**The important role of industry data connectivity using M2M and IoT applications for processing and analysis.**

Sanket Chauhan1 and Dr.Kalpesh Popat2

1 Marwadi University, Rajkot, Gujarat, India

2 Marwadi University, Rajkot, Gujarat, India  
[sanketchauhanios@gmail.com](mailto:sanketchauhanios@gmail.com)

[kapopat@gmail.com](mailto:kapopat@gmail.com)

**Abstract:** Whether it is an M2M or an IoT solution, one thing that is radical among the two is their ability to connect and manage devices in a buoyant and extensible way. Numerous platforms have emerged to assist with this endeavor. Single device vendors administer their M2M by deploying device management platforms to ensure that the drivers - that are used to connect across various networks and manage firmware alongside the software needs of the connected devices - are configured correctly. Currently, connectivity support platforms ensure that the connectivity paths are administered and monitored while also providing additional outputs like real-time connectivity status, reporting, troubleshooting, etc. The role of the device management platforms is highly integrated into the service enablement platforms and is directly related to the standardization of the support needed by the connected M2M. In the future, these connectivity support platforms are to become crucial as the latest and alternative connectivity technologies. The combination of M2M and IoT solutions brings together complicated devices, connectivity, applications, and data management processes. We have developed an expansive array of sensors, devices, and systems and will be deploying them alongside a broad and multifold range of M2M and IoT applications. Such applications can be used to monitor solutions for construction sites, surveillance systems, smart homes, and industry segments, amongst others. Each of these applications will be capable of performing detailed, user-specific tasks.

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

**Introduction**

Complex IT solutions can be compared to the design, development, and implementation of M2M solutions by addressing the M2M essentials of the vertical industries. Companies can easily standardize connectivity management and expand functionality within solutions by using connectivity support platforms. However, it is very rare for the connectivity support platform to be tailor-made to suit various connection technologies, making it the only limitation to date. After the development of applications, a huge amount of time, effort, and funds need to be invested to change/ upgrade the devices, add connectivity technologies, or integrate entirely new application requirements with the latest data models. [1][2] Resultantly, numerous purpose-built solutions are developed with restricted reuse of assimilation of the features of the connectivity support platforms.

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, which is 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.

A recent trend has been observed in application development whereby the common approach for the emerging range of M2M /IoT application platforms is an abstraction. Similar developments are expected in the connectivity support platform space which is usually the result of technological agnosticism. When the abstraction is combined with agnosticism, the developers can manage the scale and protocols on fewer platforms and focus more on application development rather 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.

When it comes to M2M and IoT, solutions tend to get generalized and diversified. The pre-established connections are more likely to face increased traffic and event loads. This makes it more difficult for the connected states of devices to expand across a dynamic range of communication technologies which include cellular, satellite networks, low-power geographic networks, and an assortment of short-range or fixed networks. In an ideal environment, it would require a lot more capacity to manage the diverse connectivity technologies than that of the connectivity platform.

Key challenges for this research it is very important to collect data relevant to the current situation of the industry and its problems. It is necessary to use real devices to cover the current situation, and it requires understanding many different protocols for data communication.

The main objective of this research is that we can easily use the current situation of the industry and its related productivity and understand the future situation and combinations from its analysis. Instead of the human introversion currently being used in product development, all the work can be done from one place easily by one machine, Which will prove to be a blessing for the coming generation.

The main contribution of this research is that the current industry 4.0 and the protocols and data communication that is being used for it can be very useful for my current research.

1. **Devices to Networks and Platforms:**

Over the last year, the machine market has become fragmented. Along with the other technological developments, recently, efforts have been made to promote standardization, openness, and simplicity; the result is - set standards that support the building of platforms upon them. [1] In this article, we discuss Ericsson's device connection platform that enables the operator to access the key features required to manage M2M business connections. Besides these, it presents examples of various business models and applications by deploying scenarios.

**1.1 Data Collection:**

Because of the existence of the traditional SIM card in the IoT world, we have adopted it as our identity. However, as the IoT markets keep developing along with the wireless technology standards, we see the SIM card, which was a physical device so far, become more and more software-centric. Ecosystem actors like SIM service providers, module manufacturers, OEMs, and Mobile Network Operators (MNOs) [4] face newfound threats due to the aforementioned trend



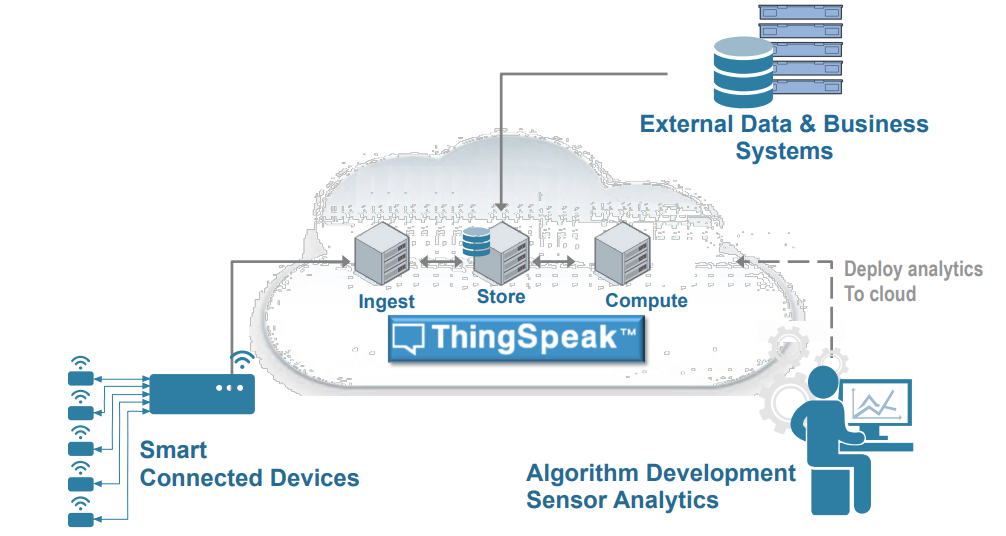
**Fig 1. Sensor Analytics and Development of Smart Devices**

Device credential storage: In the dynamic world, an IoT device must provide secure data storage. For this reason, the credentials must be stored in the device storage or on special chips that are secured to the fullest.

Exchange of communications with external service providers: Operating Systems are at a higher risk of being hacked as the credentials are encrypted and are exchanged over the mobile network with additional hardware monitor identification and authentication. The operator's profile remains open for quite some time, during which they are threatened. [15] [16]

**1.2 Data Communication:**

Data communication and connectivity form the heart of IoT. This network, where the devices can exchange information 24 hours a day, is equally reliable compared to MNO when it comes to strength and continuity. Companies can exploit the end-to-end solutions, integration of the recorded data with module sharing, and a centralized platform, irrespective of the place of the module as it always stays connected. This is because the SIM cards are a separate unit from the device module and hence, leave a trail. [4] A point of time in the future is expected to exist when mobile network operators will be unable to handle the large amount of data traffic resulting from increased devices entering the IoT network. This would result in lost connectivity, operational delays, and increased vulnerability to illegal monitoring, the performance of hacked machines, and information retrieval. [4] IoT security becomes a major concern with the propagation of vulnerable IoT devices combined with the increasing amount of data exchange over unprotected networks.



**Fig 2. Things Speak for Small Scale Deployment**

1. **Strengthen the Data Management Platform:**

The important factor, in this case, is the acquis communication as it facilitates the implementation of the IoT operational program. The benefits of this approach have been realized in the context of data on this platform, which must be recycled and processed immediately after its import. [5] The platform’s design allows it to be inverted. The Reverse charging limit of the IoT is limited to the current infrared type. The basis of the data access control is data transmission and that of the IoT output platform is data integration and validation.

**2.1 Centralized Device Management:** This allows one to manage, control, and remotely operate the devices after they are installed and connected through a safe wireless network. [5] On company-defined parameters, device management can assist in the configuration of the dynamic route and upgradation of the centrally located IoT devices’ firmware.

**2.2 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]

**2.3 Enhanced Administration and Security:** In addition to investing in full-scale administration done through a lone, intuitive cloud management portal, businesses can offer multi-level security to protect their data and devices from cyber-attacks. Besides these, they can use role-based permissions to manage the authenticated access for all types of users and control the time and method of the employees’ log on with the use of intelligent session ID and timeout management. [6][7]

**2.4 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.

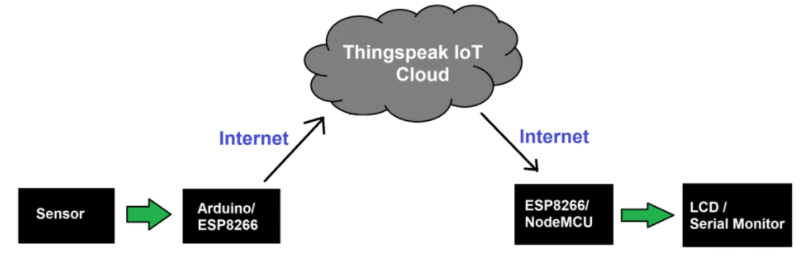
**Table 1. M2M Application Characteristics and Analysis**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |

1. **Data Transfer with MQTT**

The data is transmitted over TCP with the use of MQTT, which can be encrypted with SSL. The data transmission used for MQTT is the “Publisher-Subscriber”, [7] indicating the usage of the MQTT broker to exchange messages. In order for MQTT to work, the client - a device or a node - connects to the MQTT (over TCP). For a TLS Connection, port 1883 or port 8883 are used commonly. [13]

The connection between MQTT publishers and subscribers is the MQTT broker. The messages are sent from MQTT publishers to the MQTT subscribers, who subscribe to receive the messages so sent. The same “subjects” can contain several MQTT subscribers. Any device can either “publish” a particular “topic” (which consists of messages) or “subscribe” to one. The MQTT broker receives and sends the messages to the subscribing devices within a topic. One device can act as a publisher for certain topics while being a subscriber for the others. [8]

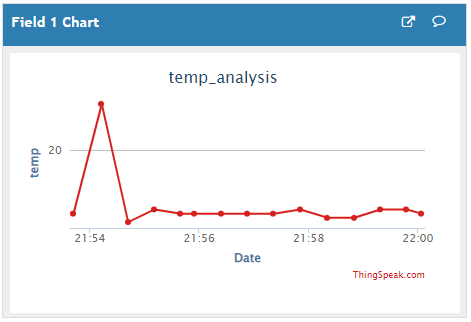
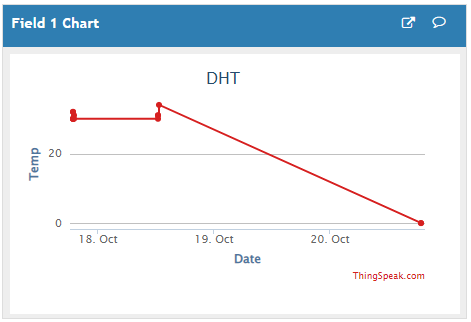


**Fig 3. Reading Data from Thing speak Block Diagram**

**3.1 Topic and Quality of Service (QoS):**

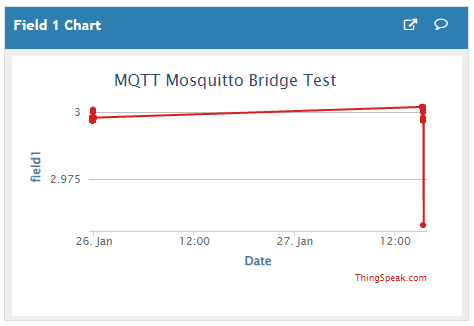
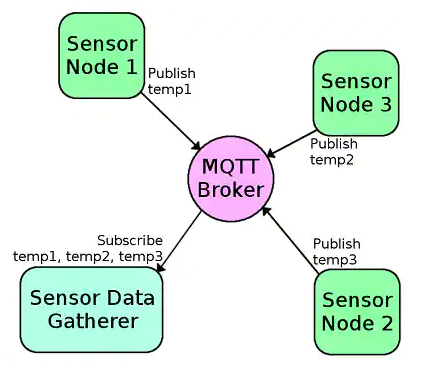
When the messages are sent to all the connected and subscribed clients, this recognizable content acts as a filter for brokers when the messages are sent by them to all the connections and subscribed clients in the MQTT - which also provides a quality service called QoS. Reliable messages can be sent at this level. A level 0 message is sent only once. [9] There are no attempts made to resend the message as they are sent on the basis of network presence. Level 1 messages are sent at least once, allowing the forwarder to send a message to the subscriber when the latter fails to acknowledge the message. The acknowledgment status of the client’s message is received by the forwarder by sending a message to the publisher. The receipt of the message is guaranteed in level 2, ensuring reliable delivery. This avoids message duplication. [8][9]

**3.2 Results:**

**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 Fig 7. MQTT Broker Result**

1. **Discussion:**

Supporting MQTT version 3.11, an integrated server holds the capability to act as an MQTT client, publishing content to an MQTT server and client who has subscribed to the topics on such an MQTT server. Specifically, the integrated server can publish MQTT messages to the MQTT server using the service pub.MQTT: integrated publication. [10]

By creating an MQTT activation, the integration server can register themes. The messages are received by the MQTT trigger and are then posted to the topic on the MQTT server, calling an activation service to process the messages is the next step. [11]

MQTT connections are used by the built-in server alias 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]

1. **Conclusion:**

This paper has provided a comprehensive review of M2M communications, and industry data connectivity using M2M and IoT applications for processing and analysis. Then, we have identified and explained the distinctive features of M2M applications and their supporting attributes from real devices for data communications. Whenever the connection overhead increased, the HTTP protocol required a connection to be established. This limitation of the HTTP protocol is overcome by the MQTT protocol. Unlike HTTP protocol where the data is reliable and synchronous, MQTT is not as reliable in every circumstance and is asynchronous. When it comes to sending data, although the HTTP protocol can be used for low-power IoT devices, the MQTT protocol is comparatively faster when it comes to sending data. This paper has provided a comprehensive review of M2M communications, discussing a general M2M communication system model, and explaining its three interlinked domains. Then, we have identified and explained the distinctive features of M2M applications and their supporting attributes from those of H2H communications. At last, we have integrated some of the key future research directions in this area to be explored further, we can take the industry program and development model even further with this model and beyond that, we can use communications and analytics very easily.

**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.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
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.