■ REVIEW ARTICLE

Emerging Trends in the Internet of Things

Dhanush Arun

American High School, 36300 Fremont Blvd, Fremont, California, 94536, USA; dhanusharun.us@gmail.com

ABSTRACT: Recent advances in low-power computing, communication, and cloud technologies have enabled the widespread proliferation of the Internet of Things (IoT). IoT refers to an interconnected network of devices communicating and collaborating to accomplish a task. IoT is used for different applications such as industrial automation, home automation, building automation, health care, and disaster recovery. This survey paper discusses different standards in IoT, the evolution of the IoT protocols, and future trends. We will first look at how the Internet evolved to IP-based standards and find any similarity between IoT and Internet networking protocols. We will also discuss "Matter," the new application layer protocol for IoT devices, defined by the Connectivity Standards Alliance (CSA).

KEYWORDS: Embedded Systems, Internet of Things, OSI Network Layer, TCP/IP, Matter.

Introduction

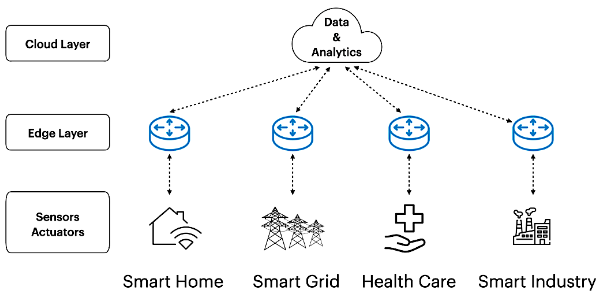

Figure 1: Illustrates the layers in an IoT system. The Cloud serves as a central hub, integrating and analyzing data transmitted from sensors through IoT protocols, enabling real-time insights and decision-making.

The Internet of Things (IoT) refers to integrating computing and connectivity to various physical objects around us, such as light bulbs, thermostats, and door locks. (Figure 1) shows an IoT system's components, including sensors and actuators, communication and networking, data processing, and application layers. Enabling computing and networking capabilities for sensors and actuators can help monitor and control our physical environment. IoT systems' constant connectivity, computing, and data analytics capability enable innovative products and services to improve comfort, productivity, security, and energy efficiency in multiple industry segments such as health care, homes, buildings, and factories. The potential economic value that the IoT could unlock is large and rapidly growing. McKinsey predicts that by 2030, IoT will enable $5.5 trillion to $12.6 trillion in value globally.[1]

In this paper, we will first discuss the different layers of a communication system using the OSI 7-Layer model, which is essential for further discussion. Section II will look at the evolution of the Internet, a global network of computers, and how it converged from multiple networking protocols to Internet Protocol (IP). The following section will study how IoT protocols emerged, evolved, and converged. It will conclude with discussions on the future trends in IoT standards.

I. OSI 7 Layer Model:

The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization, which allows diverse communication systems to communicate using standard protocols. In simple words, the OSI model provides a way for different computer systems to communicate with each other. The model breaks down network communication into seven layers based on functionality, which makes it easier to build, develop, and troubleshoot. Moreover, the OSI model's layers depend on each other to provide data, as indicated in (Figure 2). The seven layers are application, presentation, session, transport, network, data link, and physical layer.[2] The following sections briefly describe the functionality of each layer.

A. Application Layer:

The Application layer is the uppermost layer in the OSI model and serves as the interface between the user and the network. Its primary function is to enable communication and data exchange between applications running on different devices across a network. This layer is in charge of providing network services directly to end-users and applications. A few examples of protocols that operate at the application layer include HTTP (Hypertext Transfer Protocol) for web browsing, SSH (Secure Shell) for remote access, and SMTP (Simple Mail Transfer Protocol) for email.[3]

B. Presentation Layer:

The presentation layer is necessary for preparing data so the application layer can use it. The presentation layer is responsible for data decryption, encryption, and compression. Protocols in the Presentation layer are JPEG (Joint Photographic Experts Group) and ASCII (American Standard Code for Information Interchange).[4]

C. Session Layer:

The session layer is needed for opening and closing communication between two devices. The time between open and closed communication is known as "the session." The session layer ensures that the session stays open long enough to transfer all the data being exchanged and then promptly closes the session to prevent any wastage of resources. The session layer also synchronizes data transfer with something known as checkpoints. These checkpoints essentially help save any resources from being wasted. Thanks to the checkpoints, the entire transfer does not have to start from the beginning. Protocols in the session layer are PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call), and SQL (Structured Query Language).[4]

D. Transport Layer:

The transport layer is responsible for end-to-end communication between devices. This involves taking data from the session layer and breaking it into segments before sending it to the network layer. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume. Protocols in the transport layer are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and SCTP (Stream Control Transmission Protocol).[5]

E. Network Layer:

The network layer is responsible for the data transfer between two different networks. The network layer breaks up segments from the transport layer into even smaller units, called packets on the sender's device, and reassembles these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination, known as routing. Protocols in the network layer include IP (Internet Protocol) and IPSec (Internet Protocol Security).[6]

F. Data Link Layer:

The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Then, the data link layer transfers the frames from a given node to all other nodes in the network. There are also two sublayers to the data link layer: Medium Access Layer (MAC) and Logical Link Control (LLC). LLC manages the data link layer's synchronization, flow control, and error-checking functions. MAC provides control for accessing the transmission medium. Protocols in the data link layer are PPP (Point-to-Point Protocol) and HDLC (High-Level Data Link Control).[7]

G. Physical Layer:

The OSI model's lowermost layer, the physical layer, includes the physical equipment involved in the data transfer, such as cables and switches. The physical layer is needed to transfer data from one device to another. The data can be transferred through a wire by electrical signals or electromagnetic waves for a wireless medium. Before the data can be sent, it must first be converted into a bitstream, a string of 1s and 0s. The physical layer of both devices must also follow the same standard. For example, the IEEE 802.11 and IEEE 802.15 defines the physical layer for wireless LAN (Local Area Network) and WPAN (Personal Area Network).[8]

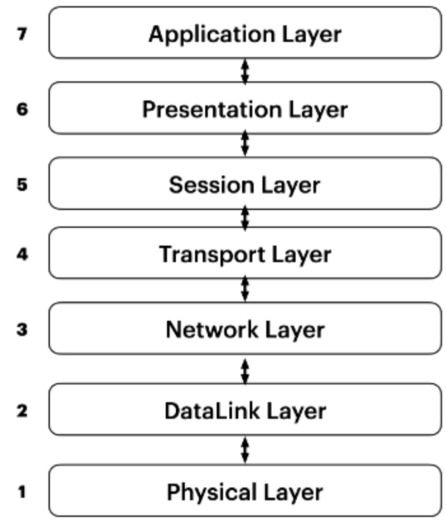

Figure 2: This is the OSI 7-Layer Model. It outlines the framework for communication in computer networks.

II. Evolution of the Internet:

This section will first discuss the beginning of the Internet, how it evolved, and finally, why all the protocols converged into IP.

A. The Beginning of the Internet:

Computers in the 1960s were very large and not portable. People back then had to send magnetic computer tapes through the postal system to share information from one computer to another. The Cold War also fuelled the development of the Internet. After the Soviet Union had launched the Sputnik satellite, the U.S. military wanted to find ways to share information even if there was a nuclear strike. This eventually led to the creation of the ARPANET (Advanced Research Projects Agency Network), the network that sooner or later evolved into what we all know today as the Internet.[9]

Before the Internet became a worldwide network, various computer networks existed. The problem was that they needed a standard way to communicate. A new communication protocol called Transfer Control Protocol/Internet Protocol (TCP/IP) was established to solve this issue. This protocol allowed different kinds of computers on various networks to "talk" to each other.[9] All networks can now be connected by a universal language everyone can understand.

This first true Internet transmission occurred on November 22, 1977, when SRI (Stanford Research Institute) originated the first connection between three disparate networks. Data flowed seamlessly through the mobile van at SRI in Menlo Park, California, and the University of Southern California in Los Angeles via London, England, across three types of networks: packet radio, satellite, and the ARPANET.[10] In (Figure 3), the interconnection of various networks into a unified inter-network is shown, which emphasizes the capability of TCP/IP for linking diverse networks into a single system.

DOI: 10.36838/v7i1.22

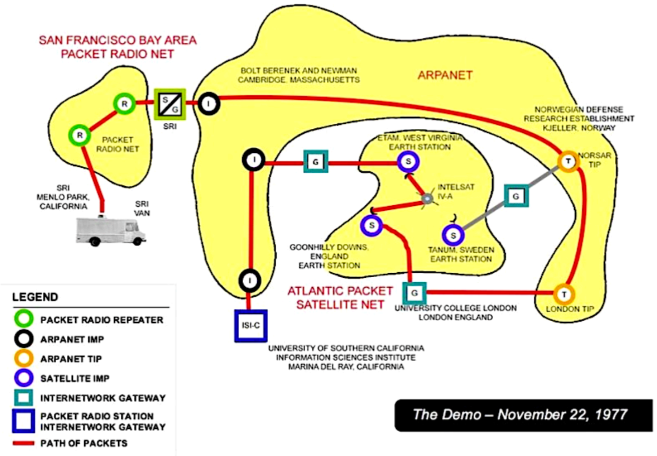

Figure 3: This map shows the first experiment connecting three different types of networks on November 22, 1977.[10] The results of this experiment show the interoperability of TCP/IP.

III. The Evolution:

This section will cover the prominent networking protocols used in the early days of the Internet and explain why they were replaced by the Internet Protocol.

A. Internet Protocol (IP):

The Internet Protocol (IP) is a set of regulations that control how data is sent and received over the Internet. IP is the network layer, which is the 3rd layer of the OSI model. It's one of the main protocols in the TCP/IP networking protocol suite, which is used universally across the internet to link data packets with a network address. On top of addressing and routing, IP is also responsible for the fragmentation and reassembly of data. It transmits data over a network by breaking down data into smaller packets. These packets are then reassembled at the destination. Before IP was introduced and gained widespread adoption, several networks were developed for specific purposes.[11]

B. SNA (System Network Architecture):

System Network Architecture (SNA) is a proprietary IBM networking framework in large-scale computing environments. Introduced in 1974, SNA was a layered protocol suite similar to the more general OSI seven-layer model. It was designed to allow mainframes to communicate with various devices across various networks, including terminals, printers, storage devices, and other mainframes. The architecture consists of components for both hardware (such as gateways, front-end processors, and controllers) and software (such as data routing, formatting, and security protocols).[12]

C. X.25:

X.25 is a network protocol suite developed in the 1970s that provided specifications for packet-switched networks, enabling data communication over wide area networks (WANs). It was one of the earliest protocols designed to allow computers to communicate over long distances and formed the foundation for the first global data networks. X.25 handles both the physical connections and the packets' transmission, making it a predecessor to modern protocols like IP.[13]

D. DECNet:

DECnet is a suite of network protocols created by Digital Equipment Corporation (DEC) in the 1970s. It was designed to connect DEC's computer systems for resource sharing and communication. It enables linking systems of various sizes and capacities, from small workstations to large mainframes. DECnet protocols supported multiple network topologies and allowed routing and data communication among connected nodes in the network.[14]

E. Network Control Protocol (NCP):

The Network Control Program (NCP) was an early protocol suite controlling communication over the Advanced Research Projects Agency Network (ARPANET), the precursor to the modern internet. NCP was developed in the early 1970s and provided rules for starting and maintaining network connections. It also made it a reality for computers to transmit and receive messages reliably over the network.[15]

F. AppleTalk:

AppleTalk is a networking protocol developed by Apple in 1983 for their Macintosh computers. It was made to allow the sharing of resources, such as files and printers, among local area network (LAN) users. AppleTalk was known for its clearness and ease of use. This was because it was plug-and-play networking, where Macintosh computers could automatically connect to the network without much configuration.[16]

G. Internetwork Packet Exchange (IPX):

Internetwork Packet Exchange (IPX) is a networking protocol primarily used in Novell NetWare operating environments. Developed in the 1980s, IPX was used for packet-switched networks and included services similar to IP from TCP/IP, allowing different types of networks to intercommunicate. Known for its simplicity, reliability, and low latency, it was especially popular in local area network (LAN) applications.[16]

IV. The Convergence:

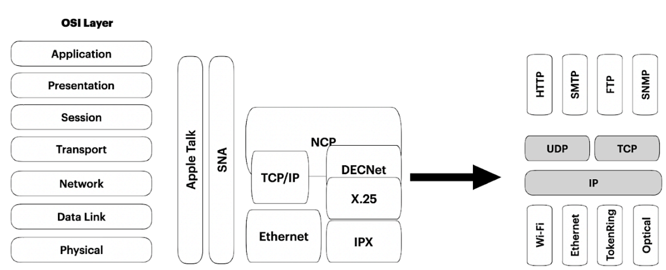

Figure 4: The internet adopted TCP and UDP for communication over IP. TCP ensures reliability, while UDP allows faster, less reliable data transfer.

TCP/IP's open, cross-platform design made it a reality for any computer or network to communicate with another. This stood in contrast to earlier protocols, many of which were proprietary and designed to work with specific hardware. This universality led to the widespread adoption of TCP/IP despite the existence of other network protocols.[10]

It took almost 15 years after the 1977 experiment for TCP/IP to defeat powerful rivals and become the dominant internetworking standard worldwide, paving the way for a unified online system like the Web. Along the way, TCP/IP took the place of powerful corporate standards such as DECNET and IBM's SNA, as shown in (Figure 4).[10]

Moore's Law states that transistors in an integrated circuit will double every two years, leading to higher performance and lower computer costs.[17] The number of computers exploded from 1000s in 1960 to 2 billion today. Based on Metcalfe's law, a network's value increases as the number of nodes connected to a network increases.[18] This fueled the modern-day Internet, a globally networked computer system that facilitates communication and data services for a vast collection of private, public, business, academic, and government networks.

V. Evolution of IoT:

This section will discuss the beginning and evolution of IoT protocols and the emerging trends in their convergence.

A. The Beginning:

In 1997, British technologist Kevin Ashton, cofounder of the Auto-ID Center at MIT, was exploring a technology framework called radio-frequency identification (RFID). RFID would allow physical devices to connect using microchips and wireless signals.[19] During a speech, Ashton coined "the Internet of Things." There were examples of IoT before then. In the early 1980s, local programmers at Carnegie Mellon would connect to a Coca-Cola machine using the internet. Using this connection, the programmers could see if a drink was available and if it was cold.[20]

B. The Evolution:

During the early 2000s, smartphones, cloud computing, and advancements in processing power created a faster way to collect, store, process, and share data. Meanwhile, intricate sensors were developed to measure motion, temperature, and moisture levels and even find a person's location or a device through geolocation.[19] These developments made it possible to communicate with digital devices and physical objects in real time. An example of an IoT product is the Ring doorbell. Ring is a doorbell that links to your phone and sends you a signal when the doorbell is pressed. It lets you see who it is and speak with them. In 2010, leading technology companies began developing their own IoT ecosystems. For instance, Apple made Homekit, Google made Google Home, and Samsung made Smartthings.[20] The issue with having all these proprietary ecosystems is that it makes it challenging for customers to set up and use multiple brands of smart devices with no interoperability. The following section will discuss IoT protocols in detail.

VI. IoT Wireless Protocols:

A. Zigbee:

Zigbee is a 2.4GHz communication protocol that develops personal area networks with small, low-power digital radios. It was designed for use in low-power, low-data-rate applications, and Zigbee is especially suited for smart homes, industrial automation, and remote sensor networks. Operating in the IEEE 802.15.4 standard, Zigbee can be used for a mesh network configuration like Internet Protocol because it enables devices to transmit data over longer distances by passing it through a network of intermediate devices to reach more distant ones. This capability, combined with its low power consumption, is what makes Zigbee pertinent for many IoT applications.[21]

B. Z-Wave:

Z-Wave is a wireless communication protocol mainly used for home automation. It uses central control hubs to enable smart home devices like lights, locks, thermostats, and sensors to talk with each other. Z-Wave runs on a low-frequency band (around 900 MHz), generally providing good penetration through walls and other obstacles in homes. Unlike Wi-Fi, which is made for high-bandwidth data transfer, Z-Wave was designed to send small packets of data, making it a good choice for managing smart devices. One of the fundamental features of Z-Wave is its mesh network architecture; devices in a Z-Wave network can relay messages to each other, allowing for extended range and reliable communication throughout any home or building. This protocol has gained massive popularity mainly because it is easy to set up and dependable.[22]

C. Bluetooth:

Bluetooth is a wireless technology standard for exchanging data between devices over small distances. It operates in the 2.4 GHz frequency band and is mainly used for connecting smartphones to headphones, speakers, smartwatches, and other peripherals. Bluetooth was developed as a cable replacement and supports point-to-point and multipoint connections. This makes it a top choice for various applications, from simple device pairing to the formation of short-range wireless networks. Over the years, its iterations, such as Bluetooth Low Energy (BLE), have expanded its use to longer-lasting battery life applications like fitness trackers and IoT devices.[23]

D. Thread:

Thread is a low-power, wireless mesh networking protocol for smart home and IoT applications. It operates in the 2.4 GHz frequency band and has secure, scalable, and reliable device-to-device communication. Unlike traditional wireless standards, Thread's mesh network lets devices interconnect and relay data to each other, ensuring strong coverage and connectivity in complex environments. Developed by the Thread Group, which includes industry players such as Google and Apple, it is becoming increasingly popular for home automation. This is due to its interoperability, security features, and seamless integration with IP-based networks.[24]

E. Wi-Fi:

Wi-Fi is a wireless networking technology that connects devices to the internet and allows them to communicate with each other without any physical cables. It uses radio waves to provide network connectivity within a local area like a building or home. It was created in the late 1990s and has become a common feature in many devices. The term "Wi-Fi" stands for Wireless Fidelity and is a trademark of the Wi-Fi Alliance. The Wi-Fi Alliance is an organization that tests and verifies that devices conform to the 802.11 family of standards.[25]

Wi-Fi HaLow (IEEE 802.11ah) is a long-range, low-power, low-speed version of Wi-Fi for IoT systems. Wi-Fi HaLow utilizes license-exempt frequencies below 1 GHz, such as 902 – 928 MHz in the United States.

F. RFID:

A Radio Frequency Identification (RFID) system consists of tags and readers. The reader scans the area for RFID tags by transmitting electromagnetic energy, which powers the tags in

DOI: 10.36838/v7i1.22

the reading area. The tags need minimal energy to power their internal RFID chip and send a response with the programmed information. RFID is used in inventory tracking, access control, and authentication applications.

VII. The Convergence:

This section will review what Matter is and how its architecture is structured.

A. What is Matter?:

Major technology companies started building their own IoT ecosystems (Google Home, Amazon Alexa, Apple Home, Samsung SmartThings), which were not interoperable. The whole industry came together to define a common standard called Matter to solve this interoperability issue. Matter is an open-source connectivity standard for IoT devices and smart homes. Matter is founded by CSA (Connectivity Standards Alliance), a large and growing group of companies from diverse industries. Some companies that are a part of CSA include industry leaders such as Amazon, Apple, and Google. Matter aims to enhance interoperability and security and make it easy for consumers to set up devices. A few of the devices Matter currently supports are light bulbs, switches, locks, thermostats, fans, and robot vacuums. Before Matter was created, consumers had to install the IoT ecosystem's proprietary apps to use the product. This was a huge issue for customers because it made it stressful for them to manage all their smart home devices. Matter can solve this problem by making it possible to control all these devices using just one app.[26]

B. Architecture of Matter:

Matter is implemented in the application layer of the OSI model. It uses IP-based protocols such as Wi-Fi and Thread, as seen in the lower layer of the Matter architecture (Figure 5). Matter is compatible with multiple connectivity options because it is an IPv6-based protocol that uses transport layer protocols such as TCP/UDP. Moreover, Matter supports bridging existing technologies, namely Zigbee, Bluetooth Mesh, and Z-Wave. This feature helps integrate existing IoT technologies into an interoperable environment to create a more user-friendly IoT device experience.[27]

C. The Future of Matter :

Technology companies in CSA are actively integrating the Matter protocol into their ecosystem to streamline interoperability and simplify development. Google is incorporating Matter in Android and Nest platforms, offering SDKs, APIs, and tools like the Google Home Developer Console.[28] Apple is embedding Matter within its HomeKit system to make it possible to integrate any 3rd party accessory into iOS apps.[29] Amazon supports Matter through Alexa, enabling compatibility with smart hubs and devices. These companies reduce barriers to implementation by providing resources like pre-certified hardware, modular software designs, and robust documentation. There have been challenges, such as limited device type support, inconsistent connectivity, and complex certification processes. Moreover, there are high entry costs, performance bottlenecks on low-end devices, and occasional setup bugs. Just like the development of IP, Matter development will be a gradual process that requires a lot of testing and updates to become a commonplace standard.

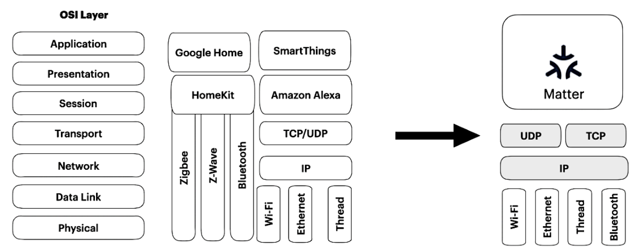

Figure 5: The Internet of Things is predicted to converge to TCP/UDP over Internet Protocol (IP), similar to how the Internet adopted these protocols for interoperability.

Conclusion

There were many networking protocols during the 1970s, but they were proprietary and could not work with each other. As a result, the IP replaced all these protocols because it could work with any device. Today's internet is based on IP. A similar pattern is forming in IoT, where all protocols are converging towards IPv6. A new application layer protocol called Matter can potentially bring interoperability to the application layer in IoT. It is highly likely that Matter will gain widespread adoption because of its interoperability and simplicity. Matter can make it a reality for consumers to buy any smart device and make it compatible with their platform of choice. However, it is important to note that Matter is still in its beginning stages and will likely need to be tested and updated before it becomes universally accepted.

Acknowledgments

I would like to thank Dr. Rana Basheer, Dr. Deepu Vijayasenan, and Dr. Koushik Sinha for their insightful comments and input. I would also like to acknowledge the Computer History Museum in Mountain View, California, for inspiring me to learn more about computers and networks.

References

1. *Where and how to capture accelerating IoT value | McKinsey*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it (accessed 2024-02-04).
2. Zimmermann, H. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications* 1980, 28 (4), 425–432. https://doi.org/10.1109/TCOM.1980.1094702.
3. *THE OSI MODEL: OVERVIEW ON THE SEVEN LAYERS OF COMPUTER NETWORKS, Sumit Kumar, Sumit Dalal, Vivek Dixit, International Journal of Computer Science and Information Technology Research, ISSN 2348-120X (online), ISSN 2348-1196 (print), Research Publish Journals*. https://www.researchpublish.com/papers/the-osi-model-overview-on-the-seven-layers-of-computer-networks (accessed 2024-02-04).
4. Costa, L. Open Systems Interconnect (OSI) Model. *JALA: Journal of the Association for Laboratory Automation* 1998, 3 (1), 28–35. https://doi.org/10.1177/221106829800300108.
5. Knightson, K. G. The Transport Layer Standardization. *Proceedings of the IEEE* 1983, 71 (12), 1394–1396. https://doi.org/10.1109/PROC.1983.12784.
6. Klerer, S. M. The OSI Management Architecture: An Overview. *Netwrk. Mag. of Global Internetwkg*. 1988, 2 (2), 20–29. https://doi.org/10.1109/65.3255.
7. Conard, J. W. Services and Protocols of the Data Link Layer. *Proceedings of the IEEE* 1983, 71 (12), 1378–1383. https://doi.org/10.

1109/PROC.1983.12781.
8. Willenegger, S. Cdma2000 Physical Layer: An Overview. *Journal of Communications and Networks* 2000, 2 (1), 5–17. https://doi.org/10.1109/JCN.2000.6596597.
9. *A Brief History of the Internet.* https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml (accessed 2024-02-04).
10. *tluong. Born in a Van: Happy 40th Birthday to the Internet*!. CHM. https://computerhistory.org/blog/born-in-a-van-happy-40th-birthday-to-the-internet/ (accessed 2024-02-04).
11. Panek, C. Understanding Internet Protocol. In *Networking Fundamentals*; Wiley, 2020; pp 103–146. https://doi.org/10.1002/9781119650768.ch4.
12. McFadyen, J. H. Systems Network Architecture: An Overview. *IBM Systems Journal* 1976, 15 (1), 4–23. https://doi.org/10.1147/sj.151.0004.
13. Bochmann, G. V.; Joachim, T. Development and Structure of an X.25 Implementation. *IEEE Transactions on Software Engineering* 1979, SE-5 (5), 429–439. https://doi.org/10.1109/ TSE.1979.230181.
14. Sylor, M. W. Managing Phase V DECnet Networks: The Entity Model. *IEEE Network* 1988, 2 (2), 30–36. https://doi. org/10.1109/65.3256.
15. Lammle, T. Introduction to TCP/IP. In Understanding Cisco Networking Technologies, *Volume 1: Exam 200-301*; Wiley, 2020; pp 63–104. https://doi.org/10.1002/9781119659082.ch3.
16. Cooper, S. H.; Teller, P. J. Configuring a Large LAN for TCP/IP, Appletalk, and IPX. In *Proceedings of 20th Conference on Local Computer Networks*; 1995; pp 264–268. https://doi.org/10.1109/ LCN.1995.527353.
17. *Moore's Law.* Intel. https://www.intel.com/content/www/us/en/newsroom/resources/moores-law.html (accessed 2024-02-04).
18. Wang, C.; Wang, Y.; Jiang, C. Scaling Laws of Network Traffic Load: A Theoretical Explanation of Metcalfe's Law. arXiv December 18, 2023. http://arxiv.org/abs/2312.11110 (accessed 2024-02-04).
19. *Internet of Things | Definition, History, Examples*, & *Privacy Concerns | Britannic*a. https://www.britannica.com/science/Internet-of-Things (accessed 2024-02-04).
20. Foote, K. D. *A Brief History of the Internet of Things*. DATAVERSITY. https://www.dataversity.net/brief-history-internet-things/ (accessed 2024-02-04).
21. Ramya, C. M.; Shanmugaraj, M.; Prabakaran, R. Study on ZigBee Technology. In *2011 3rd International Conference on Electronics Computer Technology*; 2011; Vol. 6, pp 297–301. https://doi.org/10.1109/ICECTECH.2011.5942102.
22. Linh An, P. Minh; Kim, T. A Study of the Z-Wave Protocol: Implementing Your Own Smart Home Gateway. In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*; 2018; pp 411–415. https://doi.org/10.1109/ CCOMS.2018.8463281.
23. Davies, A. C. An Overview of Bluetooth Wireless Technology/ Sup TM/ and Some Competing LAN Standards. In *ICCSC'02. 1st IEEE International Conference on Circuits and Systems for Communications. Proceedings (IEEE Cat. No.02EX605)*; 2002; pp 206–211. https://doi.org/10.1109/OCCSC.2002.1029081.
24. Unwala, I.; Taqvi, Z.; Lu, J. Thread: An IoT Protocol. In *2018 IEEE Green Technologies Conference (GreenTech)*; 2018; pp 161–167. https://doi.org/10.1109/GreenTech.2018.00037.
25. Ibrahim, S. E.; Bilal, D. K. H. Performance Evaluation of Wi-Fi Network. 2012, 3 (9).
26. Tuohy, J. P. *All the smart home products that work with Matter*. The Verge. https://www.theverge.com/23568091/matter-compatible-devices-accessories-apple-amazon-google-samsung (accessed 2024-02-04).
27. *Introduction to Matter - latest - Silicon Labs Matter Silicon Labs*. https://docs.silabs.com/matter/latest/matter-fundamentals-introduction/ (accessed 2024-02-04).
28. *Matter*. Google Home Developers. https://developers.home.google.com/matter (accessed 2024-11-23).
29. Inc, *A. Matter support in iOS 16 - Apple Home*. Apple Developer. https://developer.apple.com/apple-home/matter/ (accessed 2024-11-23).

Authors

Dhanush Arun is a Junior at American High School in Fremont, California. He has a deep passion for both computer hardware and software. He is planning on majoring in Electronics or Computer Science.

DOI: 10.36838/v7i1.22