IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Internet of Things (IoT)

Rishabh Sharma[1], Akash Kumar Mahapatra[2], Aditya Abhiraj[3], Madireddy Tanil Mohan Reddy[4], Podalakuru Bala Murali Krishna[5]

[1]School of Computer Science and Engineering, Lovely Professional University, India.
[2]School of Computer Science and Engineering, Lovely Professional University, India.
[3]School of Computer Science and Engineering, Lovely Professional University, India.
[4]School of Computer Science and Engineering, Lovely Professional University, India.
[5]School of Computer Science and Engineering, Lovely Professional University, India.

ABSTRACT

In today's world, heterogeneous devices are linked through the internet. Handheld devices can be used to access and initiate a wide variety of services. You can book tickets, do banking, check traffic, pay your bills, and obtain certificates from the municipality, among other things. Many problems in IoT arise as a result of the heterogeneity of devices, including alignment and control, data management, and scalability. Many (sensing) devices in the Internet of Things continue to record and send data to a control room for review and decision-making. This paper will give you a sense of what the Internet of Things is and what the key problems and challenges are.

KEYWORDS

Internet of Things (IoT), Security, Privacy, Threats, Service-oriented architecture (SOA), Radio-frequency identification (RFID), Wireless sensor networks (WSN).

INTRODUCTION

THE INTERNET OF THINGS (IoT) is a type of network that is formed by various devices performing different tasks for a common goal. These devices (sensors) may be cameras mounted in the city to track traffic, the metrological department, civic agencies, banks, various sensors, citizens, and mobile phones, traffic police, civic agencies, and so on. These systems perform widespread and ubiquitous computing. However, there is no general definition of the Internet of Things. Several organisations have provided definitions (CCSA, ITU-T, EU FP7 CASAGRAS, IETF, and so on). The unregulated environment (mobility, connectivity, and trust), heterogeneity, scalability, mobile, variety, intimacy, interdependence myriad, unattunedness, and limited resource power are some of the properties or features or characteristics of the IoT, as are detailed vision, efficient transmission, and intelligent processing. Object recognition, triggering an event, object sensing, and object identification are the most common tasks performed in IoT. An internet connection is a great thing; it provides us with a plethora of advantages that were previously unavailable. Consider your mobile phone until it became a smartphone if you're old enough. Yeah, you might call and write, but now you have the ability to read any book, watch any movie, and listen to any song from the palm of your hand.

The argument is that linking items to the internet provides a slew of incredible advantages. We've all seen these advantages with our smartphones, laptops, and tablets, but the same can be said for anything else. And yes, we do mean it when we say that.

You may be wondering what hardware is needed to prepare an IoT solution. The response to this question is that you'll need sensors to sense the environment, followed by a remote dashboard to track your performance and view it in a more straightforward and comprehensible manner. Last but not least, you'll need a device that can serve and path.

IoT Technologies

To deploy IoT-based systems, you'll need the following ingredients**:**

i) RFID (Radio Frequency Identification): This is one of the most essential components of the Internet of Things, and it is a small chip that looks like an adhesive sticker and collects and transmits signals. RFID is made up of readers and tags. It helps us to use radio waves, tags, and readers to perform direct automatic identification and date capture. Depending on whether or not a power supply is available, FRID tags may be passive or active.

ii) WSN (Wireless Sensor Networks): This is a network of autonomous sensors that are spatially distributed. Their task is to keep track of the status of RFID items, such as their location, temperature, and movement. A sensor network's sensing nodes transmit data to their sinks.

iii) Middleware: A software layer designed to mask the complexities of various technologies and simplify communication. Its proposed architecture is service-oriented architecture (SOA).

iv) For IoT, iCloud Computing and Fog Computing are computing models that enable users to access a pool of resources on demand. Computers, networks, servers, storages, applications, utilities, and software are all examples of resources. Cloud storage for IoT has a range of problems including synchronisation, standardisation, balancing, reliability, and management. With the support of fog computation, cloud computing resources can be extended closer to users for better performance. Place, distribution, scalability, and mobility support are all features of fog computation.

v) IoT Application Software: This software is used to build a range of industry-specific applications. It provides all of the requisite amenities.

Evolution of IoT Technologies

IoT technologies, such as RFID, WSN, Smart Things, Network, Software and Algorithms, Hardware, Data Processing, and so on, have evolved over time and can be summarised as follows:

TECHNOLOGY	TIME SPAN	DESCRIPTION
RFID	1999 - going on	Wireless networks, passive recognition.
WSN	2005 - going on	WSN, cloud computing, Web 2.0 and low energy communication are some of the terms used to describe wireless sensor networks.
Smart Things	2012 – going on	Mobile computing and computer connectivity.
IoT	2017 – going on	Predictive monitoring, sophisticated sensors fusion and faster wireless networking.

Enabling Technologies

i) Identification and Tracking: RFID can be used in object detection because of its ability to identify and monitor objects. Collisions, interferences, privacy rights, norms, and incorporation are all linked to it.

ii) Integration of WSN and RFID: Many innovations, such as WSN, communication, networks, RFID, and others, are being integrated to make IoT more useful to manufacturing, healthcare, decision-making, smart city, and smart recovery center systems.

iii) Communication: Various devices with varying specifications communicate through a network.

iv) Wireless mesh networks, ad hoc networks, and cross layer protocols for wireless networks are all available.

v) Confidentiality, authentication, and availability of cutting-edge services necessitate security and privacy.

Standards

The importance of interface and middleware standardization cannot be overstated. Designing policies and distributed architecture, as well as ensuring user privacy and safety, achieving network trust, acceptability, and security, developing standards, and exploring new enabling technologies such as micro-electronic-mechanical system (MEMS) devices and ubiquitous location, are now top priorities. The following are some of the most relevant principles:

TECHNOLOGY	STANDARDS
Communication	IEEE 802.15 for ZigBee, WLAN, Bluetooth, IEEE 1888 for wireless body area network, 4G UWB, IPv6 and other wireless technology.
RFID	ISO 11785 RFID tag, air interface protocol, mobile RFID payment, smart card and so on.
Data Content and Encoding	ECP (global electronic protocol code), GPML (global physical markup language) and GONS (global object naming service) are all examples of global electronic protocol codes.
Electronic Product code	Auto-ID, serial shipping container code, global location number, global trade identification number and so on are all examples of unique identifiers.

IoT Framework

The internet of things (IoT) is a platform that incorporates ubiquitous sensing devices and applications framework, which is more versatile and scalable because it taps into the full power of cloud computing. As seen in the diagram below, cloud merges to provide scalable storage and computing time. This can be used in health, object surveillance to track their path, and environmental monitoring to determine how polluted the environment is and how it can be restored. New routes in transportation can be found to decongest the city and allow for a more convenient trip. Stuff can be rented on the cloud, so there's no need to invest in hardware, platform, or services. It may be reimbursed for the services rendered. A wireless sensor network connects a variety of sensors that track, capture, and relay data to control rooms for further analysis and prediction.

Architecture of IoT

In the sense of IoT, the layered architecture has five layers: market, application, middle, network, and perception layers.

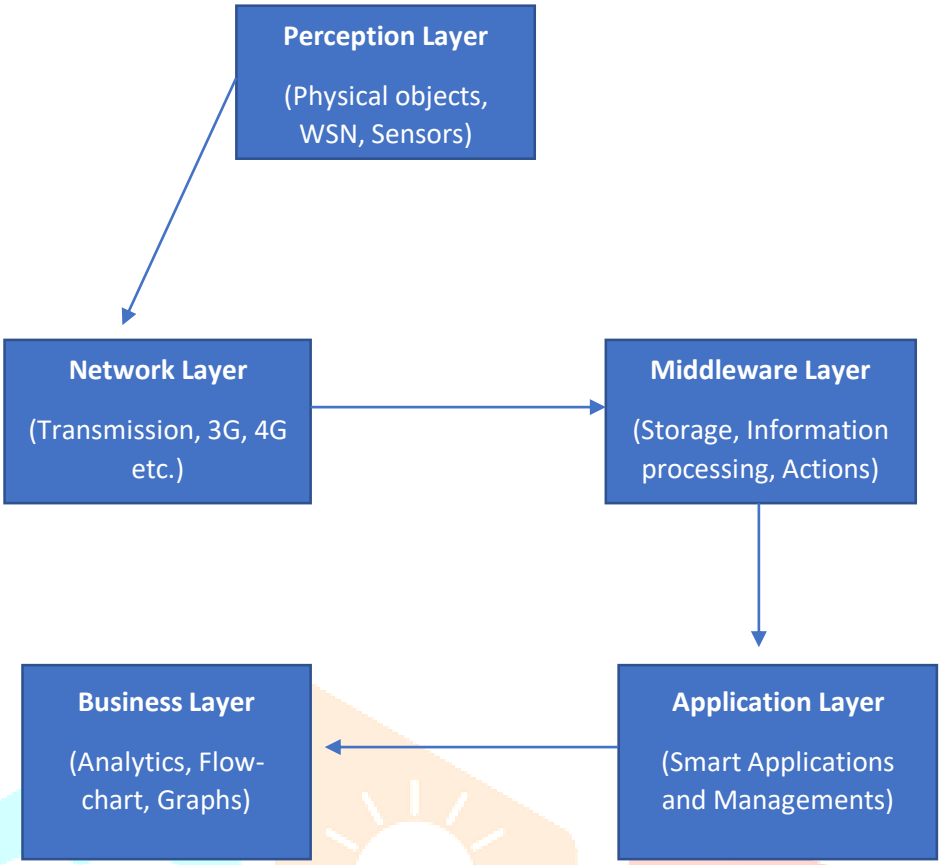
A) Business Layer: The information from the application layer is received by the business layer. This layer can create a business model, use flow graphs, and graphs, among other things, to analyses data. It also determines the company's performance rate and future plans. This takes care of a wide variety of certain activities.

B) Application Layer: This layer creates the overall object model using information from the middleware. Smart health, smart cities, intelligent transportation, and military and social site operations are examples of possible applications.

C) Middleware Layer: This layer securely transfers data from sensors to control rooms for processing. It fulfils requests obtained from the network layer. There is a data base that can be used to conduct ubiquitous computing and make decisions based on the results if necessary.

D) Network Layer: This layer transmits data from sensors to information processing systems through wired and wireless connections.

E) Perception Layer: This layer handles object recognition and keeps track of physical objects and sensors. This gathers data from the sensor and sends it to the network layer.



Challenges in IoT Developments

Standards, mobility support, transport protocols traffic characterization and Q0S support, data integrity, anonymity, addressing and networking, and digital forgetting are some of the open concerns:

A) Data Management Challenge: IoT systems capture data from a number of sources and process and store it. This data may be in a variety of formats and be handled in a variety of ways.
B) Data Mining Challenges: Since data is so large, analysis can necessitate the use of specialized mining tools.
C) Privacy Issues: Privacy must be protected during the process. When personal information about an individual must be moved, it must be kept confidential.
D) Security Issues: As the number of devices grows, so do the threats and risks of sending incorrect data. Item recognition, authentication, and authorization are all problems that need to be discussed.
E) Chaotic Challenges: A large number of devices are connected and interact with one another in order to exchange information. It can result in traffic congestion and channel bandwidth waste. As a result, congestion management and proper routing are needed.
F) Energy-efficient sensing: effective methods for detecting, collecting, and tracking the heterogeneous data obtained by various sensing sensors.
G) Architecture: It is essential to build architecture that can meet and handle requirements.
H) New Protocols: At several levels, protocols are the foundation of the IoT for different services. As a result, energy-efficient protocols must be established at the Mac layer as well as for routing. Protocols such as MAC, TDMA, CSMA, FDMA, and others are not explicitly applicable to IoT.
I) International Activities: It is gaining prominence in all sectors of society, including business, academia, and government.

IoT Security

Because of the network structure of IoT, there are several vulnerabilities. Access control, data authentication, and client privacy are all criteria for protection. Virtual private networks, transport layer encryption, onion routing, and DNS security extensions are some examples of privacy-enhancing initiatives. Since its IoT devices are typically left unattended (physical security is required), communication is digital, and its devices have limited resources, complex steps are difficult to implement:

A) Object Identification and Location in IoT: An ONS (object network system), similar to DNS, is needed for specific object identification in an IoT network. Data networking (NDN) and FIA (Future Internet Architecture) are two names that have been proposed.
B) Data Integrity and Authorization in IoT: Messages should be unchanged and accessible to the intended recipients.
C) Privacy, trust, and data confidentiality: The user's behavior when connected to the IoT network is analyzed to determine if he was a routing user or not. Authentication issues, transport security, access control, and insecure applications, to name a few.
D) Lightweight Cryptosystems and Security Protocols: a wide range of tools, including sensitive data, are available for sharing and processing. As a result, cryptosystems secure certain vital resources, and appropriate protocols should be developed.
E) Software Vulnerability and Backdoor Analysis: There may be several flaws in device security that could be exploited or breached. The breached areas must be secured to prevent infiltration.
F) Malware: There are unwanted programmes designed to hurt or learn about the plans of business competitors. They sometimes

deplete our system's resources and, on rare occasions, crash or corrupt our system's hardware. To stop them, you'll need a decent anti-virus, anti-spammer, and other security software.

G) Android Platform: The Android platform drives the bulk of today's mobile devices. As a result, an increasing number of mobile devices and smart applications are being created to communicate with these devices.

Some IoT protection standards exist, as well as privacy-enhancing technologies VP. Aside from the standards, there are several problems with privacy legislation, such as determining privacy infringements, data quality and meaning, identifying openness and data minimization, and interoperability and connectivity. Interoperability is defined as the ability for components to interact with one another and respond to the needs of the situation. Technical and cross-domain interoperability are two examples.

IoT Application

IoT can be used in the domains of transportation and smart environments, logistics, fitness, personal and social domains, and futuristic applications. They can be divided into the following classes:

A) Monitoring and Control: It collects data from different devices regarding their use, i.e., usage, in order to control and monitor the devices' performance. They can sense and control device position, fleet management, traffic information systems, environmental sensing, remote sensing, and remote medical monitoring, among other things.

B) Big Data and Business Analytics: IoT devices and machines are embedded with sensors and actuators, resulting in vast quantities of data being generated. For a business prospect, this vast data must be evaluated in order to set new business targets.

C) Information Exchange and Collaboration: Through devices linked to an Io network, people can collect and submit information. It is possible for people and sensors to work together.

D) Ad Hoc Networking: Ad Hoc networks are self-contained networks that function to provide services.

E) Secure Communication: Based on service requirements, it may build a secure channel for communication between objects and services or IoT terminals.

F) Smart houses, health care, and management of businesses.

Conclusion

This paper examines Internet of Things (IoT) standards, technology, architectures, and enabling technologies, with a focus on security, privacy, and trust. On the basis of key parameters, various techniques and methods are defined and analyzed. The effects of different treatments, threats, and vulnerabilities are investigated.

REFERENCES

[1] Buyya R, Gubbi J, Palaniswami M, , Marusic S. Web of Things (IoT): A dream, building components, and future headings. Group of people yet to come PC frameworks. 2013 Sep 1;29(7):1645-60.

[2] Monteiro E, Granjal J, Silva JS. Security for the web of things: a review of existing conventions and open research issues. IEEE Communications Surveys and Tutorials. 2015 Jan 9; 17 (3):1294-312.

[3] Ferguson AG. The Internet of Things and the Fourth Amendment of impacts. Cal. L. Fire up. 2016; 104: 805.

[4] Thierer AD. The web of things and wearable technology: Addressing protection and security worries without crashing development. Fotouhi M, Hossain MM, Hasan R. Towards an examination of safety issues, difficulties, and open issues in the web of things. 2015 Jun 27 (pp. 21-28). IEEE.

[5] Koien GM, Abomhara M. Digital protection and the web of things: weaknesses, dangers, gatecrashers and assaults. Diary of Cyber Security. 2015 Jan; 4(1):65-88.

[6] Khoo B. RFID of the Internet of Things: Issues of Security and Privacy. In2011 International Conference on Internet of Things and fourth International Conference on Cyber, Physical and Social Computing 2011 Oct 19 (pp. 709-712). IEEE.

[7] In Lee, Kyoochun Lee," the web of things: applications, ventures, and difficulties for enterprizes", business skylines (2015), 58, 431-440.

[8] D. Lu and T. liu. The applications and development of IoT", 2012, vol.2, pp. 991-994.

[9] Khan SU, Khan R, Zaheer R, Khan S. Future web: the web of things engineering, potential applications and key difficulties. InFrontiers of Information Technology (FIT), 2012 tenth International Conference on 2012 Dec 17 (pp. 257-260). IEEE.

[10] Natalizio E, Sfar AR, Chtourou Z, Challal Y. A roadmap for security challenges in the Internet of Things. 2018 Apr 1; 4 (2):118-37.

[11] Iera A, Atzori L, Morabito G. The internet of things: A survey. 2010 Oct 28;54(15):2787-805

[12] Da Xu L, Li S, Zhao S. The internet of things: a survey. Information Systems. 2015 Apr 1;17(2):243-59.

[13] Yu Y, Shang W, Zhang L, Droms R. Challenges in IoT networking via TCP/IP architecture. NDN Project. 2016 Feb 10.

[14] Kim H, Lee JH. Security and privacy challenges in the IoT [security and privacy matters]. 2017 Jul; 6(3):134-6.

[15] Rizzardi A, Sicari S, Coen-Porisini A, Grieco LA. Security, Privacy and trust in IoT: The road ahead. 2015 Jan 15; 76:146-64.

[16] Sicari S, Miorandi D, Chlamtac I, De Pellegrini F. Internet of things: Vision, Research challenges and applications. 2012 Sep 1;10(7):1497-516

[17] Zhou J, Roman R, Lopez J. Features and challenges of privacy and security in distributed internet of things. 2013 Jul 5; 57(10):2266-79.
[18] Guizani M, Al-Fuqaha, Aledhari M, Mohammadi M, Ayyash M. Internet of things: A survey on enabling protocols, technologies and applications. 2015 Jun 15;17(4):2347-76
[19] Luthra M,Vasilomanolakis E, Gazis V, Daubert J, Wiesmaier A, Kikiras P. On the privacy and security of Iot systems and architectures. International Workshop on 2015 Sep 21 (pp. 49-57). IEEE.
[20] Jia Y, Zhou W, Zhang Y, Peng A, Liu P. The Effect of Internet of things New Features on Privacy and Security: Existing Solutions, New Threats and Challenges. IEEE Internet of Things Journal. 2018 Jun 15.
[21] Mayer CP. Privacy and Security challenges in the IoT. Electronic Communications of the EASST. 2009 Feb 27;17.
[22] Salah K and Khan MA. Internet of Things security: Blockchain solutions, Review and open challenges. 2018 May 1; 82: 395-411.
[23] Ranjan R, Perera C, Khan S, Wang L, Zomaya A. Privacy of big data in the new IoT era. IEEE IT Special Issue Internet of Anything. 2015 Feb; 6.
[24] Najera P, Alcaraz C, Roman R, Lopez J. Wireless sensor networks and the IoT:" Do we need a complete integration?". 2010.