International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

IoT : Ecosystem, Middleware and Application(s) of IoT

Aniruddha Jathar, Shrikant Bhandalkar
Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

Article Info
Volume 8, Issue 1
Page Number: 314-322

Publication Issue :
January-February-2022

Article History
Accepted :20 Feb 2022
Published: 28 Feb 2022

ABSTRACT

As the world moves towards Metaverse. In the near future, billions of IoT devices will be interconnected via the Internet. Due to the nature of the IoT environment, it is vulnerable to hostile attack.To maintain sustainability in IoT ecosystem, this paper evaluates some of the middleware software improvements required in IoT world. AS we know there are many devices interconnected to each other a software called middleware is required for intelligence for IoT exchanging of data from multiple devices and also allows them to communicate with each other and collect data to make smart decisions. IoT middleware also analyzing the data to make the best operation approaches which are needed for various modules as well proposes security for the software. Also, this paper discusses some of the applications of IoT in near future. In this paper effort has been made to put the new and innovative applications of IoT in near future.

Keywords: -Ecosystem; Ecosystem Layers; Middleware; Processing; Applications

I. INTRODUCTION

With the improvements in the latest technology and the rapidly increasing pace of total number devices, it is estimated to have around 46 billion devices connected to cloud by 2023 worldwide, pushing the world into Industry 5.0. This will have user enabled with more cloud-based services which are provided by cloud service provider (CSP) [1] However, due to its heterogeneous and complicated architecture it raises multiple security issues and challenges. As IoT is open in nature IoT environment makes it vulnerable and susceptible to security and privacy of the user. As there are billions of IoT devices which will interact with each other by sharing information over the public networks. This, invites intruders to interfere and steal the important and private data from the system and obtain critical information. Also, if security measures are not deployed properly there can be many problems to the user due to lack of essential credentials from their device.

As for the applications in IoT we can interconnect multiple devices either they are heterogenous or homogeneous in nature having overlapping transmission range over each other so they can communicate efficiently.

For example, when a user is watching TV in the 's living room, a sensor installed in the refrigerator needs to refill the 's water bottle in the refrigerator because the water level has reached the threshold. If

the sensor detects that, the refrigerator broadcasts a "search"-a person who generates a message to all sensors installed in the house, such as the living room, lobby, drawing room, dining room, etc. Finds the location of and gets the information. Can be sent to him, he can go to the fridge and refill the water bottle. All of these sensors are close to the overlap transmission range of 810 meters each, so it is free to communicate with each other and share messages with each other.

II. ECOSYSTEM COMPONENTS

1. **Sensing and embedding components:** We join temperature, spinner, pressure, light sensors, GPS, Electrochemical, Gyroscope, RFID, and so on to procure information in view of a specific use case. For instance, for car use cases, we utilize Light identification sensors alongside strain, speed and imagery sensors. Picking the right detecting parts is a vital stage for a useful use case [2].
2. **Connectivity:** A significant part of the IoT climate is network. Without consistent network between IoT sensors end gadgets, and examination or processing parts, we can't execute a utilization case. Allow us to list down the different modules of network layers [2].
3. **IoT Cloud:** when the data is collected it is transferred to the cloud for processing the cloud is where the high-performance facilities handle the data and stores it to make the decisions. [2].
4. **Analytics DataManagement:** Industry grade IoT arrangements require securing, overseeing and controlling enormous scope crude and handled information. By and large, cloud-based structures are utilized to fill the need in view of business needs. Exceptionally enormous scope associations, equipped for dealing with enormous scope information (as immense as petabytes each *second*) frequently set up their own information focuses to deal with this [2].
5. **End-user devices and user interface:** It is an interface that is easily accessible for the IoT user.This is the place where user can set their preferences and control the system. The interface must be very friendly, which allows user to have better interactions with the user [2].

III. IOT ECOSYSTEM (ARCHITECTURE AND IT'S LAYERS)

- **Perception Layer:**In the perception layer, number of sensors and actuators are utilized to assemble helpful data like temperature, dampness content, intruder detection, sounds. So, on the principal of this layer is to get data from environmental factors and to pass information to another layer. It changes signal over the actual amounts caught and changes over it into simple or computerized signals for additional handling. There is a wide scope of sensors accessible to catch information including area, temperature, direction, development, vibration, speed increase, dampness, and so on Probably the most widely recognized sensors utilized in different IoT applications [3].
- **Network Layer:**As the name proposes, it is the interfacing layer among insight and middleware layer. It passes the data to middleware which it gets from perception layer utilizing organizing innovations like 3G, 4G, UTMS, Wi-Fi, infrared, and so forth This is likewise called communication layer since it is answerable for correspondence among discernment and middleware layer. All the exchange of information done safely keeping the got information secret [3].

[3] When portions of the IoT solutions are organized, they actually need messaging protocols to share

information across devices and with the cloud. The most well-known conventions utilized in the IoT biological systems are **DDS, AMQP, CoAP, MQTT.**

DDS (the Data Distribution Service): This service directly interconnects the IoT devices to each other and to applications which are addressing the requirements of real-time systems.

AMQP (the Advanced Message Queuing Protocol): This protocol is used for aiming at peer-to-peer data exchange between servers.

CoAP (the Constrained Application Protocol): This protocol is a software protocol which is designed for constrained devices. As the end nodes are limited in memory and power (for example, wireless sensors). It is almost like HTTP but uses fewer resources.

MQTT (the Message Queue Telemetry Transport); This is a lightweight messaging protocol which is built on top of TCP/IP stack for centralized data collection from less-powered devices.

- **Processing/Middleware Layer:**Middleware Layer has a few progressed highlights like storing, calculating, processing and action taking capabilities. It stores all informational index and in light of the gadget address and name it gives fitting information to that gadget. It can likewise take choices in light of computations done on informational collection acquired from sensors [3].

[5] All the data is handled here and as it flows through it is handled via IoT platform which includes two major stages: **i] Data accumulation stage**

ii] Data abstraction stage

i] Data accumulation stage: The constant information is caught by means of an API and put to rest to meet the prerequisites of non-real-time applications. The data gathering part fills in as a mid-point between event-based data generation and question-based data usage.

ii]Data abstraction stage: In data abstraction, data preparation is fixed so that user using the applications can use it to generate insights. The whole process has following steps:

a. Combining data from different sources, both IoT and non-IoT devices.

b. Reconciling multiple data formats; and

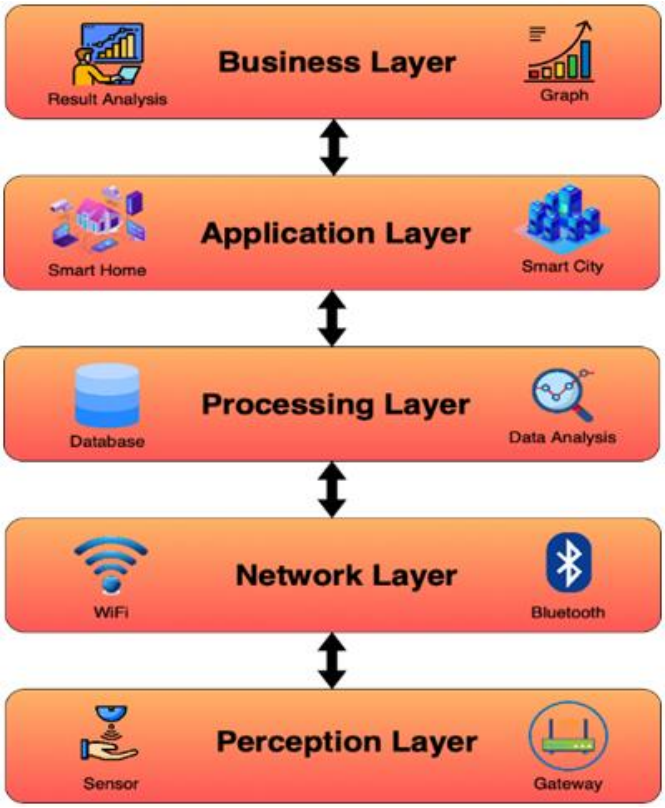
c. Aggregating data in one place or making it accessible regardless of location through data virtualization.

- **Application Layer:**An application layer is also called as an Abstraction Layer. The application layer deals with all application cycle in according to the data got from middleware layer. This application includes sending E-mails, actuating caution, security framework, turn on or off a device, smartwatch, watering plants and so forth. Application layer deals with the application-based services to the consumer and defines all the applications of IoT which has been deployed. It has the authority to provide the things needed for the applications [3].

There may be many services for lots of different applications depending on the data gathered by the sensors. Some of the application layer protocol are as follows: CoAP, MQTT, AMQP, RESTful HTTP, SMQTT, DDS, XMPP, MQTT-SN, etc. [3].

- **Business Layer:** Business or domain logic is carried out in a layer called as business layer i.e., all rules and regulations that are particular to the problem that the application has been built. The accomplishment of any application doesn't rely just upon advancements utilized in it yet in addition how it is being conveyed to its buyers. Business layer does these undertakings for the gadget. It includes making flowcharts, charts, examination of results, and how gadget can be improved, and so on [3].

The information produced in the previous layers brings meaning and importance only if it results in a problem-solving solution and meeting with the goals of the business [3].



IV. MIDDLEWARE

As the name proposes, middleware is a product that is situated in the center (between two things). The essential objective of a middleware is uniting various frameworks so they can communicate with one another. The job of middleware isn't just to empower correspondence however to work with it. No middleware can be applied to each situation, so they are for the most part worked for explicit or set of situations. In the writing IoT middleware arrangements are now and again alluded to as IoT stages or IoT middleware stages in light of the fact that by and large, the middleware is a stage, however it isn't the main sort of IoT stage. In IoT, middleware goes about as an interpreter. To show it, envision a situation where three individuals from various identities banter. In the event that they don't have a typical language among them (the normalization choice), they would require an interpreter interceding the discussion. Presently envision that the three individuals are various applications (APPs). Applications convey through APIs (the language), each APP has its own API. Without a middleware (the interpreter) each APP must-see each different API. This straightforward thought permits clients to zero in on the issue, on the grounds that rather than realizing how every application functions, clients control information from one application (the middleware) [4].

Microsoft Azure IoT Suite is an IoT middleware platform which has been developed by Microsoft. It supports MQTT, AMQP, and REST communications with its server. Their business model is PaaS Azure services easily allows interaction with such as machine learning, Data warehousing, and much more this is the biggest advantage of all [4].

Amazon IoT platform isan IoT middleware platform which has been developed by Amazon. It supports MQTT, REST, and WebSocket's communications with its server. One of the biggest best thing about of Amazon IoT is that it easily allows the customers to interaction with other Amazon services such as S3, CloudWatch, Machine learning, etc. Amazon IoT platform business model is PaaS [4].

V. REFERENCE MODEL FOR IOT MIDDLEWARE

[4] Whenever IoT is advanced, wonderful situations are introduced where contraptions concentrate on client propensities and furthermore respond to them, working on personal satisfaction and client experience. The majority of the introduced situations wrap up with a sentence like this one: "all of this with negligible human mediation." These situations are just conceivable on account of middleware stages that incorporate information from every one of the gadgets and follows up on it. Hence, Middleware is available in most IoT situations. Gathering information and respond appropriately is an urgent element in IoT on the grounds that most gadgets are little, and asset compelled to settle on complex choices. Accordingly, the middleware stages are liable for part of the insight in IoT. To satisfy their

objectives, the modules of an IoT middleware stage engineering should reflect IoT requirements as follows: **i)interoperability, ii) persistence and analytics, iii) context, iv) resource and event, v) security and vi) Graphical User Interface (GUI).**

Interoperability module: The IoT is a heterogeneous climate, and the middleware stage is the integrator. Accordingly, it ought to give an API that permits programming to open functionalities to different applications and things without sharing real code. Programming interface demands made by things/applications can be performed through any convention, so the middleware ought to at minimum help the most well-known IoT application conventions, like CoAP, MQTT, and HTTP(S). The module ought to likewise uphold standard information portrayal techniques, as XML (extensible Markup Language) and JSON (JavaScript Object Notation), as well as paired encodings (Apache frugality, Google convention support), another information portrayal that is arising for IoT is SenML (Sensor Markup Language) [4].

Context module: In a correspondence, setting gives significance to a discussion. IoT conditions are relied upon to adjust to environmental factors and setting will assume a huge part in such manner. A framework is setting mindful on the off chance that it is equipped for giving pertinent data or administrations as per the assignment requested by the client. As to cooperation, frameworks are grouped into three degrees of context-awareness: i) Personalization, ii) Passive, and iii) Active [4].

- Context-awareness personalize is the point at which the framework screens the climate and recommends activities as indicated by the checked information (e.g., a client strolls into a room, and the framework inquires as to whether he should turn on the lights) [4].
- Passive context-awareness is the point at which the framework screens the climate and follows up on the progressions to the climate independently (e.g., a client strolls into a room, and the framework independently recognizes assuming that the client can explore through the room and turns on the light with the right level of radiance) [4].
- Active context-awarenessinfluences the capacity to adjust to new conditions or conditions, and is profoundly associated with occasion location/the board. For setting attention to be accomplished, it must be demonstrated. As of late the metaphysics-based demonstrating has become standard, producing various guidelines. A famous standard is OWL (Web Ontology language) that is upheld by W3C (World Wide Web Consortium) [4].

Resource and Event module: For gadgets to be effective in their activities, they should know what they can perform and their inner activity status (battery level, inward/outside temperature, current memory utilization), so they can publicize their assets and find assets from others. Different gadgets are relied upon to speak with each other all the while they could offer same help, and better gadgets are expected to be mentioned again and again than that of the others. This implies that they cannot generally give the best administration, because of memory imperatives (an excessive number of solicitations being handled), or even limitations from the actual world, for example, distance. These issues are a worry connected with the variety of activities and the limits of the little gadget. Middleware stages can limit these issues by overseeing and enhancing these cooperation's [4].

Security module: IoT won't become well known without attachment and-play. This implies that middleware ought to be adaptable enough for the normal client to deal with. Tragically, simplicity of use (convenience) is challenging to accomplish with the degree of safety required by middleware. Assuming the information could be altered or recovered by a pernicious client or application, the dangers would be boundless. Encryption, for model, is

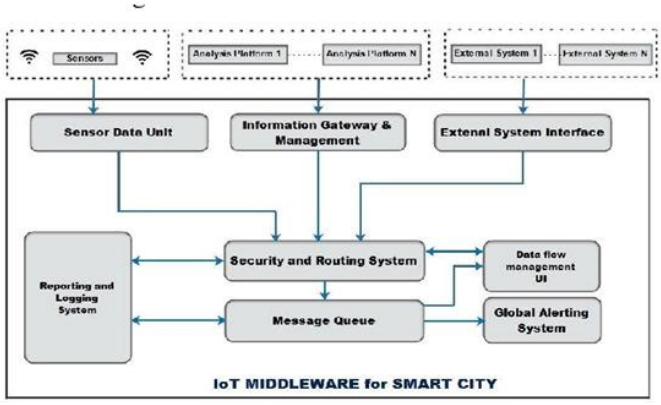
expensive (in regards to handling), so lightweight encryption apparatuses or calculations should be utilized for this objective, along with a lightweight cryptographic convention. Public keys expect that endorsements are refreshed when they lapse, and proliferating these updates to each gadget is certifiably not a basic undertaking. Both cryptography and public keys are essential security highlights that are normal on the current Internet, and their limits in IoT show the issue close by, so every security angle that is effective and can be incorporated only on a strong server is gladly received [4].

Graphical User Interface: A graphical UI (GUI) is an unquestionable requirement for each advanced programming, as it makes applications easy to use. In IoT middleware, the GUI is frequently alluded as Dashboard, in light of the fact that numerous information will be traded, and dashboards present information in a manner that is not difficult to peruse. Regardless of GUIs being so significant, it is normal for open-source middleware stages don't have a local GUI, depending rather on incorporations with outsider applications, for example, Freeboard or Grafana to give dashboards [4].

VI. IOT MIDDLEWARE FOR SMART CITIES (APPLICATIONS)

IoT basically make the universe of machines move towards knowledge by bestowing faculties to them. The faculties or sensors gather the information for the machines or frameworks for translation or handling. The information gathered through these sensors should stream to their assigned handling center(s) furthermore the data produced in the wake of handling should be drifted back to the data via this middleware. The continuous progression of information from the creating end to the consuming end and back can be guaranteed with a lining and directing component. A typical stage which gives a lining and steering system to this information is one of the significant parts of an IoT middleware for smart cities [6].

The IoT middleware for urban communities is a brought together center point where the utility frameworks impart to their own makers, information assortment units, sensors and with every other (required frameworks) for synchronized tasks. This IoT middleware framework likewise comprises of an informing framework, a lining and a steering framework which can course information to any investigation stage furthermore a security framework. [6].

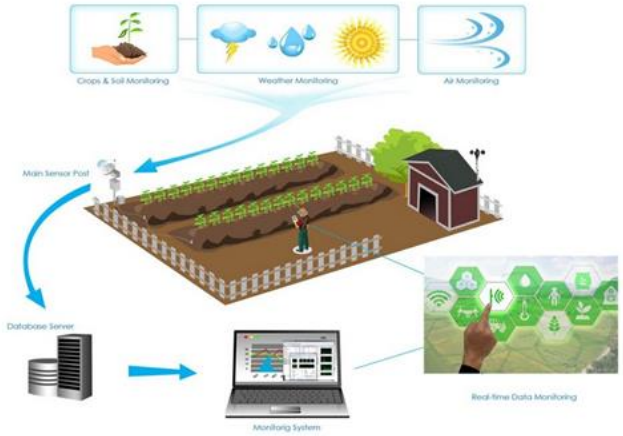


1) Autonomous City:A city turns out to be genuinely brilliant provided that it is an independent city where the heterogeneous utility frameworks and sub-frameworks inside the smart city speak with one another for coordinated activity. A common middleware stage is fundamental towards it [6].
2) Centralized Control for Authorities: In smart city specialists must have a unified control over the information that courses through the different utility and sub frameworks. The specialists should have the option to see the information gained and taken care of by these frameworks. Additionally founded on the necessities the specialists should have the option to course the information from a utility framework to another framework where this information is required [6].

3) Reduced Capex and Opex: A typical middleware for all the IoT frameworks in a brilliant city will diminish the Capex and Opex than individual independent frameworks. Use of equipment and labor supply assets can be expanded by joining all frameworks to a single central point. Various programming permitting cost can likewise be disposed of in such a sending [6].
4) Sustainability and Maintainability: In a smart city the frameworks are sent for longer periods might be never-ending, so manageability and viability are main pressing issues. A halfway made due, adaptable middleware can resolve this issue to an incredible stretch out by giving highlights like rule-based activities autonomous decision-making, real-time alerting, status monitoring etc. [6].
5) Vendor Neutrality: By executing a middleware for all the framework which is a work over open industry norms all the sub framework vendor's will be compelled to keep the guidelines. This will prompt a merchant impartial, interoperable eco framework. This will likewise have an effect in the expense of the frameworks [6].

VII. APPLICATIONS OF IOT

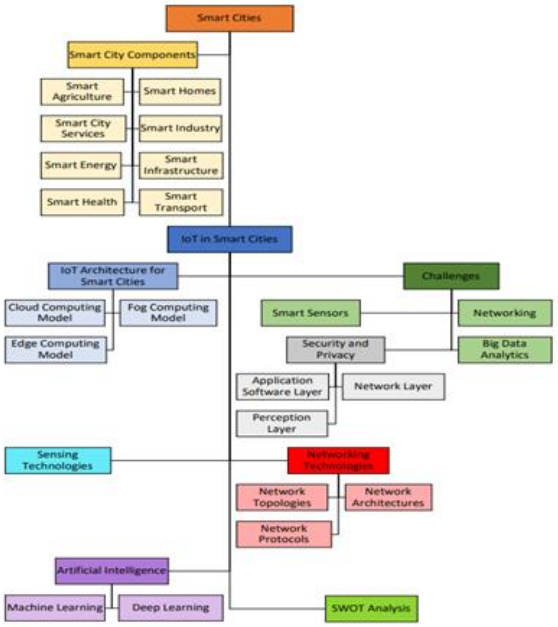
- **IoT in agriculture:** [7] Farming is the foundation of the emerging nation like India. The Failure/Successful development of farming yields of harvest can turn the fortunes of farmer(s) as it would assist him with getting more income for his horticultural produce however it would likewise brag the Gross domestic product of the country. Effort of IoT can impact the existence of the rancher as by organization of the sensor hubs somewhere inside the dirt, can help the ranchers to design the month and season when to plant the seeds, keep the developing sapling solid by keeping it liberated from sicknesses by the use of the right quality and amount of bug sprays, proper and opportune conveyance of water into the dirt so that yield of the crop is high and producers of crops can receive rich benefit of his produce.



- **Disaster management:** [7] IoT can play an important part in anticipating the event of normal disasters like: - Thunderstorm, Earthquake, Floods, Hail storm, Tsunami, Incessant Rains, High Speed Winds, High Speed Tides so that the opportune clearing of individuals should be possible from the impacted area(s) where regular disasters is probably going to struck in near future. The sending of the sensor hubs in the impacted regions and the bury and intra correspondence between the SHIP (Small, Partitioned, Discontinuous and Partitioned) group arranged organization of IoT agreeable hubs helps in the speedy spread of the hubs to the segregated and cut off areas struck by the calamity so the alleviation activity can be start as quick as could be expected and individual scan be protected at the earliest and migrated to safe areas.
- **Medical use of IoT:[8]** In the Urban situation the clinical consideration offices can effectively be given to the people, be it rich or poor however to give clinical and medical care offices to the destitute and oppressed individuals in the hilly landscape is a troublesome undertaking. Also known, the rocky locale is lopsided, rough and hard to walk

and explore. In the event that the emergency is expected to the event of any regular disaster the issues is increased dramatically as the areas would have suffer streak floods and regular avalanches with a result street gets cutoff and the emergency vehicle may not be capable reach to the distant towns and town in the bumpy locale. The IoT is adept for such sort of situations as in the whole region is covered with senor-based equipment node (Radio module) which can be used to detect the overarching conditions in the impacted region and the townspeople can utilize these hubs to send the Alarm or SOS messages to the alleviation and salvage groups with the goal that the group of clinical specialists and paramedics staff can be ship off give clinical offices to the impacted individuals.

- **5G:** [8]5G allows quicker, steadier, and safer availability that is propelling everything from self-driving vehicles, to shrewd lattices for sustainable power, to AI-empowered robots on factory floors.5G is the subsequent stage in the advancement of portable remote innovation, and it is recommended that 5G will bring higher rates, lower idleness, and more dependable availability to gadgets, empowering a large group of new applications in field of IoTs. Therefore, numerous worldwide innovation organizations are in a licenses "ARMS RACE" for aggregating their own 5G-related patent portfolios.
- **Smart Cities:** [10] A smart city is comprised of a few parts which are outlined Shrewd city applications regularly have four viewpoints related with them, the first is the assortment of information, the second is its transmission/gathering, third is the capacity and fourth is investigation. The assortment of information is application subordinate and has been a genuine driver for sensor advancement in the different spaces. The subsequent part is the trading of information, this includes information transmission from the information assortment units towards the cloud for capacity furthermore checking. This undertaking has been accomplished in a few habits, many urban city adventures have city-wide Wi-Fi organizations, 4G and 5G innovations are being utilized, as well as different kinds of neighborhood networks which can convey information either on a nearby level or a worldwide level.



VIII. CONCLUSION

This study was intended to learn more about the ecosystem of the IoT platform, its multiple layers from which we focused more on the middleware and its security. As we have seen that IoT is an ever-growing field of engineering with vast opportunities and ideas to get unfolded using IoT in upcoming years. Also, we discussed about some of the applications which were developed and implemented. However, there are many more fields of applications where IoT can be explored and exploited in different area of SET (Science, Engineering and Technology). Considering all these facts developers and researchers need to focus on developing and designing more towards IoT

field of research. Thus, in this manner we can get a safe and helpful IoT environment in our day-to-day life.

IX. REFERENCES

[1]. Shafiq Ul Rehman, Parminder Singh, Selvakumar Manickam "Towards Sustainable IoT Ecosystem" 2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE)

[2]. https://learn.g2.com/iot-ecosystem

[3]. https://www.geeksforgeeks.org/5-layer-architecture-of-internet-of-things/

[4]. Mauro A. A. da Cruz, Joel J. P. C. Rodrigues, Senior Member, IEEE, Jalal Al-Muhtadi, Valery Korotaev, Victor Hugo C. Albuquerque, Member, IEEE "A Reference Model for Internet of Things Middleware" IEEE Internet of Things Journal

[5]. https://belkiot.in/5-layer-architecture-of-iot/

[6]. Tintu Joseph1, Roopesh Jenu1, Ajmal K Assis1, Sajith Kumar V A1, Sasi P M1, Dr. Alexander G1 "IoT Middleware for Smart City (An integrated and centrally managed IoT middleware for smart city)"

[7]. Sapna Chaudhary, Rahul Johari, Riya Bhatia "CRAIoT: Concept, Review and Application(s) of IoT"

[8]. https://www.mewburn.com/news-insights/top-5-fields-of-technology-for-internet-of-things-iot-patenting

[9]. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/5G-iot

[10]. Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar, Adel Elmaghraby "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges"