iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

IoT Smart Home: Protocols and Architectures

Jiby J. Puthiyidam[1], Dr. Shelbi Joseph[2],
[1, 2] *School of Engineering, Cochin University of Science & Technology, Kochi, India*

Abstract: ***The term Internet of Things has been around us for the past couple of decades, but still no one can say that it is fully functional and operational. The reason for this is the lack of a unified architecture and the unavailability of acceptable standards and protocols for IoT components. One of the major application areas of IoT is the Smart Home environment. Smart homes are more relevant now than ever as the single person homes increases worldwide. Single person homes lack social support for the inmates, and they need to depend more on technology to improve their comfort and convenience. IoT assumes that all the 'things' in its environment are intelligent enough to perform some kind of sensing, processing and communication features. In this paper, we review the various protocols at different layers in the IoT stack that are used to connect the things to each other and to the internet and compare the popular IoT application layer protocols exist today. We consider the application layer protocols MQTT, AMQP, CoAP, XMPP and DDS in terms of their message type, transport protocol, Security etc. And also discuss the advantages and disadvantages of each one at different aspects.***

Keywords: Smart Home, interoperability, MQTT, AMQP, CoAP, XMPP, DDS

I. INTRODUCTION

A home is not only built by the bricks and cement alone, but also with the social interactions and relationship between the persons living there. A home is a place where people relaxes and take rest after a day full of work, meeting or journey. Everyone should feel comfort, convenience and security at their home. A home has a very crucial role in building and maintaining an individual person's relationship with other family members. Gidden (1984) [1] says that a home is both an individual space and a unit of social interaction, ie. a socio- spatial system that represent basic forms of social relations. Communication and interaction among family members are important to form a healthy family [2]. Thus home is a place where people relax (both physically and emotionally) and also feel comfort. It is also a place for social interactions.

After a busy day when we return to our home, nobody wants to engage with the house hold activities immediately. They need to take rest and relax. If a cup of coffee is readily available when we enter our home, it will make us feel fresh both physically and mentally. If the Air Conditioner is already ON when we enter into the bedroom or water is warm in the bath tub, the comfort and convenience would be different. In the present social set up, other family members, spouse, mother etc. may do some of these tasks in advance for us.

Studies reveal that single person households grow rapidly across the globe, especially in developed countries liks USA, South Korea etc. [3]. This scenario forces us to rewrite the definition of a home as a social space. In the future, inmates may not receive the required and expected social support at home. In a single person home, we cannot expect anybody to help us at home to help us in our daily activities and even if somebody share the home with us, they might not have enough time to take care of others. The social interaction and relationships may be affected. The rapid developments in communication technology alleviate this problem to some extent. Now, people can contact others instantly by utilizing the advent in technology. But the comfort, convenience and security at home may be greatly affected.

At the same time, smart home technology, aiming to provide comfort and convenience to the inmates also grows rapidly. A smart home refers to a home where the house hold devices and appliances are fully connected and systematically inter act each other to provide the necessary services to the users. These devices communicate each other to automatically control the functions of various home appliances and to provide convenience to the user. A single person home have no social support as there is not a second person at home to support the one living there. Hence, providing enhanced convenience, comfort and secure living style through smart home concept is more important, especially in the case of single person homes where an elderly person or a person with some inability lives. In order to design and develop a smart home to achieve the above mentioned services in a home without any user intervention, the devices, furniture and other equipment's in the home should also be smart. They must be incorporated with sensing, processing, storing and communication features. The easiest and cost effective way to attain the communication among various devices and share information is to make use of the existing internet connection. Since these devices have limited processing power, storage capacity and communication capabilities unlike the computer and other devices specifically designed to work with the internet, the present TCP/IP protocol cannot be used as such. We need protocols that deal with this low power, constrained

devices.Over the last couple of decades, the Internet has been in a constant state of evolution. Alongside, developments in the Internet technologies, technologies in Sensor Networks and Near Field Communication using RFID tags have also been evolving. Convergence of these technologies is leading to the possibility of direct machine-to machine communication over the Internet. This concept has led researchers and manufactures to foresee the benefits of bringing more and more machines online and allowing them to be a part of the web. These devices form a vast network of autonomous, self-organizing devices with limited processing and communication capabilities. This vision has evolved later to the most fastly developing area referred to as the Internet of Things (IoT). The main idea behind IoT is that everyday objects can be equipped with identifying, sensing, networking and processing capabilities. These features let to communicate with one another and with other devices and services over the Internet to achieve some useful objective.

The significance of IoT enabled smart homes is clear now. Internet of Things (IoT) assume that everything in the real world with a physical or virtual existence can be made to intelligent by enabling them to perform some kind of sensing, processing and communication capabilities. These 'things' may need to share their resources to cooperatively attain the desired task. Internet of Things is not only linking connected electronic devices by using the Internet; it is also web-enabled data exchange in order to enable systems with more capacities "smartness". In other words IoT aims for integrating the physical world with the virtual world by using the Internet as the medium to communicate and exchange information.

A primary goal of interconnecting devices (e.g., sensors) and collecting/processing data from them is to create situation awareness and enable applications, machines, and human users to better understand their surrounding environments. The understanding of a situation, or context, potentially enables services and applications to make intelligent decisions and to respond to the dynamics of their environments. Data collected by different sensors and devices is usually multimodal (temperature, light, sound, video, etc.) and diverse in nature (quality of data can vary with different devices through time and it is mostly location and time dependent). The diversity, volatility and ubiquity make the task of processing, integrating, and interpreting the real world data a challenging task.

The paper starts with a brief discussion about the requirements of smart homes in section II. In the next section we'll have a look on various protocols and architectures at various level of IoT stack. In section IV we'll compare the requirements and performance of popular protocols at the IoT application layer. Finally, the conclusion and future scope is given in the last section.

II. SMART HOME REQUIREMENTS

A smart home is supposed to meet the requirements of the inmates. Designing and implementation of smart home faces may challenges. Some design challenges of smart homes are discussed below:

A. Standards

There are different types of devices in a home. They include furniture, home appliances, intelligent devices, sensors etc. We are not sure where these devices are installed, when they need to be activated, what are their capabilities etc. We need the integration and cooperation of these devices to achieve the true smart home perspectives. These devices with different capabilities and functionalities need to communicate each other. They require a standardized network transmission and a seamless platform to cooperate with each other.

B. Management of smart devices

More and more new applications are added to the smart home environment daily and many more will be added in the future. Some of the existing applications may need to be updated with more functionality. There must be provisions to manage smart home applications to dynamically add new applications and to upgrade the existing ones .

C. Reliable and secure functioning

Users of smart home might not have enough expertise and knowledge to manage the intelligent devices in their home. Again, they do not have a dedicated administrator to monitor and manage the applications at their home. The smart home applications should be able to function properly under any circumstances without any interrupt or delay. These applications should be secure and reliable even in the absence of a central controller or an administrator. Also, these applications should not affect and violate the security and privacy matters.

D. Diversified users

Users of the smart home applications may use it for various purposes and requirements. The use of an application depends on the situation. Some outside parameters may also affect these applications. Therefore, these applications should satisfy the requirements and convenience of all categories of users and ensure the expected results by inference.

E. User-Oriented Designs

There exist plenty of applications for smart home and many more will be coming in the future days. These applications may be designed for different scenarios and situations. But the prime importance should be given to the users. These applications should be designed with the user in mind, should meet the user requirements and provide an easy to use interface if interactions are required.

In order to satisfy the above mentioned requirements of a smart home, a context aware system that manages and monitors a smart home is required. Since the devices (Resources) of a smart home need to interact and communicate each other frequently, one of the major requirements of smart home application is the Resource discovery. The devices in a smart home may be placed either at fixed positions (static) or be moved around by being carried by some moving objects or people (mobile). These devices, whether mobile or static, need to establish connection with other devices when they come in their contact range. This forms an opportunistic networking scenario, where static and fixed elements may periodically interact with opportunistically.

The basic concept of Internet of Things depends on the sharing and collaboration of information among the participating devices. Context-aware resource discovery is required in IoT environments and hence is very important smart homes. A general definition of context says that it is the information needed to interpret something. This definition is vague in nature, does not provide a good understanding and is not useful for computing purposes[4]. Many researcher tried to define context, but most of them were specific to a particular domain such as Human Computer Interaction, localization systems etc. Miraoui et al. defines that " A system is said to be context aware if it can automatically change the form of its services or provide a service in response to the change in the value of information or a set of information that characterizes those services" [5]. This definition explains awareness as a reaction of the system to modifications to information values in terms of triggering a service or changing its form independently of the applications [5]. This definition seems to be simple and complete as it consider both triggering information and form changing information. Resource discovery can be classified into two classes, Device Discovery and Service Discovery

III.IOT ARCHITECTURES AND PROTOCOLS

IoT is an area where a lot of research and development currently being in progress. Many protocols are being added to the IoT environment as there is no standard protocol accepted by everyone. Most of the IoT Protocols were developed by the leading vendors and manufactures in the area to promote their own products and protocol choices. They come up with new versions of protocols to address the requirements of their products. These protocols are suitable for a broad range of applications. The application developer should have a clear idea regarding their specific requirements and limitations to ensure that the correct set of protocols is chosen for the various management, application, security and communication features. Then the designer should select the best implementation technique for the system.

A. Protocol Features Uncovered

Communication is one of the important features of IoT Protocols [9]. In IoT also, the communication is based on the TCP and UDP protocols used for the internet communication. Both have its own merits in the IoT environment and various protocols exist based on each of these standards. Some developers claim that UDP has advantage in performance and size that result in minimizing the cost. TCP on the other hand, guarantee the delivery of all data without errors.

Another important protocol feature is *messaging*. As the IoT nodes may be mobile or stationary, they need to connect and disconnect frequently with other nodes in its proximity. These nodes may also need to connect to different cloud applications. In this scenario, the publish/subscribe or request/response model is preferred. Such protocols can manage the connection and disconnection operations dynamically and can support many nodes. Two popular protocols CoAP and HTTP/REST are based on request response without a publish and subscribe approach.

The *system architecture* of IoT protocols includes client server, tree, star, bus and P2P. Most of the protocols follow the client server architecture but performance wise; P2P and bus are the best.

As more and more devices and applications are entering in to the IoT domain, *scalability* is very important. Scalability in the client/server environment can be achieved easily by extending the number of servers available. In Star and tree topologies, scaling is achieved by adding extra leaves on the tree, but with added burden in communication.

The protocol that we select should the capability to deal with resource constrained devices. As IoT world is full of resource constrained, low power devices with limited processing and storage capacity, the protocol that we select should also be capable of managing such devices. Again, this nodes may need to switch between on and off positions to save power and other limited resources, the protocols must support frequent connection and disconnection etc.

Interoperability is a major requirement in the IoT environment as the devices and applications are developed and distributed by various vendors and manufactures without any globally accepted standard. IoT users want these sensors and devices to work together. By using a set of standardized protocols and standardized communication/messaging services the true interoperability among the IoT devices can be achieved.

B. Standards Organisations

There are several standards organizations for developing and supporting standards to offer interoperability and communication among IoT devices [11]. The Institute of Electrical and Electronics Engineers (IEEE) offer standardisation efforts for Physical, Media Access Control (MAC) and Application layers to meet the new requirements of IoT (eg. Low power, battery constrained devices). The Internet Engineering Task Force (IETF) has three main working groups for the connectivity between network-enabled devices and the network (e.g. Internet); 6LoWPAN, Routing Over Low Power and Lossy Networks (ROLL) and Constrained Restful Environments (CoRE) working groups[11]. The Internet Protocol for Smart Objects (IPSO) Alliance also promotes the use of Internet Protocol (IP) for the networking of embedded sensor and actuator (smart) devices to transmit their observation and measurement data in the IoT domain. IPSO also complements the effort of other standards organisations such as IETF, IEEE, the Industrial Internet Consortium (IIC), the Open Connectivity Foundation (OCF) (formerly Open Interconnect Consortium (OIC)), World Wide Web Consortium (W3C) and others by documenting and running interoperability tests of different IP-based standards released by these standards organisations [11].

C. IoT Communication Protocols

The IoT standards protocols are offered by Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU) and other pioneers in the field. These protocols were proposed to meet the current and future IoT requirements. The commonly used communication protocols in the IoT world are listed in figure 1.

Session		**MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, …**	**Security**	**Management**
Network	**Encapsulation**	**6LowPAN, 6TiSCH, 6Lo,** Thread, …	TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, …	**IEEE 1905, IEEE 1451,** …
	Routing	**RPL, CORPL, CARP, …**		
Datalink		WiFi, **Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE**, 3G/LTE, NFC, **Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7,** ANT+, **LTE-A, LoRaWAN, …**		

Fig 1: IoT communication Protocols [11]

D. IoT Data Link Protocols

1) IEEE 802.15.4e: It extends IEEE 802.15.4, the most commonly used wireless standard and supports low power communication to meet IoT requirements.
2) IEEE 802.11AH: A light version of IEEE 802.11 wireless standard, designed with less overhead to meet IoT requirements.
3) Wireless HART: A secure and reliable MAC layer protocol. Uses advanced encryption methods and offer reliability.
4) Z-Wave: A low power MAC protocol used for IoT communications. It is suitable for small range communications. It follows master/slave architecture.
5) Bluetooth Low Energy (BLE) or Bluetooth Smart : A short range communication protocol mainly used for in-vehicular networking. It uses ten times les energy than classical Bluetooth while its latency can reach 15 times. It follows master/slave architecture.

E. Network Layer Protocols

These protocols are used for the routing purposes. We divide the network layer into two sub layers: routing layer and encapsulation layer.

1) RPL (Routing Protocol for Low-power and lossy networks): It is a distance vector protocol. It builds a DODAG (Destination Oriented Directed Acyclic Graph). DODAG has only one route from the each leaf to the root.

2) CORPL (Cognitive RPL): An extension of RPL.
3) CARP (Channel Aware Routing Protocols): A distributed routing protocol. Mainly used for under water communication. It can be used for IoT as it use light weight packets.
4) 6LoWPAN: The most commonly used encapsulation standard. It encapsulates IPv6 long headers in IEEE 802.15.4 small packets, which cannot exceed 128 bytes. It supports different length addresses, low bandwidth, different topologies, low power consumption etc.

F. Session Layer Protocols

This section discusses the protocols for message passing in Iot systems.

1) MQTT (Message Queue Telemetry Transport) : Introduced by IBM. It follows a publish/subscribe architecture. Three main components: publishers, subscribers and broker.
2) AMQP(Advanced Message Queuing protocol): It runs over TCP. Provides a publish/subscribe architecture similar to MQTT. Here the broker is divided into two components: exchange and queues. Exchange: receive publisher messages and distribute them to queues.Queue : represent topics and subscribers subscribes it. CoAP (Constrained Application Protocol): designed to provide lightweight RESTful (HTTP) interface. REST(Representational State Transfer) is the standard interface between HTTP client and servers. CoAP is designed to enable low power sensors to use RESTful services while meeting their power constrains. It is build over UDP.
3) XMPP(Extensible Messaging and Presence Protocol): Originally designed for chatting and message exchange applications. A TCP based protocol based on XML.

IV.COMPARISON OF APPLICATION LAYER PROTOCOLS

The major communication protocols for IoT environment includes Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP) and Data Distribution Services (DDS). A brief discussion about these protocols is given below.

A. MQTT

A publish-subscribe messaging protocol developed for resource-constrained devices (lightweight M2M communications). It was developed by IBM in 1999 and standardized by Organization for the advancement of structured Information Standards (OASIS) in 2013. MQTT is TCP based protocol. It is simple and light weight and suitable for Machine to Machine communication. For message delivery, MQTT support three different kinds of Quality of Service(QoS). The messages can be delivered exactly once, at least once and at most once [12]. To ensure privacy, the TCP connection may be encrypted with TLS/SSL. An extended version, MQTT-S, on the other hand works with UDP.

1) *Architecture:* MQTT has a client/server model. Every sensor is a client and it connects to a server, known as a broker, over TCP. It is message oriented. Every message known as a topic, is published to an address. Clients may subscribe to multiple topics. Every client subscribed to a topic receives each message published to the topic. The publisher subscriber model allows one-to-one, one-to-many and many-to-one communication between MQTT clients.
2) *Downside:* MQTT uses TCP connections. MQTT clients must support TCP to connect to MQTT broker[11]. The connections are open to the broker all the time, a problem in resource constrained environments. MQTT topic names are often long strings which make them impractical for 802.15.4. MQTT lacks encryption. The protocol was intended to be lightweight and encryption results in added overhead. MQTT messages are not labeled with types or other metadata to help clients understand it. Clients must know the message formats up-front to allow communication.

B. AMQP

A message queue based protocol arose from the financial industry and standardized by OASIS. It provides publish/subscribe communication which results in lower bandwidth and less message processing that extends the battery life. AMQP use TCP transport protocol. Its store and forward feature ensures reliability [13]. AMQP also provides three different kinds of QoS similar to MQTT: At most once, at least once and exactly once. Security is handled with TLS/SSL protocols [14].

1) *Architecture:* The major payers in AMQP architecture are Publisher, Exchanger and subscriber. Publisher is a device in IoT environment that publish some information. This information is stored in message queues. Exchangers are used to route message to appropriate queues. Subscribers are interested in subscribing and receiving the information stored in message queues [10].
2) *Downside*: AMQP has low success rate at low bandwidths.

C. CoAP

A protocol specifically developed by IETF CoRE (Constrained Resource Environments) group. It supports a subset of HTTP functions, but unlike HTTP CoAP is designed for the needs of constrained devices. CoAP is a request/response protocol. CoAP runs over UDP, not TCP. In CoAP, a sensor node is not a client, but may also act as a server. The sensor (in the server role) provides resources which can be accessed by clients to read or change the state of the sensor. CoAP supports four message types: Confirmable, Non-confirmable, Acknowledgement and Reset. Because CoAP is built on top of UDP, the security protocols SSL,TLS etc used with TCP are not suitable to provide security. DTLS, Datagram Transport Layer Security provides the same assurances as TLS but for transfers of data over UDP.

1) *Architecture*: Clients and servers communicate through connectionless datagram. For the addressing purpose, UDP broadcast and multicast can be used. CoAP follows a client/server model. Clients make requests to servers, servers send back responses. CoAP uses HTTP commands (GET, PUT, POST and DELETE) for interacting with resources [15].
2) *Downside*: Request/Response architecture is not suitable for IoT device as Publish/Subscribe model because. CoAP has no built-in security features. DTLS is not designed for IoT. DTLS does not support multi-cast [16]. CoAP over DTLS create confusion and extra overhead to HTTP server.

D. XMPP

It is a TCP protocol based on XML. It started as a chat application; hence it supports contact list managing. It performs the exchange of structured data between connected entities. This protocol can easily be extended to include publish subscribe systems. It is decentralized in nature. XMPP has TLS/SSL security built in the core specification [14].

1) *Architecture:* XMPP does not have a central XMPP server; decentralization is a major advantage [17]. Individuals can place their XMPP servers. Different clients and various server architectures can communicate each other [18]. It supports client-server and server-server communications.
2) *Downside:* XMPP lacks end-to-end encryption and it doesn't have the QoS (Quality of Service) functionalities. XML messages require XML parsing that need additional computational capability and more power consumption.

E. DDS

Designed by the Object Management Group (OMG), DDS has a publish-subscribe message pattern and is more suitable for the real-time systems. It uses both TCP and UDP transport layer protocols and has excellent QoS(It has nearly 23 QoS). DDS detects dynamic changes in meta-events[11]. DDS has its success in Military and Industrial areas [19].

1) *Architecture:* DDS transmits data between publisher and subscriber as topics. Data on the topic is generated by the DataReader in subscriber and Data Writer in publishers [20].
2) *Downside:* DDS does not support interoperability between different vendors/implementations. Its high overhead of IP multi-cast prevent it from developing on mobile nodes and wireless networks. QoS policies are applied only in strict DDS environments.

TABLE I
CHARACTERISTICS OF APPLICATION LAYER PROTOCOLS

Protocol	Standardisation Group	Transport Layer Protocol	M2M Commn. Support	Message Pattern	Security	QoS (Delivery Notification)
MQTT	IBM, OASIS	TCP	Yes	Publish/Subscribe	TLS/SSL	• Exactly once • At least once • At most once
AMQP	OASIS	TCP	Yes	Publish/Subscribe	TLS/SSL	• Exactly once • At least once • At most once
CoAP	IETF CORE Group	UDP	Yes	Request/Response Publish/Subscribe	DTLS	• Confirmable • Non-confirmable • Acknowledgement • Reset
XMPP	IETF	TCP	No	Publish/Subscribe	TLS/SSL	No guaranteed QoS

DDS	OMG	TCP/UDP	Yes	Publish/Subscribe		Supports nearly 23 QoS (Security, durability, priority, reliability etc.)

TABLE II
PROS AND CONS OF DIFFERENT APPLICATION LAYER PROTOCOLS

Protocol	Advantages	Disadvantages
MQTT	• Header size -2 bytes, makes it suitable for constrained networks • Useful for applications where interaction between devices are required • Use of publish/subscribe architecture makes it suitable for IoT devices	• MQTT clients must support TCP/IP to connect to MQTT broker. • MQTT clients should have an open connection to broker all the time, affects battery life. • Centralised broker become a single point of failure
AMQP	• Store and forward feature guarantees reliable message delivery • Can send large amount of message/second compared to REST	• Low success rate with low bandwidths.
CoAP	• Most light weight protocol (due to UDP) • Easily integrated with the web (supports HTTP functions) • Support uni-cast and multi-cast. • Suitable to control devices through commands.	• Request/Response architecture is not suitable for IoT device as Publish/Subscribe. • Has no built-in security features. • DTLS is not designed for IoT • CoAP over DTLS create confusion to HTTP server
XMPP	• Decentralisation (No central XMPP Server) • Allow servers with different architectures to communicate • Can be used with chat applications	• Not Provide QoS. • Not Suitable for M2M • Streaming XML has overhead. (require XML parsing results in increased computation and power usage)
DDS	• Suitable for real-time IoT • Has powerful QoS • Detects dynamic changes in events • Scalable, extendable and efficient standard	• Does not support interoperability between different vendors/implementations. • High overhead of IP multi-cast prevent it from developing on mobile nodes and wireless networks. • QoS policies are applied only in strict DDS environments.

V. CONCLUSION AND FUTURE WORK

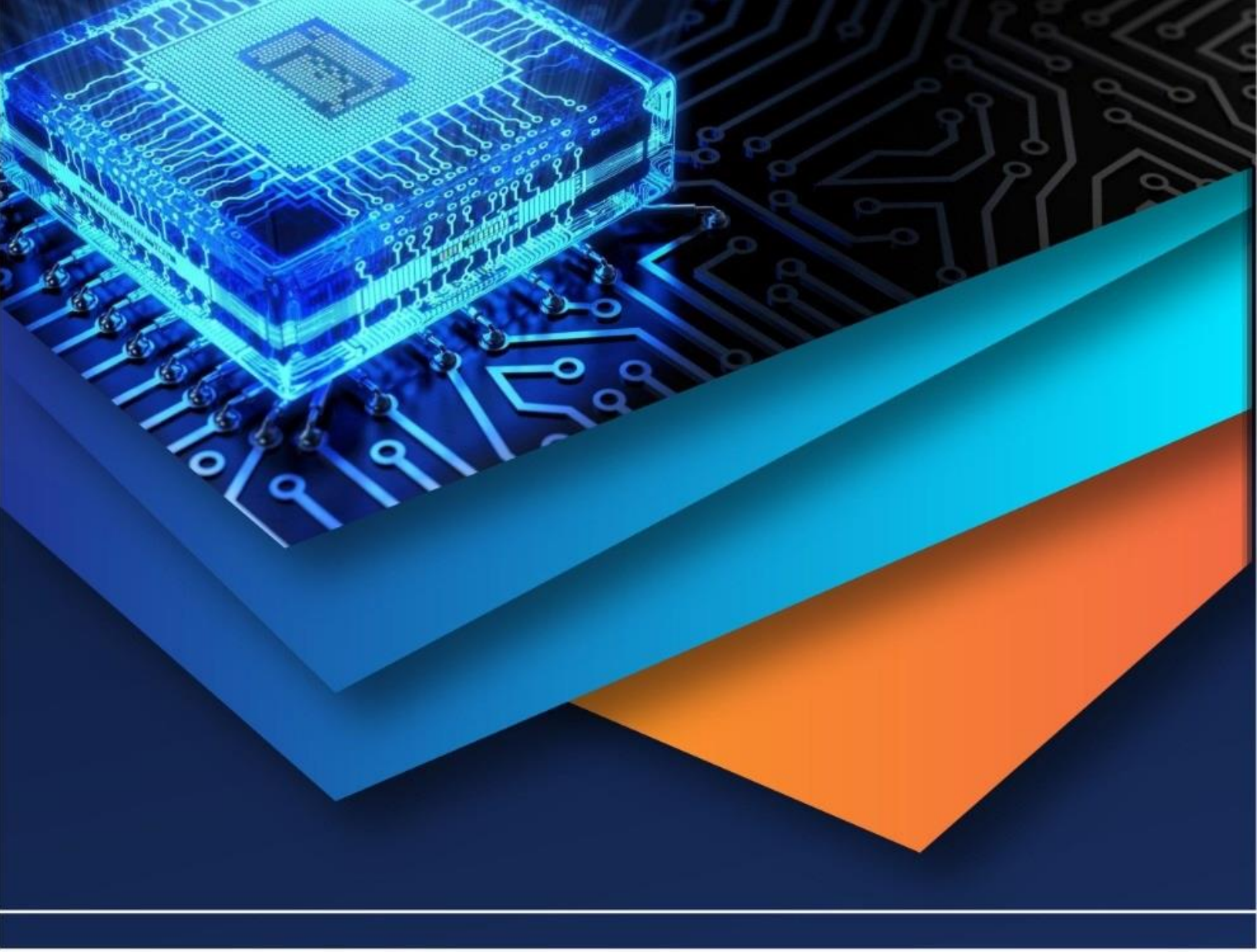
In this paper we have discussed the various application/session layer protocols available for use in a smart home environment. We have presented the application player protocols that have gained much popularity and widespread usage in the recent times, by comparing analyzing their performance and requirements. Our study shows that there are several factors that may affect the selection of the appropriate application layer protocol. While selecting a protocol, we need to consider the computational and communication abilities of the devices, the battery life and the target application. Hence it is not easy and advisable to select one protocol as superior over others. The selection of a particular protocol depends on the application. Table 1 summarizes the comparison of the characteristics of different application layer protocols and their suitability under various applications. The merits and demerits of these protocols are discussed in Table 2.

After carefully analyzing the various existing application layer protocols and identifying their usefulness in the world, we have decided to implement these protocols to obtain an experimental comparison among them. Context-aware resource discovery is much expected in smart home environment. Our future work is proposed to design and develop an improved dynamic context level

application layer protocol that can act accordingly depending on the situation. Our final result should be an easy to use dynamic protocol that is suitable for use in the smart home environment.

REFERENCES

[1] Giddens A. (1984), 'The constitution of Society: Outline of the Theory of structuration', Univ. Of California Press.
[2] Davey, A.J.,& Paolucci, B.(1980), 'Family interaction: A study of shared time and activities, Family Rlations', 43-49
[3] U.S. Census Bureau, (2016), Current population survey annual social and economic supplements, 1960 to 2016. https://www.census,gov/hhes/families/files/graphics/HH-4.pdf
[4] G.Chen and D.Kotz,"A Survey of Context-Aware mobile computing research", Department of Computer Science, Darmouth College, Technical Report 2000.Moeiz Miraoui, Nesrine Rtimi, Rim Cherif and Chakib Tadj, "Context-aware Services Adaptation for a Smart Living Room", 2014 IEEE
[5] Pablo Calcina Ccori, Laisa Carolina Costa De Biase, Marcelo Knorich Zuffo, Flavio CSoares Correa de Silva, 'Device Discovery strategies for the IoT', IEEE International Symposium on Consumer Electronics, 2016
[6] T.A. Butt, I.Phillips, L.Guan and Oikonomou, 'Trendy: An adaptive and context-aware service discovery protocol for 6LoWPANs', in proceedings of the Third International workshop on the Web of Things, ACM, 2012.
[7] Andras Kalmar, Rolland Vida, Markosz Maliosz,'CAEsAR: A context aware addressing and routing scheme for RPLnetworks.
[8] Kim Rowe,'Internet of Things Requirements and Protocols', Embedded computing, 2015
[9] Tara Salman,'Networking protocols and standards for Internet of Things', http://www.cse.wustl.edu/jain/cse570-15/ftp/iot_prot/index.html
[10] Y. Fathy, P.CBarnaghi and R. Tafazolli,"Large Scale Indexing, Discovery and Ranking for the Internet of Things(IoT)", ACM Transactions on the Web, Vol.9,No.4, Article 39, March 2010.
[11] D.Locke, "MQ Telemetry Transport(MQTT) v3.1 protocol specification", IBM Developer works Technical Library 2010.
[12] Frank T, Johnson, Trude H.Bloebaum, Morten Avlesen, Skage Spjelkavik, Bjorn Vik, "Evaluation of Transport Protocols for Web services".Military Communication and Information system Conferences, 2013.
[13] Karagiannis, Periklis Chatzimisios, Francisco Vasquez-Gallego, Jesus Alonso-Zarate," A survey o n application layer protocols for the Internet of Things", Transaction on IoT and Cloud Computing, January 2015
[14] M.R. Palattella, N.Accettura, X.Vilajosana, T.Watteyna, L.A.Grieco,G.Boggia and M.Dohler, " Standardized Protocol Stack for Internet of (Important) Things", IEEE communication surveys & Tutorials, 2013
[15] .A. Alghamdi, A. Lasebae, M.Aiash, "Security Analysis of The Constrained Application Protocol in the Internet of Things", Second International Conferenc
[16] P.Saint-Andre, "Extensible messaging and Presence Protocol(XMPP): Core", 2011. Available at http://tools.ietf.org/html/rfc6120. untrusted service providers and curious buddies", The International Journel on Very Large Data Bases (VLDB), 2011
[17] Rowe, "Internet of Things Requirements and protocols", Embedded Computing, 2015.
[18] Yoon G., Choi J., Park H., & Choi H.,"Topic Naming Service for DDS", International Conference on Information Networking(ICOIN), IEEE, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY