A survey on IoT architectures, protocols, security and smart city-based applications.

:-Reviewed and Summarized by

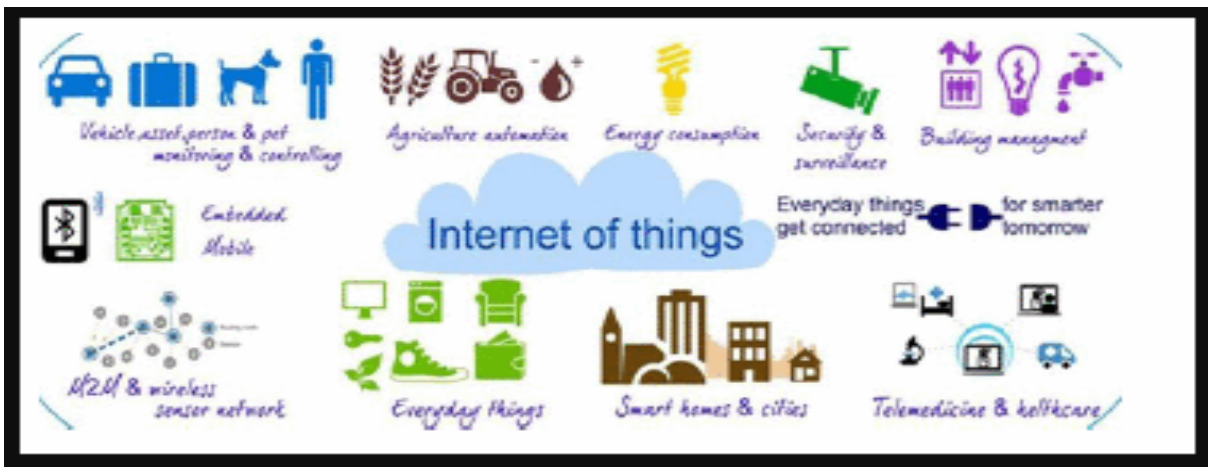
Harsh Kumar

AI &DS 'A'

Introduction:

In the introduction of the paper the publisher has mentioned how IOT have become an integral part of our lives. It tells through IoT, real world things are a part of the Internet, seamlessly combining physical and digital world. With all this, without a second thought, we can say that IoT is the "Future of Internet". Benefits of IoT are indisputable in every part of life. Development of IoT in current environment foresees many advances in smart cities, smart homes, digital health.

This survey paper presents an overview of IoT architectures and protocols, its security concerns and its smart city based applications of IoT and is positioned for wide novice audience to give an insight into various aspects of IoT.

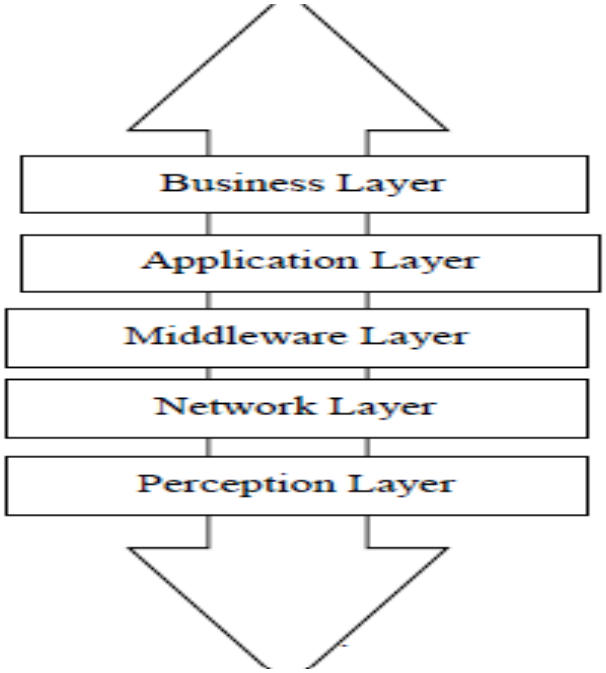


P.C: - Research Paper published by IEEE.

Works Related to IOT

The second section of the paper have been divided into three parts A, B and C where he has explained the IOT Architecture in A, Protocols Iniot (about the protocols and security measures of IoT) and in third i.e. C section he has explained how IoT takes care of security measures by using many technologies looked into the basic and service-oriented architecture of IoT.

- A section very well explains the functionalities of all the layers present in the IOT basic layered architecture, (The perception layer consists of sensor devices viz, RFID, ZigBee, Quick Response (QR) code, etc. to deal with overall device management and to collect specific information by each type of sensor devices. The network layer forwards information from perception layer to upper layers and keeps sensitive information confidential from sensor devices. Functions of middleware layer are service management and storing lower layer information into the database. The application layer manages IoT applications such as smart health, smart transportation, etc. The business layer covers entire IoT applications and services management.) and also tells how it is service oriented by explaining all the four layers(Sensing, Networking, Service and Interface).



- Section B discusses some of the IoT data protocols and how they interact with the IoT gateway.

  One of the protocols mentioned is MQTT (Message Queuing Telemetry Transport) which runs over TCP/IP and provides ordered, lossless connections. It is a client-server messaging protocol that delivers messages with minimized transport overhead. There are three quality of service (QoS) levels for MQTT: "at most once," "at least once," and "exactly once." MQTT also has a mechanism for detecting abnormal disconnections. Another protocol mentioned is CoAP (Constrained Application Protocol) which is used for constrained nodes and networks. CoAP provides a request-response interactive model, supports built-in services and resources, and meets web requirements such as multicasting, minimized overheads, and simplicity.

  AMQP is an open standard application layer protocol that is message-oriented, queuing, routing, and secure. XMPP is a protocol for real-time communication, used in applications such as voice and video calls. WebSocket enables browser-based applications to establish two-way communication with the server, which includes a handshake and message framing. It increases interaction between the

browser and web server as it facilitates the transfer of real-time data to and from the server over TCP port number 80. WebSocket also provides full-duplex communication.

- Section C explains how IoT takes care of security measures by using many technologies; The technologies which it uses are ZigBee, Bluetooth, RFID(Radio Frequency Identification) and Wifi.
  ZigBee protocol, which is a wireless communication standard for short-range applications. It was developed by the ZigBee Alliance and provides low-cost, low-power, and reliable communication. The ZigBee protocol stack contains four layers, which are positioned on top of the Physical and Media Access Control (MAC) layers defined by IEEE 802.15.4 standard. The ZigBee protocol contains Application, Network, and Security layers. Zigbee interfaces directly with the MAC layer which includes services like Access Control, Encryption, Frame Integrity, and Messages in Sequence. Zigbee cryptography uses 128-bit keys and Advanced Encryption Standard (AES) encryption to protect data. Three types of keys are used: Network Key, Link Key, and Master Key.
  Bluetooth protocol, which is an open standard for short-range radio frequency communication. Bluetooth provides four security modes, Security Mode 1-4, that range from no security procedures to security procedures initiated after link establishment. It also provides three encryption modes, Encryption Mode 1-3, to provide confidentiality.
  some of the potential networking threats that Bluetooth technology is prone to, such as Bluejacking, Car Whisperer, and Bluesnarfing. Bluejacking involves sending Short Messaging Service (SMS) to other Bluetooth devices, and attacker can be saved as contact if content is not appropriately documented. Car Whisperer, in this attacker can transmit content to car's speakers or can receive content from microphone in the car. Bluesnarfing is when hackers access Bluetooth devices and get the content of devices through International Mobile Equipment Identity.

(RFID) Automatic identification of things and people is done by RFID. RFID has three components viz., tag, reader and back-end database [16]. RFID operates in three frequency ranges Low Frequency (LF), High Frequency (HF) and Ultra High Frequency (UHF). RFID devices are divided into two groups: Active and Passive.

Wi-Fi is a wireless communication technology that allows for internet access through radio signals. It can be subject to various types of attacks, such as those related to network access control, data security, and network design. WiFi has six security modes, including overall network security, encryption with WEP, WPA, and WPA2, MAC address filtering, protocol filtering, hiding SSID broadcast information, and IP address assignment. WiFi is also vulnerable to various threats, such as wireless network eavesdropping and search wireless signal attacks.

IOT Applications:-

The publishers mentioned 7 applications such as Assisted Driving, Mobile Ticketing, Social Networking, Sensing, Homes and Offices, Identification and Authentication, and Theft and Losses, whose details includes assisted driving for improved navigation and safety, mobile ticketing using NFC tags, social networking with real-time location updates, sensing for real-time monitoring of patients' conditions, home and office automation with sensors for convenience, identification and authentication for security in healthcare, and tagging and tracking of precious objects to prevent loss.

Comparisons and Discussions mentioned in the paper:-

The first comparison is done between Different Application Layer Protocols and IOT:

Protocol	Transport	QOS Option	Security	Architecture
MQTT	TCP	YES	TLS/SSL	Publish/Subscribe
CoAP	UDP	YES	DTLS	Request/Response
AMQP	TCP	YES	TLS/SSL	Publish/Subscribe
XMPP	TCP	NO	TLS/SSL	Publish/Subscribe Request/Response

The second comparison is done between Security Measures of IOT included in the paper

Security Measures	Number of Security Modes/Keys	Security Threats
ZigBee	3	Bus Pirate and GoodFet
Bluetooth	4	Bluejacking, Car Whisperer, Bluesnarfing
RFID	3	Clandestine scanning, Tracking, Skimming and cloning
Wifi	6	Wireless Network Eavesdropping

Conclusion

In this paper, they have presented the detailed survey on IoT architectures, protocols, security and smart city based applications. Firstly, they have presented a common IoT architecture that addresses essential factors like QoS, confidentiality, reliability, integrity, etc. by explaining the parts where application layer protocols are required to handle communication. Secondly, they have presented the essential application layer protocols

that have attained focus for IoT as well as providing a comparison among each other. Thirdly, they have identified various security measures by using many technologies like ZigBee, Bluetooth, RFID and WiFi. Finally, we have presented various current smart city based IoT applications.

Bibliography:-

Google Scholar

IEEE Explorer

Authors of the research paper;
Parul Datta
Computer Science Engineering Department, Chitkara University, India
Bhisham Sharma
Computer Science Engineering Department, Chitkara University, India