Ben Dhaou, H. Tenhunen, and N. Mvungi, "Real time performance analysis of secure IoT protocols for microgrid communication," *Futur. Gener. Comput. Syst.*, vol. 116, pp. 1–12, Mar. 2021, doi: 10.1016/j.future.2020.09.031.
- [47] R. P. Kumar and S. Smys, "A novel report on architecture, protocols and applications in internet of things (IoT)," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Jan. 2018, pp. 1156–1161. doi: 10.1109/ICISC.2018.8398986.




- [48] L. Mainetti, L. Patrono, M. L. Stefanizzi, and R. Vergallo, "A smart parking system based on IoT protocols and emerging enabling technologies," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec. 2015, pp. 764–769. doi: 10.1109/WF-IoT.2015.7389150.
- [49] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (IoT) communication protocols: review," in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690. doi: 10.1109/ICITECH.2017.8079928.
- [50] B. B. Gupta and M. Quamara, "An overview of internet of things (IoT): architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, Nov. 2020, doi: 10.1002/cpe.4946.
- [51] P. Datta and B. Sharma, "A survey on IoT architectures, protocols, security and smart city based applications," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2017, pp. 1–5. doi: 10.1109/ICCCNT.2017.8203943.

BIOGRAPHIES OF AUTHORS






Mr. Abdal Motalib Misbah Alshrif    is M. Sc student of computer science at Azhar university Egypt. He has been granted the B. Sc degree in computer science with major field in networking academy Cisco from higher institute of sciences. Gharian-Libya, he also holds training in unix and oracal in Egypt at 2007. He can be contacted at email: motalib.shrif@gmail.com.



Ashraf A. Gouda    received the B.Sc. in Computer Science from Zagazig University, Egypt, M.Sc. degree in Mathematical Statistics from Al-Azhar University, Cairo, Egypt and the Ph.D. degree in Mathematics and Computer Science from Budapest University of Technology and Economics (Doctoral School of Mathematics and Computer Science), Budapest, Hungary. He has been a assistance professor of Computer Science with Al-Azhar University. His research interests include, artificial intelligence, machine learning, quantum machine learning, neural networks and quantum neural networks, Internet of things, rare event Simulation and computational of multivariate probability distributions, applied probability, PERT Modeling and optimization techniques. He can be contacted at email: gouda@azhar.edu.eg.



Dr. Mohammed Abdel Razek    is a Professor of Computer Science at Azhar University. He holds a Ph.D. in Computer Science - Artificial Intelligence – from University of Montreal, Canada in 2004. His research focuses on the design of a new application using artificial intelligence techniques on E-learning, Medicine, Cybersecurity, Internet of Thing, and others. He has more than 80 papers published in international journals and Conferences. He serves as an editor member for many Journals and as a reviewer of many international conferences. As a postdoctoral fellow at NSERC, Canada, He had worked in creating intelligent signing system to manipulate a huge database containing customers' purchases at Retail Company. He has been added to Who is Who in the world in 2009. He can be contacted at email: abdelram@azhar.edu.eg.