IJIT

by Sanket Chauhan

Submission date: 11-Mar-2022 09:58AM (UTC+0530)
Submission ID: 1781661612
File name: IJIT_-_Paper_4.docx (205.6K)
Word count: 2635
Character count: 14775

Abstract

This vast estate of sensors, devices, and systems will be developed and deployed alongside a wide, diverse, and innovative range of M2M and IoT applications, including personal applications, health monitoring solutions, construction site surveillance systems, smart meters, automobiles connected. , remote monitoring solutions for industrial and agricultural equipment, just to name a few. Each of these applications will perform specific and detailed tasks defined by users.

The ability to connect and manage devices in a resilient and scalable way is critical to M2M and many IoT solutions and a range of different types of platforms have emerged to help with this effort. Device management platforms typically manage M2M devices deployed by a single device vendor, ensuring the correct drivers are used to connect across multiple networks and manage the firmware and software requirements of connected devices. Connectivity support platforms, which are currently primarily mobile-centric, enable and manage SIM startup, configuration, and activation tasks. These platforms ensure that connectivity paths are managed and monitored and provide some additional tools such as real-time connectivity status, reporting, troubleshooting, and, in a mobile environment, SIM request and profile creation. As the support required by connected M2M devices becomes more standardized, the role of device management platforms is increasingly integrated into service enablement platforms. These connectivity support platforms will become critical as new and alternative connectivity technologies. M2M and IoT solutions bring together complex directivity, applications, and data management processes.

Keywords: *Devices transferring data, Connectivity Platform, M2M and IoT Solutions, Automotive industry, Emergence of the IoT*

1. Introduction

By addressing the M2M requirements of vertical industries, the design, development, and implementation of M2M solutions can be compared to complex IT solutions. Using connectivity support platforms allows companies to standardize connectivity management and extend functionality within solutions. The current limitation is that in very few cases, connectivity support platforms have been designed to be flexible or adaptable concerning different connection technologies. Once applications are developed, it takes a lot of time, effort, and money to change devices, add connectivity technologies, or adopt and integrate new application requirements with new data models. [1][2] This typically leads to multiple purpose-built solutions with limited reuse or integration of connectivity support platform features.

We have already seen a similar trend in application development where abstraction has become the approach of choice for the emerging range of M2M / IoT application platforms. We expect similar developments in the connectivity support platform space characterized by growing technological agnosticism. This combination of abstraction and agnosticism allows you to manage the scale and protocols on fewer platforms and allows developers to focus more on application development than specific communications technologies or features of the device. Managing multiple connectivity technologies is a complex task. [3] Multi-technology connectivity platform providers are challenged to work with different protocols, manage multiple billing, real-time data, and reconciliation functions, and ensure secure and resilient communications across a wide range of communication technologies.

Scalability is not just about numbers, it also has to address the dimension of heterogeneity. In M2M and IoT, solutions will be increasingly generalized and diversified. Existing connections will face higher traffic and event loads, and perhaps more difficult, connected states of devices could be spread across an ever-growing range of communication technologies including cellular but also satellite, low-power geographic area, various fixed networks, and a variety of short-range networks. Ideally, managing this diversity of connectivity technologies will require more capacity of the connectivity platform.

2. Devices to Networks and Platforms

We are at a turning point right now. This is because the market between machines has become very fragmented over the last year, varying vertically, corporately, and geographically. Recently, along with technological advances, many efforts have been made to promote standardization, openness, and simplicity. The result is that standards are set and platforms built on

top of those standards. [1] This article discusses Ericsson's device connection platform, which gives an operator access to key features needed to manage M2M business connections, including device management, subscription management, and self-service. It also presents examples of different business models and applications with deployment scenarios.

2.1 Data Collection

In the world of IoT, we adopted the traditional SIM card as the identity because it was already there. However, the security of devices or things is changing. With the development of IoT markets and wireless technology standards, we are seeing the physical SIM card becoming more and more software-centric. This trend introduces new threats for ecosystem actors, such as SIM service providers, module manufacturers, OEMs, and mobile network operators (MNOs). [4]

Fig. 1 Sensor Analytics and Development of Smart Devices

Businesses that rely on IoT devices need to reassess key aspects of their operations to secure IoT operations.

Device credential storage: In this changing world, an IoT device or thing must provide secure data storage. Therefore, the credentials must be stored in the device storage or on special chips with the highest value security level.

Exchange of communications with external service providers: because the credentials are encrypted and exchanged over a mobile network with additional hardware monitor identification and authentication, Operating systems are more likely to be hacked, so the operator's profile remains open for quite some time they are threatened. [15] [16]

2.2 Data Communication

At the heart of IoT are data communication and the connectivity that enables it. The strength and continuity of this network, in which devices exchange information 24 hours a day, is as reliable as the MNO. Because SIM cards leave their way behind as a separate unit from the device module, companies can take advantage of end-to-end solutions, tighter integration between recorded data and module sharing, and a centralized platform, no matter where the module is placed and forwarded, the module stays connected. [4] As more and more devices enter the IoT network, mobile network operators will eventually get to the point where they cannot handle all the data traffic. As a result, businesses will experience operational delays, lost connections, and increased vulnerability to illegal monitoring, information retrieval, and the performance of hacked machines. [4] With the proliferation of vulnerable IoT devices and connected devices and the increasing volume of data exchange over unprotected mobile networks and the Internet, IoT security is a major concern.

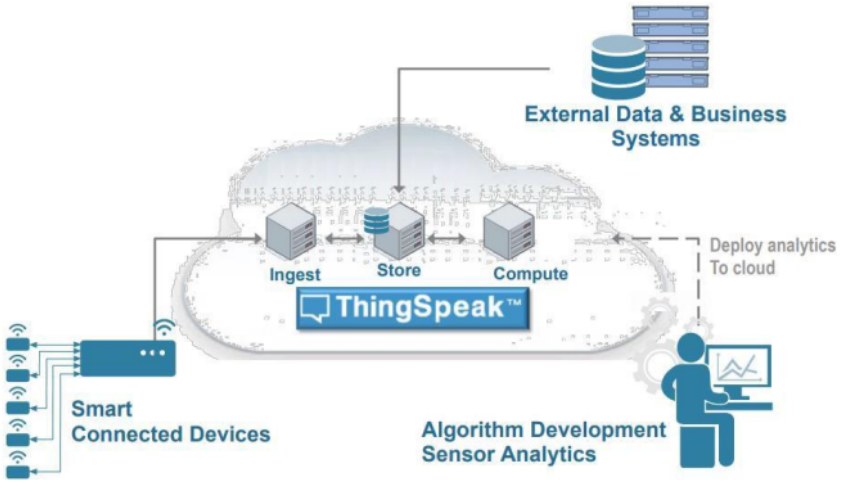

Fig. 2 Thing Speak for Small Scale Deployment

2.3 Strengthen the data management platform

In this case, the acquis communication is an important factor in the implementation of the IoT operational program, and the real benefits of this approach have been realized in the context of data and data on this platform. As soon as the platform is imported, the platform must be recycled and processed. [5] The platform is designed to be inverted, and IoT reverse charging is limited to the current infrared type. Data access control is based on data transmission, IoT output platform is based on data integration, validation, and data validation.

Centralized Device Management: Manage and secure devices once they are installed on-site, connected through a reliable wireless network, and allow remote operation. [5] Device management allows dynamic remote configuration, deployment, and firmware upgrades of installed IoT devices from a central location, all based on company-defined parameters.

High-performance data management: With advanced data encryption technology and a wide range of data collection, transport, storage, and delivery features, you can ensure the integrity and confidentiality of your intellectual property. [14]

Enhanced Administration and Security: Invest in comprehensive administration through a single, intuitive cloud management portal. Businesses can provide multiple levels of security to protect their data, devices, applications, and platform from external and internal cyber threats. In addition, they can manage authenticated access with role-based permissions for all user types and control how and when employees log on with intelligent session ID and timeout management. [6] [7]

Flexible Application Development: Innovate in multiple approaches to build dashboards, develop web and mobile applications, and integrate enterprise systems or cloud-based big data analytics to deliver data for flexible connectivity features and device management.

Table 1: M2M Application Characteristics and Analysis

M2M Application	Communication	Privacy	Obstruction	Energy consumption
Home Automation	Many to One (* to 1)	Low	Low	High
Smart Health Service	Many to One (* to 1)	High	High	High
Smart Grid	Many to One (* to 1)	High	High	Low
Smart City	One to Many (1 to *)	Low	High	High
Vending Machine	One to Many (1 to *)	High	Low	Low
Traffic Monitoring	Many to One (* to 1)	Low	High	High
Telemetry	Many to One (* to 1)	High	Low	Low

3. Data transfer with MQTT

Using MQTT, data is transmitted over TCP. Can be encrypted with SSL. The “publisher-subscriber” data transmission model is used. [7] This means that messages are exchanged using the MQTT broker. First, the client (a device or node) establishes a connection to the MQTT broker over TCP. Most commonly, port 1883 or port 8883 is used for the TLS connection. [13]

An MQTT broker is a central node that connects MQTT publishers to MQTT subscribers. MQTT publishers send messages and MQTT subscribers subscribe to receive messages. Several MQTT subscribers can belong to the same "subject". Messages are divided into “topics”; a device can "publish" a particular topic or "subscribe" to a topic. Within a topic, messages are exchanged when the MQTT broker receives them and then sends them to subscribing devices. A device can be both a publisher for some topics (publishes measured values) and a subscriber for other topics (responds to commands that control the output). [8]

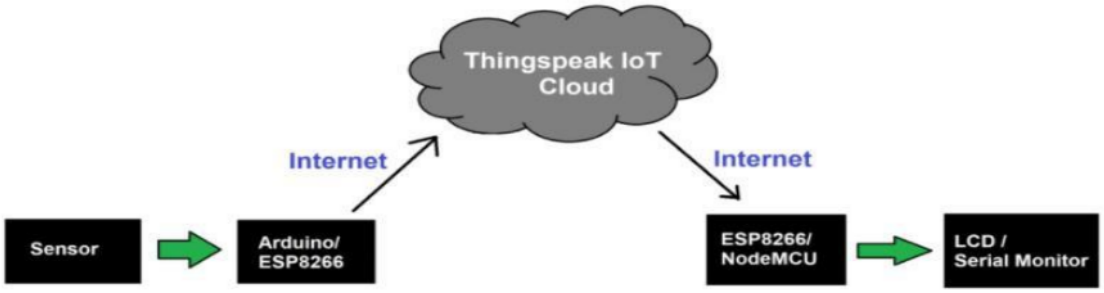

Fig. 3 Reading Data from Thing speak Block Diagram

3.1 Topic and Quality of Service (QoS)

In MQTT, this is recognizable content that acts as a filter for brokers when they send messages to all connected and subscribed clients. MQTT provides a quality service called QoS. This level delivers reliable messages. A level 0 message is sent only once. [9] Messages are sent based on network presence and no attempt is made to resend the message. Level 1 messages are sent at least once, so if the subscriber (acknowledgment) does not acknowledge the message, the forwarder sends a message to the publisher to get the acknowledgment status of the client message. Level 2 guarantees the receipt of the message. With this level, we can guarantee that the message is delivered reliably and duplication of sent messages is avoided. [8] [9]

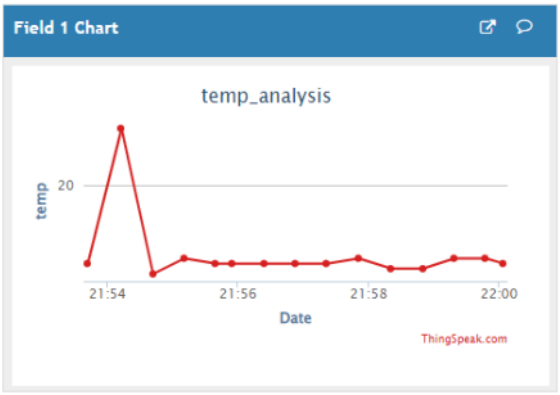

Fig. 4 Temp. Result Field 1

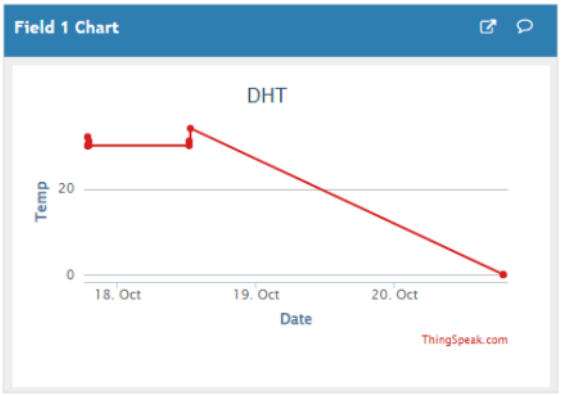

Fig. 5 DHT Result Field 1

The DHT11 sensor was connected to digital PIN 4 from UNO. The sensor read the temperature and humidity and then the (public) information was sent to the broker. The MQTT broker used in this study was a Mosquito, an open-source MQTT broker from the Eclipse product. [9] The data that was then entered into the broker was subscribed to by the client application. The List application was built to use Python, which can install an MQTT library called PAHO, an open-source application.

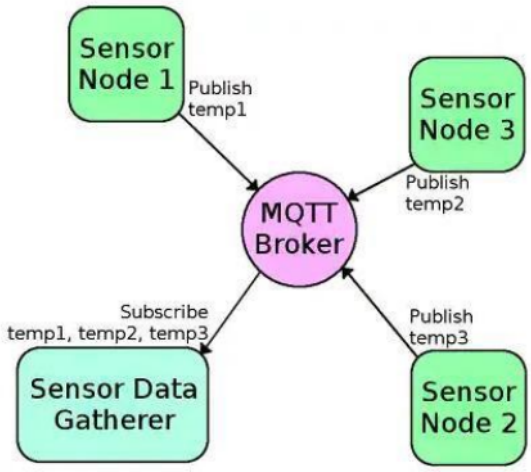

Fig. 6 MQTT Broker Integration

An integrated server that supports MQTT version 3.1.1 can act as an MQTT client that publishes content to an MQTT server and an MQTT client that subscribes to topics on the MQTT server. Specific:

The integrated server can publish MQTT messages to the MQTT server using the service pub.MQTT: integrated publication. [10]

The integration server can register themes by creating an MQTT activation. The MQTT trigger receives messages that are posted to the topic on the MQTT server and then calls an activation service to process the messages. [11]
The built-in server alias uses MQTT connections to connect to the MQTT server. The call is required at the pub.MQTT service: publish MQTT alias links to publish the message to the MQTT server. Similarly, MQTT activation specifies the MQTT connection alias, which it uses to identify the MQTT server from which it retrieves messages and from which activation activates a subscription. [11] [12]

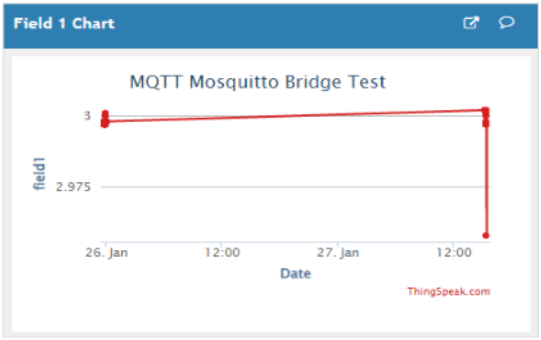

Fig. 7 MQTT Broker Result

4. Conclusion

Since the HTTP protocol requires a connection to be established whenever the connection overhead increases, this is not required for the MQTT protocol. Data sent using HTTP protocol is reliable because it is synchronous, but MQTT is not reliable in all situations. MQTT is an asynchronous protocol. The time it takes to send data using the MQTT protocol is fast compared to the HTTP protocol, which is useful for low-power IoT devices.

References

[1] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," IEEE Commun. Mag., vol. 49, no. 4, pp. 60–65, 2011.

[2] Yan Zhang, Rong Yu, Shengli Xie, Wenqing Yao, Yang Xiao, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," IEEE Commun. Mag., vol. 49, no. 4, pp. 44–52, 2011.

[3] D. B. Seo, C. S. Jeong, Y. B. Jeon, and K. H. Lee, "Cloud infrastructure for ubiquitous M2M and IoT environment mobile application," Cluster Comput., vol. 18, no. 2, pp. 599–608, 2015.

[4] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," 2016 IEEE Wirel. Commun. Netw. Conf. Work. WCNCW 2016, no. Wd5g, pp. 428–432, 2016.

[5] H. Li, D. Seed, B. Flynn, C. Mladin, and R. Di Girolamo, "Enabling Semantics in an M2M/IoT Service Delivery Platform," Proc. - 2016 IEEE 10th Int. Conf. Semant. Comput. ICSC 2016, pp. 206–213, 2016.

[6] Barros, J., Rodrighues, M.R.D., 2006. Secrecy Capacity of Wireless Channels, In: Proceeding of the IEEE International Symposium on Information Theory (ISIT 2006), Seattle, WA, 9-14 July 2006.

[7] Korner, C.I., Korner, J., 2002. Broadcast channels with confidential messages. IEEE Trans. Inf. Theory 24 (3), 339-348.

[8] Wyner, A.D., 1975. The wire-tap channel. Bell Syst. Tech. J. 54, 1355-1387.

[9] Fleisch, E., 2010. What is the internet of things? An economic perspective. Economy. Manage. Finance. Markets 2, 125-157.

[10] Floerkemeier, C., Roduner, C., Lampe, M., 2007. RFID application development with the academic middleware platform. IEEE Syst. J. 1 (2), 82-94.

[11] He, W., Xu, L., 2012. Integration of distributed enterprise applications: a survey. Hendricks, K.B., Singhal, V.R., Stratman, J.K., 2007. The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. J. Operat. Manage. 25 (1), 65-82.

[12] Hepp, M., Siorpaes, K., Bachlechner, D., 2007. Harvesting wiki consensus: using Wikipedia entries as vocabulary for knowledge management. IEEE Internet Compute. 11 (5), 54-65.

[13] Hernandez-Castro, J.C., Tapiador, J.M.E., Peris-Lopez, P., Li, T., Quisquater, J.-J., 2013. Cryptanalysis of the sasi ultra-lightweight RFID authentication protocol. arxiv.

[14] Sharma, P. and Padole, D.V., 2017, March. Design and implementation soil analyzer using IoT. In 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-5). IEEE.

[15] Ciuffoletti, A., 2017. OCCI-IoT: an API to deploy and operate an IoT infrastructure. IEEE Internet of Things Journal, 4(5), pp.1341-1348.

[16] Mois, G., Folea, S. and Sanislav, T., 2017. Analysis of three IoT-based wireless sensors for environmental monitoring. IEEE Transactions on Instrumentation and Measurement, 66(8), pp.2056-2064.

[17] Xu, Y., Mahendran, V., Guo, W. and Radhakrishnan, S., 2017, January. Fairness in fog networks: Achieving fair throughput performance in MQTT-based IoTs. In Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual (pp. 191-196). IEEE.

Sanket Chauhan is a Ph.D. scholar of Marwadi University, Rajkot, Gujarat. He obtained his Master's degree in Computer Application at CHARUSAT University, Changa. He is currently a Technical Trainer / Corporate Trainer / Developer. He has taken a 150+ seminar/webinar and workshop on iOS Application Development, Python, IoT, and Digital Marketing across Gujarat colleges and universities. He is a member of the Computer Society of India. Right now, He is an Apple Authorized Trainer.

Dr.Kalpesh Popat is currently working as Associate Professor at Marwadi University, Rajkot, Gujarat. He obtained his Master's degree in Computer Application from IGNOU in 2003. He is a member of the Computer Society of India. He has published 30+ Paper in International Journal. His research area is mobile computing.

IJIT

ORIGINALITY REPORT

51%	45%	9%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	y1cj3stn5fbwhv73k0ipk1eg-wpengine.netdna-ssl.com Internet Source	16%
2	machinaresearch.com Internet Source	16%
3	R A Atmoko, R Riantini, M K Hasin. "IoT real time data acquisition using MQTT protocol", Journal of Physics: Conference Series, 2017 Publication	6%
4	www.netio-products.com Internet Source	5%
5	enterprise-iot.org Internet Source	4%
6	www.ijrte.org Internet Source	2%
7	ebin.pub Internet Source	1%
8	www.emeraldinsight.com Internet Source	<1%

9	J. Maha Kavya Sri, V. G. Narendra, Vidya Pai. "Chapter 29 Implementing and Testing of Internet of Things (IoT) Technology in Agriculture and Compare the Application Layer Protocols: Message Queuing Telemetry Transport (MQTT) and Hyper Text Transport Protocol (HTTP)", Springer Science and Business Media LLC, 2019 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		