ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 9, September 2013

MQTT based Services using in Cloud IoNT Technology

Dr. Syed Nisar Ahmed[1]

Assoc. Prof. of Physics, Osmania College, Kurnool, India

ABSTRACT: The Internet of Nano Things (IoNT) provides seamless communication and transmission of data for the given range of operations. Increasing interconnection of nanosensors and nanotechnology with consumer devices and other physical assets have led to an immense growth in the scope of internet. Internet of Nano things (IoNT) provides capabilities for inter-communications between nano devices for data collection, processing and sharing with the end-users. IoNT has found applications in various industries such as healthcare, manufacturing, transportation and logistics, energy and utilities, media and entertainment, retail and other services. Use of MQTT protocol is publish-subscribe-based messaging protocol. It works on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker. The World Economic Forum has convened a network of experts to support the growth of a secure and reliable industrial internet of things (IIoT). These experts (the Network) are drawn from the business strategy, critical infrastructure, insurance, manufacturing, policy, security research and the technology communities. This paper describes about the Network recognizes that the vulnerable state of safety and security within this exponentially growing sector is untenable and has identified a number of challenges in the development of an optimally secure IIoT. It has focused on actionable solutions to those challenges. Google Cloud IoT is a set of fully managed and integrated services that allow you to easily and securely connect, manage, and ingest IoT data from globally dispersed devices at a large scale, process and analyze/visualize that data in real time, and implement operational changes and take actions as needed. MQTT stands for Message Queue Telemetry Transport.

KEYWORDS: MQTT, IoNT, Security Systems, IoT, Cloud

I. INTRODUCTION

The Network has developed a protocol framework through which actors can be aligned on the shared responsibility that ensures the security of IIoT products, practices and infrastructure. The IIoT ecosystem is not controlled by any particular stakeholder, neither is there a single discernible category of actors encharged with primary responsibility for its governance[1]. Nanoscale devices and systems characterized with their size of 100 nanometer and below are predominantly used to study phenomena such as near field behavior in electromagnetics and optics, single-electron effects and quantum confinement in electronics and other effects in biological, fluidic and mechanical systems[2]. Internet of nano things (IoNT) is the interconnectivity of such nanoscale devices over the internet and other communication networks. When the risk of harm is so widely spread, public safety and preventive security can only be meaningfully addressed with a collective commitment to the mutual obligations of confronting the challenges of a complex interconnected environment.

1.1. Internet of Things security architecture

When designing a system, it is important to understand the potential threats to that system, and add appropriate defences accordingly, as the system is designed and architected[3]. It is important to design the product from the start with security in mind because understanding how an attacker might be able to compromise a system helps make sure appropriate mitigations are in place from the beginning. The Network should increase awareness about as shown in Fig.1 IIoT security concerns and their consequences[4]. User awareness about IIoT security issues, and even less so expertise in remediating IIoT security gaps, is low across all user communities and across vertical markets – from small business start-ups to sophisticated enterprise technologists[5]. There is particular concern about security awareness at the IIoT device level, where connected devices and sensors typically lack security capabilities that are de rigueur in information technology systems; e.g., password change functionality and over-the-air updates.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 9, September 2013

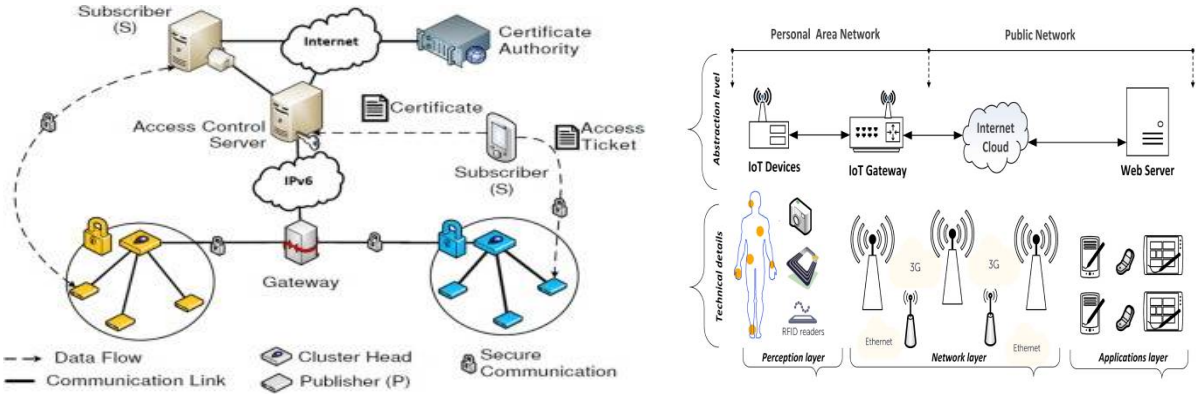

Fig:1. Internet of Things security architecture

In addition to low awareness, entities deploying IIoT systems tend to attribute less weight to the future consequences of security breaches than would be expected based on standard models of time discounting[6]. Without countervailing stakeholders that are biased towards future consequences, the direct and collateral damage to third parties would constitute a significant market failure. The insurance industry constitutes such a stakeholder and its engagement will propel behavioural changes by entities deploying IIoT systems, to whom underwriting services could be impacted by non-compliance with security standards[7].

The Network should increase awareness about IIoT security concerns and their consequences. User awareness about IIoT security issues, and even less so expertise in remediating IIoT security gaps, is low across all user communities and across vertical markets – from small business start-ups to sophisticated enterprise technologists[8]. The IIoT Safety and Security Protocol (the Protocol) generates an understanding of how insurance, which plays an integral part in the incentive structures of cybersecurity norm-setting and governance, can facilitate the improvement of IIoT security design, implementation and maintenance practices. The framework is intended to strengthen security IIoT services using active hardening processes that can be validated through proven penetration, configuration and compliance techniques.

II. MQTT A PROTOCOL

MQTT a protocol for transporting messages between two points. Sure, we've got Messenger and Skype for that; but what makes MQTT so special is its super lightweight architecture, which is ideal for scenarios where bandwidth is not optimal. As shown in fig.2 the MQTT high-level architecture is primarily divided into two parts – a broker and a client. Therefore, MQTT clients have very specific and simplified tasks. The publisher-client publishes MESSAGES with a TOPIC and QUALITY; the subscriber-client subscribes to MESSAGES with a TOPIC and QUALITY. And that's pretty much the gist of it[9].
Also, MQTT clients are very good runners! They will run on almost any OS – Mac, Windows, and Linux; as well as single-board and mobile operating systems like Raspbian

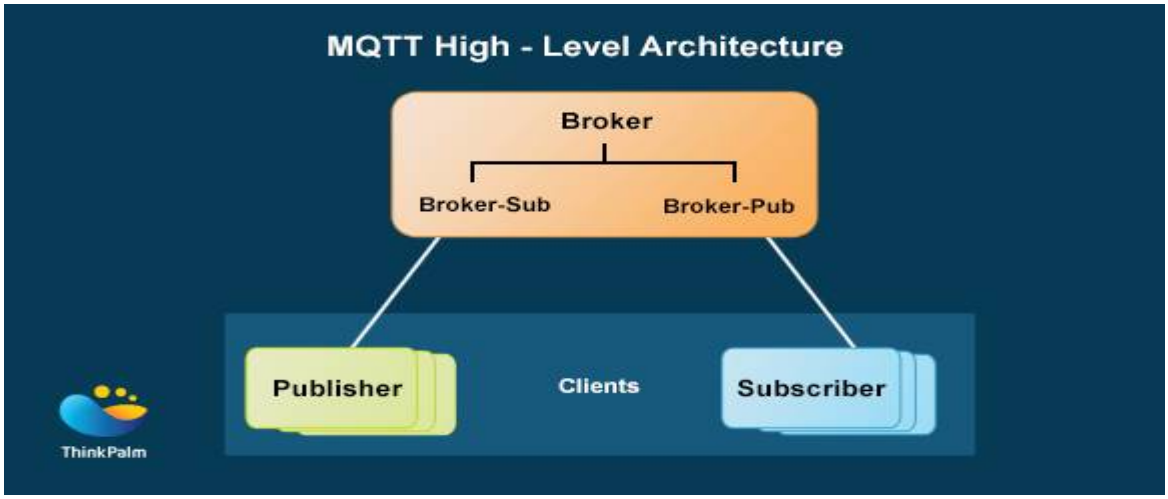

Fig:2. MQTT Architecture

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 9, September 2013

Internet of Nano Things (IoNT) infrastructure can be deployed as a combination of various nanotechnologies and nano devices. The IoNT infrastructure depends on the area of operation and required bandwidth for a particular application. Deployment of IoNT infrastructure provides high speed of communication and reduces the bandwidth pressure on existing communication infrastructure. The growth of the Internet of Nano Things (IoNT) primarily focuses on improving processing capabilities, providing larger storage capacity at lower costs and increasing the role of communication terminals. The IoNT infrastructure can be deployed in various eco-systems such as electro-magnetic waves, Wi-Fi, Li-Fi, radio frequency identification (RFID) and nano antenna. A broker acts as the heart of the architecture with capabilities of both subscriber and publisher. It is the point of contact for all clients. A broker's primary job is to queue and transmit messages from a publisher client to the subscriber client[10]. However, it can also possess heavier capabilities (such as SSL certification, logs, database storage, etc.) based on requirements, set-up, and the broker service used. and Android. They even exist as apps! As shown in below fig.3

Fig.3. Security services shown in Cloud

An MQTT system consists of clients communicating with a server, often called a "broker". A client may be either a publisher of information or a subscriber. Each client can connect to the broker. Information is organized in a hierarchy of topics. When a publisher has a new item of data to distribute, it sends a control message with the data to the connected broker. The broker then distributes the information to any clients that have subscribed to that topic. The publisher does not need to have any data on the number or locations of subscribers, and subscribers in turn do not have to be configured with any data about the publishers.

If a broker receives a topic for which there are no current subscribers, it will discard the topic unless the publisher indicates that the topic is to be retained. This allows new subscribers to a topic to receive the most current value rather than waiting for the next update from a publisher.

When a publishing client first connects to the broker, it can set up a default message to be sent to subscribers if the broker detects that the publishing client has unexpectedly disconnected from the broker.

Clients only interact with a broker, but a system may contain several broker servers that exchange data based on their current subscribers' topics.

A minimal MQTT control message can be as little as two bytes of data. A control message can carry nearly 256 megabytes of data if needed. There are fourteen defined message types used to connect and disconnect a client from a broker, to publish data, to acknowledge receipt of data, and to supervise the connection between client and server.

MQTT relies on the TCP protocol for data transmission. A variant, MQTT-S, is used over other transports such as Bluetooth.

MQTT sends connection credentials in plain text format and does not include any measures for security or authentication. This can be provided by the underlying TCP transport using measures to protect the integrity of transferred information from interception or duplication.

III. CLOUD IoT PLATFORM

Google's serverless Cloud IoT platform as shown in fig.4. eliminates the need to build and maintain costly infrastructure for your IoT data analysis. Connect easily to the cloud and accommodate all your globally dispersed devices using Cloud IoT Core's protocol bridge with automatic loading balancing and horizontal scaling[11]. Ensure secure device connections with industry-standard protocols and lower your total cost of ownership with no capex or ongoing maintenance required.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 9, September 2013

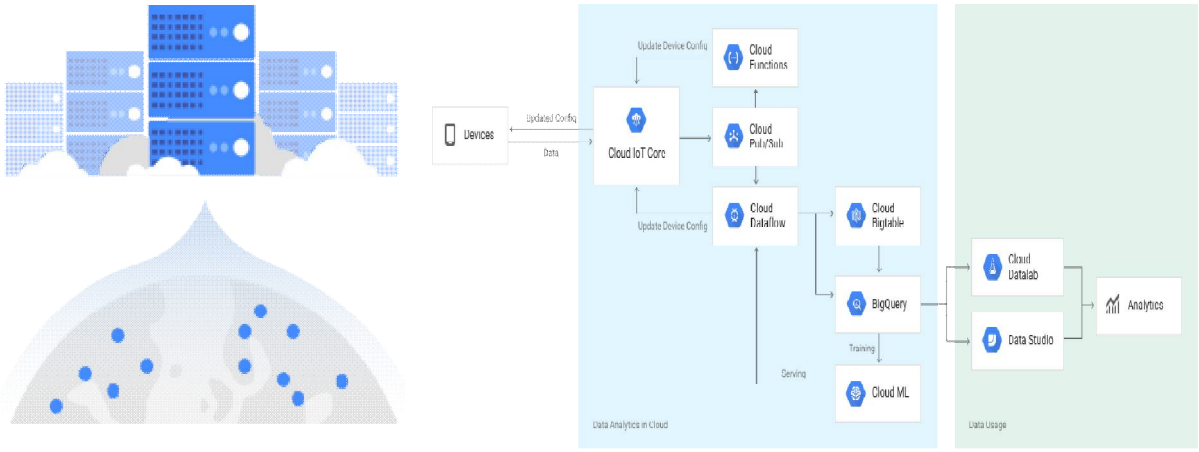

Fig.4. Serverless Cloud IoT platform

IV. IMPLEMENTATION

4.1. REST API over HTTP/HTTPS/Websockets:

- As is already known, this is a great option for apps <-> cloudcommunication. Abundant support and frameworks are available for handling all the common use cases.
- This is also a good option for IoT device (server) <-> app (client) communication in the local network. Again the reason is that this model is abundantly supported in the app ecosystem. And most Wi-Fi enabled IoT devices already support a web server.
- This can (and is) also be used for device <-> cloud communication. So essentially the IoT device acts as a Web Client. The one problem that you have to work around is that HTTP is a challenge-response protocol. So the device will either have to keep polling the server for new updates, or use long polling, or use websocket.

4.2. CoAP:

- CoAP runs on UDP and thus can be run on extremely resource constrained environments. It offers semantics parallel to HTTP for the most part.
- It is a good mechanism for local network communication, particularly when their is an ecosystem of other CoAP devices[12].

4.3. Encryption

Entities deploying IIoT systems must ensure that new devices and associated applications support current, generally accepted security and cryptography protocols and best practices, where applicable. Data both at rest and in transit, that is scored in the risk assessment to be protected, should include sufficient industry accepted practices to secure the data. Many industrial protocols currently in use were not designed with security in mind and lack basic authorization and encryption features. Entities deploying IIoT systems should properly address these challenges utilizing additional security controls and upgrade to systems supporting encryption whenever possible.

V. MEETING THE CHALLENGES

One of the major factors driving the growth of IoNT market is the rise of ubiquitous connectivity. With the increasing number of computer devices and interconnection capabilities over the internet, various industrial applications of IoNT have been identified. The interconnection of nano devices has enabled efficient communication of data between different devices or components of a system. Thus, through IoNT, organizations are able to reduce the complexity in communication and increase the efficiency of processes using such connected devices. Moreover, government's support for the development of IoNT technology for healthcare has further increased the demand and awareness of IoNT. However, the growth of the IoNT market faces a few challenges due to privacy and security issues. Since critical data is communicated between devices over the internet, concerns related to security of the data have risen. Another factor which hinders the growth of IoNT market is the huge capital investment required for the development of nanotechnology[13].

- Apart from being light weight, MQTT offers publish/subscribe semantics (on the same socket) which makes it easier to program on the IoT device side. IoT cloud service providers like AWS IoT and Everything and others offer MQTT based device connectivity.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 9, September 2013

- It requires a message broker (server) for its functioning. This makes it a good option for remote/cloud communication, since the cloud server acts as the message broker between the IoT device and other app/services[14].
- This also makes it NOT a great option for local network communication between devices, because it requires the end-user to deploy an additional broker in her system.

VI. RESULTS AND DISCUSSION

Industrial and business-level consumers (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices Ultimately, it is we security professionals who have to perform the necessary risk assessments and make the necessary controls adjustments[14]. But this is not a long-term solution given the use of IoT across businesses, homes, and organizations of all sizes… including those with no security teams. Service providers, that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services

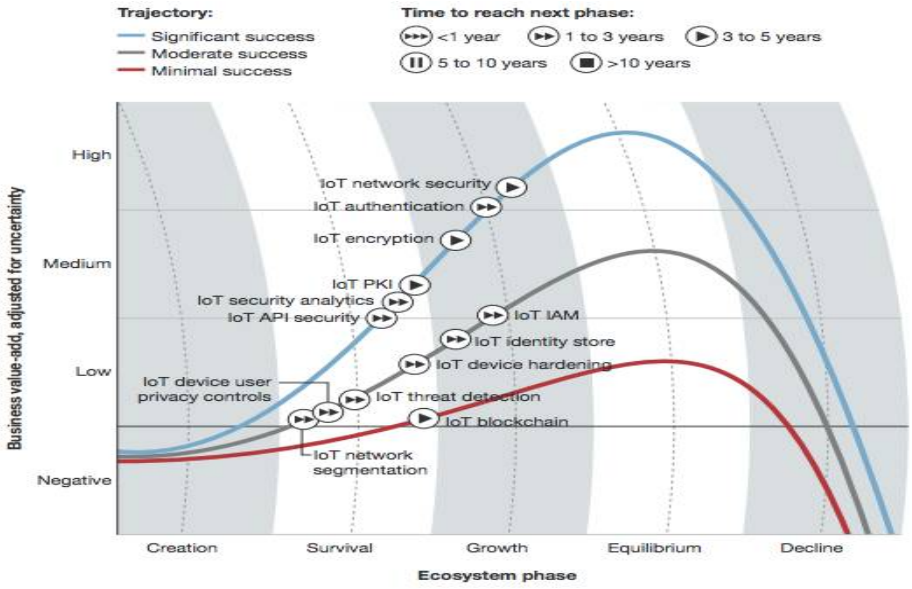

Fig.5. IoT Security graph

I agree with the Department of Homeland Security principles (below) in its Strategic Principles for Securing the Internet of Things that it is everyone's responsibility to meet IoT challenges:
IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed and IoT manufacturers to improve security for both consumer devices and vendor managed devices.

VII. CONCLUSION

These IoT Application Layer communication protocols, CoAP and MQTT have been tipped as the most suitable protocols currently being implemented in most IoT applications, the reason being that they are light weight and are suitable for constrained devices, such as sensors. Chapter 6 is dedicated to the comparison and interoperability between the two main IoT protocols, MQTT and CoAP. In comparison, it was reviewed that it all depends on the preference and the application. Either protocol is suitable for IoT applications because both are designed for lightweight devices and suitable to a constrained environment. It would be nice to see these principles voluntarily followed, but that is unlikely to happen unless consumers and businesses demand it. Microsoft and Adobe, for example, were largely pushed to more secure practices by consumers and bad public relations related to breaches. I hope it doesn't take several highly destructive events to get IoT developers, manufacturers, service providers, and users on board with IoT security. The Semantic interoperability provides a different dimension to the data interoperability at the Application Layers protocols. This means that interoperability must take place at a higher level of the protocol stack than raw data transferred.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787 – 2805, 2010.
[2] Consortium et al., "Industrial internet reference architecture," Industrial Internet Consortium, Tech. Rep., June, 2010.
[3] A. B. HEU, P. G. HEU, A. O. CEA, and J. Stefa, "Internet of things architecture," 2011.
[4] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security.
[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT).
[6]H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?," IEEE Communications Letters, vol. 15, no. 4, pp. 461–463, 2011.
[7] K. on Security, "Ddos on dyn impacts twitter, spotify, reddit".
[8] W.Rouths, Science Thomson Reuters, "Web of science databases." https://webofknowledge.com.
[9] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS)
[10] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, no. 1, pp. 112–116, 2011.
[11] P. Adolphs, H. Bedenbender, D. Dirzus, M. Ehlich, U. Epple, M. Hankel, R. Heidel, M. Hoffmeister, H. Huhle, B. K¨archer, et al.,
[12]S. Park et al., "Ipv6 over low power wpan security analysis draft- 6lowpan-security-analysis-05," tech. rep., IETF Internet Draft, 2009.
[13] P. R. Pietzuch, Hermes: A scalable event-based middleware. PhD thesis, University of Cambridge, 2004.
[14] M. Eisenhauer, P. Rosengren, and P. Antolin, "Hydra: A development platform for integrating wireless devices and sensors into ambient intelligence systems," in The Internet of Things, pp. 367–373, Springer, 2010.