iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** I **Month of publication:** January 2020

DOI: http://doi.org/10.22214/ijraset.2020.1028

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: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

A Survey on Contemporary and Core IoT Standards and Protocols

Meghana M
Department of Information Science and Engineering, VVIET, Mysuru.

Abstract: ***In today's world of connectivity, IOT has become the new promising magic pill that helps in exchange of information across a million of devices for the better technological growth towards a smart and healthy society. There is no doubt ,that IOT has changed the scenarios drastically helping to make best use of 'connectivity' element in devices and making the impossible – a definitely possible phenomenon opening a sea of opportunities in the field of wearables, smart home automations, connected healthcare, cyber security, smart farming, connected cars, supply chain, retails etc., To make things work, it is highly important that all the functional elements forming the IOT framework must be chosen exactly according to the need of the specific application. Be it the low-power short range networks, IOT processors, analytical tools and algorithms for building the models, associated APIs(Application Programming Interfaces), simple yet strong security mechanisms, device management approaches, various other platforms , IOT applications have to be highly interoperable across a variety of technicalities. But a swift growth of IOT is raising a new hurdle – 'Standardization'. Though standardization involves the implementation and development of technical standards based on the consensus of different alliances such as users, firms, interest groups, governments and other standard organizations, IOT standardizations are becoming increasingly complex. An IOT standardization process has to be highly vigilant, and a lot of coordination ventures are needed to be able to make sure that the devices, networks and applications from different parts of the world connect and exchange information following the established standards set up. To embrace the new emerging technologies, it is required that various IOT standards such as Identification standards, Network standards, Security standards, Data standards etc., must be enabled with appropriate design and implementation procedures.***
Keywords: IoT, interoperability, standardization, Identification standards, Network standards, Security standards, Semantic interoperability.

I. INTRODUCTION: WHY STANDARDIZATION?

Today, the best part about companies manufacturing IOT devices is that the consumers have a lot of options to choose their products, to make choices among the latest specifications, the availability, features, cost comparisons and a lot more. But also due to the competition among the growing brands, vendors force the consumers to clasp onto their products so that the dependability factor and hence the business increases. But it's also important for the manufacturers to realize that consumers look for a multiple range of features to fit in their requirements and would select those that best suits their products no matter the services offered are from different companies. For instance, the smart cars these days have an embedded system to detect if the temperature of the car is maintained optimally to make sure it is always ready for the drive. The security system which ensures that the car owner is informed of these automated actions taken place within the car and has complete control of it, has to be in pace with the temperature control system. Usually, we find that the vendors producing automated environment control systems don't worry about keeping the safety measures in par and the other way round. Hence it's extremely important that there has to be a platform that allows versatile devices to operate together and in sync with other systems which helps a lot of device manufacturers to work together without actually having to develop products different from their core specialization. As with the cost, it is advised to keep better prices for the latest, most desirable and fresh products providing greater economical edge to the business as well as consumers. This is where the technical standards come into the picture. It's always fascinating and trouble free for the users to operate and work with those products that easily fit into various systems. To set up and monitor these standards, there are many organizations involving software firms, device manufacturers, service providers, open source forums and many such companies basically playing vital roles in contributing to the development of well-established standards for the ease of IOT functioning and interoperability. Few of them worth mentioning are IETF, CASAGARAS, ETSI, EPC Global, W3C, IEEE, OASIS, OGC etc,. Most of the IOT challenges can be hence solved using comprehensive standardization framework with integrated standards under a single vision and thus enable a more efficient, seamless connectivity all the time by dynamically consolidating diversified capabilities. The value and commercial viability of IoT will have tough time to perform at best unless the standards are implemented.

II. TYPES OF STANDARDIZATION

There are a number of evolving IOT standards which are expanding the vast and different capabilities of various devices. Beginning with networking, routing, security, manageability, device interoperability, application level interoperability and a non-exhaustive list of standards are now in the field to facilitate easy working of the devices together. In this paper, we focus on the core interoperability standards at networking level, device standards, security and privacy standards.

A. Networking Standards

The wireless network protocols play a circumscribing role in IoTs, and have grown hugely in the last half decade. We restrict our discussion to the most recent and commonly used networking standards which mainly includes IEEE 802.11ah also called HaLow, IEEE 802.11af known as White-Fi, LTE-M, LoRaWan, Thread, ZigBee. Communications at the elementary level are greatly influenced by the standards that are used for the information exchange between the devices.

1) *IEEE 802.11ah(HaLow):* The products assimilating the IEEE 802.11ah standards are named as WiFi HaLow by the WiFi Alliance Group. This wireless networking standard was released in 2017 and has an edge of wider coverage range of about 20 kms and higher data rates. It is a low-energy consumption entity, where the stations are combined together to reduce the contention on the air media, utilize relay to expand their reach up to 900-MHz band and the predefined wake/doze periods are highly helpful in lowering the power consumption. WiFi enabled companies working on sensor level technology can make use of the HaLow to ensure a good penetration despite the structural obstructions . Though promising, HaLow is not a yet a global standard and is usually found in products designed and deployed in some parts of U.S, Europe and China.
2) *IEEE 802.af(White-Fi):* The most sought-after solution for connectivity White-Fi uses many unused channels at once, it performs well for very long range devices, up to several kilometres and with high data rates. But the downside is that the channels are different based on geo-locations and since the same channels are not available everywhere, device vendors are not ready to incorporate this standard. Even though it offers long range wireless networks and little power consumption like HaLow, the very purpose of ‘standardization’ to fit into everything is lost.
3) *LTE-M(Long Term Evolution for Machines):* This is a type of wide area network standard best suites the IoT with secured cellular networks for long range communications, that offers little power consumption enabling a wider range of cellular devices and services. Higher data rates, security, voice over the network, ability to stay intact even during a power failure and mobility like features look attractive, but the higher cost and the bandwidth consumptions will disappoint a little. Also known as 4G, it is capable of providing worldwide connectivity and helps in tracking the mobile devices over long distances. Because it works over the cellular networks, it can also be utilized to observe, control and receive critical data from various IoT devices stocked into trains, ships, trucks etc., Since it is supported by 3GPP and GSMA, there is always a door open to get back to 3G/2G when LTE network is not available.
4) *LoRaWan(Low Power Wide Area Network):* A very simple proprietary networking standard which is defined and controlled by LoRa Alliance is LoRaWan. It focuses on wide area networks and is suitable for long range communications. Here gateways are used to transmit messages between end devices and servers and the wireless communication is based on the single-hop link between them. LoRaWan works across the unlicensed radio spectrum by making use of lower radio frequencies with a longer range. There are regional specifications officially defined for LoRaWan, as there are country-specific limitations. The cost considerations are relatively low and it uses software-based AES-128 encryption for security.
5) *Zigbee*: Zigbee is an obvious choice for the device manufacturers when they are only interested in incorporating the most fundamental features like- connectivity, security and coverage. It is a low power, low data rate based on mesh network topology suitable for home and office utilities in a small network area covering up to 100 meters LOS. Zigbee Alliance owns the Zigbee standard, and is responsible for defining the specifications, maintenance and publication of standards. The closer proximity and lower data rates highlight the longer battery powers to last for years. It is based on IEEE 802.15.4 specification that has wide range of applications in IoT healthcare devices, home automation, low power devices designed for small scale industry. To make things easy for IoT devices to work together, Zigbee has also introduced a new open standard language for the IoT, known as ‘dotdot’ and is now ready with the latest Zigbee 3.0.
6) *Thread:* Thread is another popular mesh networking, IPv6 compatible, low power consuming wireless networking standard built upon IEEE 802.15.4, it carries IPv6 packets over 6LowPAN (low power personal area network). Known for its low power consumption and high security, it is relatively easy for the consumers to install, add, authorize and remove devices across the network. Home automation systems comprising of numerous sensors, actuators and many such devices in order to be able to communicate with each other using a common standard makes immense use of Threads.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

Z-Wave and Sigfox are the other contemporary IoT communication standards that also consume less power and used primarily for network communication. But due to the challenges faced and onset of latest standards, that are much more competitive, more attention is garnered by the above mentioned technology standards.

B. Device Standards

IoT devices which are the cells of IoT frameworks talk to each other and work together in sync to perform the specified task. Smart homes, Smart meters and a non-exhaustive list of applications make use of IoT devices to alert and notify users about various scenarios using the sensors, gateways, actuators. Every day, every action in controlled environments integrated with a large number of IoT devices are making our lives easy. In a way, we are trying to build a digital nervous system which can see, hear, speak, sense, locate variety of information. But majority of these IoT devices are constrained in one or the other way, lacking better UI features, battery power, memory, computational powers, sufficient bandwidth etc.,

Despite these drawbacks, the IoT devices today are capable of connecting and communicating with internet and cloud based services/applications for smart operations. In order to connect to any service across the network, we use a range of standards to identify, control and manage these IoT devices. Some of them are discussed below.

1) *Device Discovery:* A group of standard protocols which identify services hosted on cloud and get connected to it include mDNS, DNS-SD, Simple Discovery Service Protocol. The important ones are as follows.

a) *mDNS(Multicast Domain Name System):* mDNS is a domain name system kind of protocol to identify the IP address given the host name of a system. Since it requires no auxiliary infrastructure , it is extremely useful in small networks that does not contain a local name server. It is published as a RFC 6762 standard. The unicast DNS packet format is used in its payload structure.

b) *DNS-SD(DNS based Discovery Service):* This is a popular service discovery protocol that only utilizes existing records without needing any new records or messages to circumvent any fundamental variations in the underlying DNS protocol. It is used to resolve the services available in a network efficiently by ensuring that the host names remain intact despite the changes in its IP addresses.

c) *Simple Discovery Service Protocol:* Devices make use of this protocol to easily communicate with each other through plug and play utility by enabling the users to perform the minimal actions and configurations from their end. Control points in Universal Plug and Play network use this protocol search for the devices, services provided by them and their accessibility.

2) *Device management and Self configuration:* One of the greatest problems the companies face today as a consequence of multitude of devices and different standards to which they conform is " device management". Usually, every device manufacturer deploys and uses a proprietary management software called 'ecosystem' in IoT. Most commonly used are explained in brief.

a) *LwM2M(Lightweight M2M):* The standard LwM2M protocol is light, quick, well-built and best suited for low capacity devices. This protocol from OMA(Open Mobile Alliance) has multiple functions such as device management over sensor/cellular networks, increase the requirements of applications, transfer service data from network to devices across the network etc.,

b) *TR-069(Technical Report 069):* TR-069 is a well-known standard that has to be proven as the one that is deployed by many of the service and network providers to assist with the tasks of monitoring and diagnostics, software management and auto configurations by employing CPE(Customer Premises Equipment) to manage the remote network devices. Networking devices such as routers, gateways and modems are provisioned under this standard.

c) *OMA-DM(Open Mobile Alliance – Device Management):* OMA-DM is a device management standard more of which is concerned towards the mobile devices such as tablets, PDAs, mobile phones etc., and assist in preparing the device before using it, to set up and configure parameters and certain settings, to provide patches , report bugs and their fixations.

3) *Device Identity*: A strong identification mechanism needs to be in place, to verify the authenticity of the IoT devices in the functioning system. Such standards will secure the IoT devices and will create a immutable identity for each of them. It is to be noted that only after the device is proven to be authentic, it must be allowed to participate in the communication. Few standards which covers device identification are briefed below.

a) *EPC(Electronic Product Code) :* EPC is a unique identifier standard that universally identifies every object present physically in any part of the world and designed as a supple framework that provides support to the already present coding schemes currently found in barcode applications. It serves as an industrial standard for global RFID usage. It has variety of representational forms like binary format compatible with RFID tags, text formats supported in enterprise systems for data sharing etc,.

b) *uCode(Ubiquitous code):* uCode is another unique device identification standard associated with physical objects that uses 128-bit code to uniquely identify objects. It is controlled by a uID centre in Japan that handles the root server and the servers of Top Level Domain(TLD) and Second Level Domain(SLD) . uCode can be in the form of RFID tag, acoustic tag, active RF/Infrared tag or a print tag like barcode or QR code.

c) *IPv6:* IPv6's critical role in IoT's growth is very obvious by now from the way the exponentially increasing IoT devices are addressed with 128-bit long IP addresses. Identifying every single IoT device on every nook and corner of the globe is made possible because of IPv6 standard that comes with a bundle of advantages such as auto-address assignments of the devices, automatic exchange of IP configuration data, security etc,.

d) *URI's(Uniform Resource Identifiers):* Another identification standard for accessing the devices over a network specified by IETF is URI.As per the IETF specifications, the resources does not necessarily have to be web elements , but can also be door sensors, microprocessor chips or others.

C. Security Standards

The heterogeneity and large scale structure of IoT devices and multiple networks are the toughest parts of IoT security which have multiple challenges to be addressed.

Beginning with the object identification part of ensuring the integrity of the IoT devices, its authentication, authorization, preserving data privacy, encryption techniques to controlling IoT malware, every step requires a lot of precautions and evaluations to meet the security requirements through well-defined, verified standard protocols.

End-to-end security mechanisms ensure that the devices communicate safely, without being altered by third party in the middle of the communication and all the messages are encrypted that only authorized users can manipulate the data. Above mentioned security characteristics are better handled by TLS(Transport Security Layer) protocol and X.509 certificates.

It's important to note that there are many standards available at different layers of IoT stack such as at device level, network level, application level and these technological standards specially pertaining to security is a vast topic as there is a large number of organizations working towards developing secure IoT protocols such as IoT Security Foundation, IEEE, The Online Trust Alliance, ETSI, The Open Web Application Security Project, NIST, IoT IAP, IRTF and many more.

We will limit our discussion to some of the prominent security standards defined at different levels such as COSE, OSCOAP, ACE,EDHOC, EALS(application layer protocols), 6LowPan, IPsec and RPL security defined at network layer, IEEE 802.15.4 at data link layer.

1) *COSE:* The Object Signing and Encryption is a IoT security protocol based on CBOR(Concise Binary Object Representation) which is an encoding format enhanced for lightweight parsing in constrained devices. Processing of signatures, MACs, details of the encryption, the keys used for encryption and their representation using CBOR are described using COSE.
2) *OS CoAP:* Object Security CoAP is an end to end security mechanism for CoAP based on CBOR and COSE that performs HTTP-CoAP proxy functionality, upholds notifications and fragmentation schemes specified for CoAP , CoAP proxy forwarding operations and also provides security for group communications in CoAP.
3) *ACE (Authentication and Authorization in Constrained environments):* This security protocol defined at application layer specifies a variety of communication and security mechanisms between Client and Resource Server such as MQTT profile, OS CoAP and DTLS profiles to sustain different IoT deployments.
4) *EDHOC(Ephemeral Diffie-Hellman Over COSE):* Another security protocol that works at the application layer is a light weight key exchange protocol where message exchanges are based on CBOR and COSE where session keys are established with perfect forward secrecy. Other offerings of this protocol are identity preservation, mutual authentication etc,.
5) *EALS(Enrolment with Application Layer Security):* A certificate enrolment protocol that works at application layer specifies public key certificate enrolment procedures authenticated with application-layer security protocols suitable for IoT deployments.
6) *6LowPAN:* Currently leading technology in IoT communications enabling end-to-end IPv6 communications between the nodes that helps in providing distributed sensing applications. It's adaption layer portrays the services needed by IP layer on the services offered by IEEE 802.15.4 MAC layer. Secure and non-secure modes are the 2 modes in which IEEE 802.15.4 layer functions in which the secure mode addresses security issues such as integrity, confidentiality, access control and non-secure mode also known as Access Control List mode only suffices to provide limited security features.
7) *IPsec(Internet Protocol Security):* The collection of security protocols for Internet which mainly uses cryptography and other authentication mechanisms to ensure confidentiality and integrity in the end to end communication.

8) *RPL security:* A network layer security protocol that is based on distance vector routing extending support to integrity and message confidentiality with the help of 3 security modes namely 'Authenticated mode' responsible for device authorization before network admission, 'Pre-installed mode' to monitor the integrity, confidentiality and authentication of data of the symmetric keys that are pre-configured and 'Unsecured mode ', the default one to assist in the transmission of RPL control messages. It uses AES 128-bit keys for encryption.
9) *IEEE 802.15.4:* A Zigbee based security protocol for low power, low cost protocol to acquire the desired level of protection with symmetric cryptography key specifications, specified at the physical and MAC(Media Access Control) layers of the network. Low level functions such as data transmission, link quality indication and clear channel assessment are fulfilled at the physical layer while the MAC layer witnesses frame delivery acknowledgement, channel access mechanism, association and disassociation, frame validation, guaranteed time slot management etc,.
10) *DTLS:* DTLS(Datagram Transport Layer Security) is an end to end security protocol designed from the existing standards enhances the security and protection of messages by ensuring a powerful authentication, confidentiality and integrity during communication. Reordering of messages, eavesdropping, fragmentation, message loss, tampering, DoS(Denial of Service) prevention procedures and duplication of messages are all overcome using DTLS.
11) *X.509 Certificates:* X.509 certificates make use of X.509 public key infrastructure standard to join a public key with an identity enclosed in a certificate. These are the digital certificates that provide maximum security compared to other contemporary security mechanisms issued by a Certification Authority that is trustworthy.

D. Semantic Interoperability

The current progress and developments witnessed in IoT is exponentially increasing and the standardization efforts to offer advanced solutions with cross platform technologies in terms of device, security and networks are drastically growing. But to the other end, there is also this Semantic interoperability which equips various business entities and services to analyse and interpret the information exchanges using several different approaches. IoT is now growing beyond the connectivity of devices, sensors to exchange information but is more focused on creating new opportunities and capabilities, providing more sophisticated encounters to achieve much better and efficient actions. It applies to various layers of the communication stack and applied to have a common understanding of a variety of tokens and labels which are elucidated to the data that is exchanged. Resource Description Framework(RDF) and Semantic Sensor Network ontology(SSN) standards are well known ones in the market.

1) *RDF:* A semantic interoperability standard that is strongly connected and capable enough to bring in data from different applications , directly access, interpret the merged data. The best part is that they can be accessed and used directly without any pre-processing. SPARQL is the query language used for querying the data. Developed by W3C-World Wide Web Consortium, the framework uses XML(Extensible Mark-up Language) and URI(Uniform Resource Identifier) as the distribution standards.
2) *SSN:* SSN is another W3C standard for designing various sensor devices, platforms, observations and environment knowledge serving as a building block to acquire interoperability across different IoT devices. SSN focuses on different sensor perspectives and are set out in terms of accuracy, precision, resolution, scale etc,.

III. CONCLUSIONS

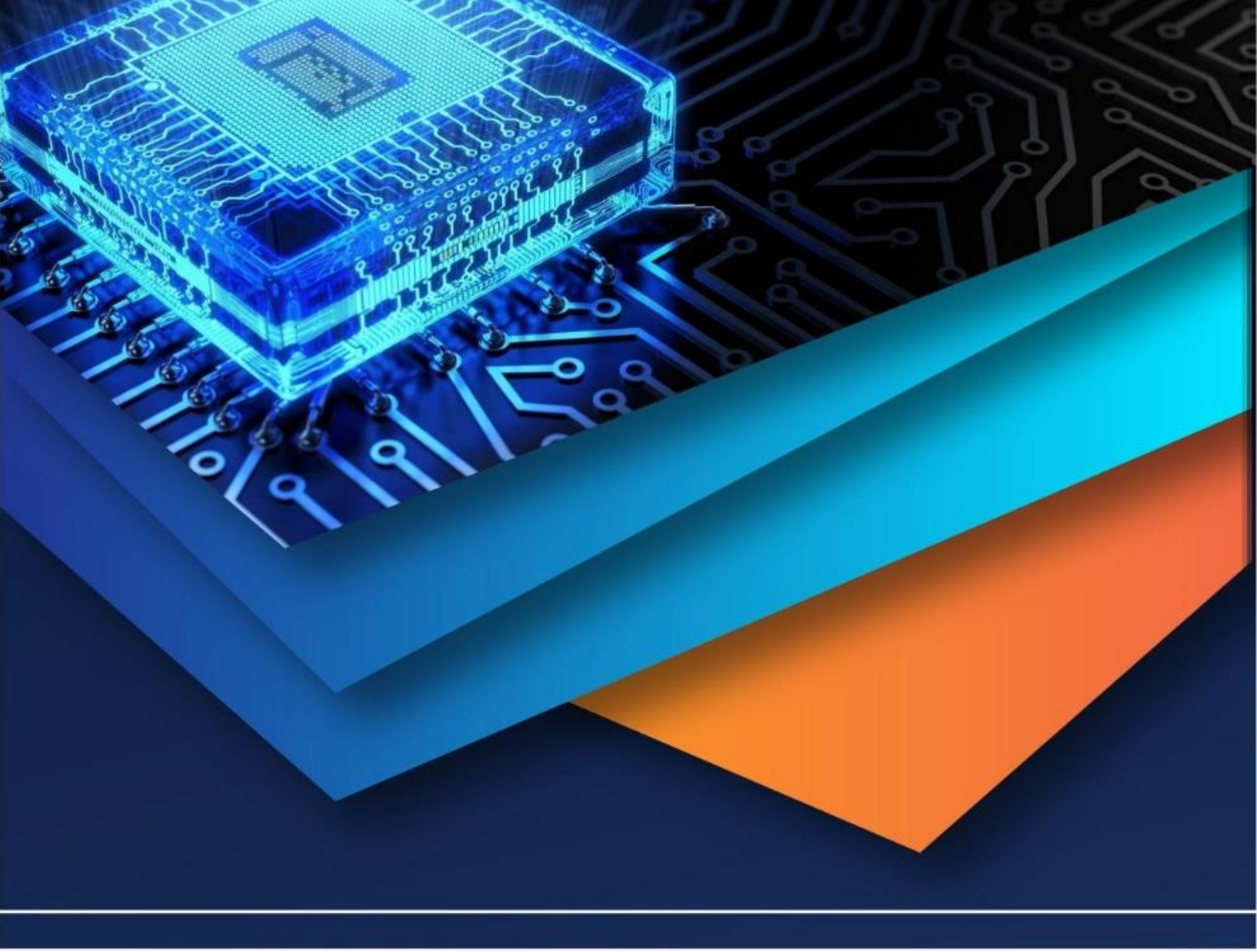
We have so far discussed several standards pertaining to networks, devices, security and privacy and semantics. The discussion here is limited to the most popular and commonly used standards that are most relevant in the current scenario. In every category, the standards are grouped under multiple criteria and a glimpse of each of those standards are reflected. Since network, device and security standards and protocols are the core standards upon which any IoT framework is constructed, this discussion can be considered as a go-to reference for the most recent, relevant standards grouped accordingly based on the application specification. Standardization in IoT is never an easily exhausting arena because of several variety of choices available in the market and its scope expands up to the horizon of available options and specifications to choose from. In the successive research papers, there are many other dimensions of IoT standardizations to be focused on in more depth.

IV. ACKNOWLEDGMENT

I would like to thank all the faculties of Dept. of Computer and Information Science Engineering, VVIET, Mysuru, my parents, family members, friends and anonymous reviewers' encouragement and constructive piece of advice that prompted for a new round of rethinking of research, additional experiments and clearer presentation of technical content.

REFERENCES

[1] Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities STEPHANIE B. BAKER 1 , WEI XIANG2 , (Senior Member, IEEE), AND IAN ATKINSON3
[2] A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications 90(11):20-26, March 2014.
[3] Internet of Things in Industries: A Survey Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li
[4] Borgia, E. (2014) The Internet of Things Vision: Key Features, Applications and Open Issues. Computer Communications,
[5] Semantic Gateway as a Service architecture for IoT. Interoperability. Pratikkumar Desai, Amit Sheth and Pramod Anantharam.
[6] IETF Standardization in the Field of the Internet of Things (IoT): A Survey .Isam Ishaq *, David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester
[7] A Survey of Protocols and Standards for Internet of Things Tara Salman, Raj Jain.
[8] Making sense of interoperability: Protocols and Standardization initiatives in IOT Ronak Sutaria, Raghunath Govindachari, Mindtree Research Labs, Bengaluru, India.
[9] A Survey on Security and Privacy Issues in Internet-of-Things Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li , and Hongbin Zhao.
[10] Which IoT Protocol? Comparing standardized approaches over a common M2M application Konstantinos Fysarakis, Ioannis Askoxylakis, Othonas Soultatos, Ioannis Papaefstathiou, Charalampos Manifavas, Vasilios Katos.
[11] Wireless Sensor Networking in the Internet of Things Rohini Anand Nimbekar1 Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Mumbai, India.
[12] IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) - Analyzing its suitability for IoT, Dr. Lakshmi Devasena C, 12.12IBS Hyderabad, IFHE University, India
[13] Wireless Sensor Networks for Healthcare JeongGil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Fellow IEEE, Andreas Terzis, and Matt Welsh
[14] Creating solutions for health through technology innovation Karthik Vasanth , Jonathan Sbert Product Line Manager, Texas Instruments.
[16] https://searchhealthit.techtarget.com/essentialguide/A-guide-to-healthcare-IoT-possibilities-and-obstacles



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY