Impact of IoT on Personal Area Networks (PANs)

Thilakarathna D.R.T.D.[a], Gamage N.H.[a], Mendis B.P.U.[a], Kavindya P.M.S.[a], Sammani H.M.[a], Senanayake M. M. V. [b]

[a]Department of Scientific Computing, [b]Department of Knowledge Engineering & Communication, Faculty of Computing, University of Sri Jayewardenepura

[a]tharinduthilakarathna2003@gmail.com , [a]nipunharsh3@gmail.com , [a]pasinduudana12m2@gmaul.com , [a]sachinikavindya2023@gmail.com , [a]hirushisammani23@gmail.com , [b]vindya@sjp.ac.lk

ABSTRACT

The Internet, as a revolutionary technology, continues to develop new technologies and software, making it accessible to all. Today, the most common forms of communication are either human-to-human or human-to-device communication; however, the Internet of Things (IoT) foresees a promising future for machine-to-machine (M2M) communication. Many novel wireless technologies, including ZigBee and Bluetooth, compete to provide the Internet of Things with low-power wireless communication solutions; however, in some IoT applications, the technological options are constrained by hardware resource limitations, low power consumption requirements, and overall device costs. Low power consumption is a basic prerequisite for enabling IoT expansion. Besides low power consumption, other requirements must be considered, such as technology cost, security, manageability, usability, wireless data rates, and communication ranges, among others. This paper discusses how the Internet of Things is transforming PANs, with particular focus on proximity communication protocols such as IEEE 802.15.4, Bluetooth, and ZigBee. The scope of this study extends beyond conventional device interconnection to cover new application areas like smart homes, healthcare, wellness, and wearables, succinctly presenting key trends and challenges from current literature, technology standards, and empirical evidence while analyzing critical factors in IoT-integrated PANs such as network scalability, privacy, interference control, and data security, which introduce new complexities to design and administration. This research offers details of IoT-PAN integration by conducting an analysis of wireless integrated personal area networks to identify research gaps and propose future directions. It defines the most important communication protocols and examines adequate levels of security and privacy, analyzing relevant literature to develop a robust framework that enables researchers and practitioners to address gaps in the literature regarding IoT-PAN integration. Therefore, this paper highlights the importance of PAN solutions that are secure, adaptable, and interoperable to enable next-generation IoT ecosystems by providing future insights.

KEYWORDS: *Internet of Things (IoT), Machine-to-Machine Communication (M2M), Personal Area Networks (PANs), SOHO (Small Office/Home Office), BLE (Bluetooth Low Energy)*

INTRODUCTION

The use of IoT devices and related technologies as catalysts for great shifts in our daily activities is becoming increasingly important. We may find ourselves sometimes observing, while at other times not recognizing, an IoT device embedded in everyday devices around us. To advance the public imagination, next-gen IoT applications, such as Internet-connected user gadgets, household control systems, and energy control systems, are emerging to bring about the manifestation of the "Smart home" concept and thus create further demand for Personal Area Networks (PANs).

Recent market data emphasizes rapid growth and the exciting potential of the IoT market. The global IoT market is projected to be approximately USD 64.8 billion in 2024 and grow to USD 153.2 billion by 2029, primarily driven by recent advances in connectivity, sensing capabilities, and cloud integration (MarketsandMarkets, 2024). The enterprise IoT market, specifically, has experienced rapid growth and is estimated to be approximately USD 600.8 billion in 2023, growing to more than USD 1.8 trillion by 2032 (Pangarkar, 2025) . Despite this predicted growth, enterprises still face challenges related to IoT adoption, such as successfully integrating IoT solutions into legacy systems, lengthy product development cycles (time-to-market has increased by over 80% in the last 4 years, to approximately 41 months), and ongoing

https://doi.org/10.54389/LTCQ5147

challenges regarding security, interoperability, and data management (Paraskevopoulos, 2024). These issues require robust architectural design, the use of standardized communication approaches, and better management approaches to fully realize the potential value of IoT-enabled systems.

A PAN is basically a computer network that interlinks computers or devices within an individual's immediate vicinity. A PAN limits networks to roughly 10 meters (33 feet) or less per person. This short-range network facilitates communication between devices or allows them to connect to the Internet and to higher-level networks, where a single master device serves as a gateway. A typical PAN consists of a computer and printer, a mobile telephone, a tablet, a PDA, and accessories for entertainment purposes such as video game consoles, TV remotes, wearables, and speakers, among others. PANs facilitate communication between devices in a SOHO (Small Office/Home Office) environment and allow resource sharing, data transfer, and application sharing using either wired or wireless connections. Therefore, IoT can be used to enhance PANs, which means that even greater demand arises from the continuous miniaturization of devices with technological evolution, facilitating data and resource sharing across different devices. Unlike traditional PANs, which have limited range and capabilities, PANs enhanced with Internet of Things (IoT) capabilities use more advanced protocols like ZigBee and BLE. The convergence of IoT with PANs therefore enhances energy efficiency, data transmission speed, cost efficiency, automation and control, and device interconnectivity within PANs.

While IoT-based PAN solutions are growing rapidly, existing research has gaps that remain unexplored that may prevent fully realizing this technology's potential. Research has emphasized protocol optimization, energy efficiency, and device interoperability, but has provided less focus on standardized security paradigms for IoT-enabled PANs. Many studies have focused on specific technical elements without creating integrated models combining security, scalability, and latency. Most studies assess performance in laboratory conditions rather than real-world large-scale implementations, particularly for heterogeneous PANs where multiple IoT devices from different vendors must work together. These gaps require longitudinal studies, rigorous cross-vendor compatibility testing, and developing adaptive protocols driven by network dynamics and emerging cyber threats. IoT integration into PANs has changed their uses and features. Once focused on simple device connection, PANs now support smart environments where multiple devices work together to automate tasks, monitor health, and improve daily life. This evolution brings technical challenges including security, energy efficiency, and scalability that must be resolved.

In pursuit of the objectives, this paper is structured in the following manner. Section 2 gives an overview of PAN technologies and their communication protocols. Section 3 describes key technologies and the applications of advanced technologies. Section 4 states the critical analysis, challenges, and limitations, and Section 5 states future directions and open issues. Finally, conclusion and implications for further research are presented in Section 6.

BACKGROUND

Definition of IoT and PAN

Personal Area Network (PAN)

PAN is a small-range network connection that connects devices within a range of 10 meters. Devices like smartphones, tablets, laptops, and Bluetooth devices communicate with each other using this network. There are two types of PANSs: wired and wireless.

Wired: Uses physical connections like cables to connect devices within about 10-15 meters. There are several examples of wired PANs. USB (Universal Serial Bus) is universal and most widely used for computers, peripherals, and smartphones. FireWire was a previous standard that allowed high-speed data transfer, typically used with video cameras and audio equipment. Thunderbolt is a connection standard that enables superfast transfers of large files between laptops, external storage, and displays, among other devices.

Wireless: A wireless network connects devices without cables or physical connections. It connects devices like smartphones, tablets, and personal computers to a small office or home space. Examples of wireless PANs include Bluetooth, Zigbee, Near Field Communication (NFC), Infrared (IR), and Wi-Fi Direct (Yasar, 2024).

Real-World PAN Developments: The practical implementations of PANs are ever-increasing across a variety of industries, and PANs are an important enabling technology that allows devices to connect, and transfer data within short distances. In the health care industry, PANs allow for continuous monitoring of patients via wearable medical devices and enable the collection and transmissions of vital signs to providers (Kumar, et al., 2023). In smart home environments, PANs facilitate the pairing of various systems like lighting, smart thermostats, security cameras, and entertainment units to give automated control to the user (Li, et al., 2023). Similarly, industries use PANs to keep track of assets and to ensure worker safety through sensor-based wearables. Additionally, consumer electronics now rely heavily upon wireless PAN protocols like Bluetooth and Zigbee, allowing seamless connectivity of smartphones, headphones, fitness trackers, and peripherals. The increasing implementation of PANs demonstrates their significance as reliable infrastructures necessary to enable our everyday lives that are increasingly embedded within the IoT.

Protocols	Use case	Features
Bluetooth	Audio devices, wearables, mobile phones	Low latency, moderate power consumption.
Zigbee	Smart home sensors	Mesh networking, long battery life.
IEEE 802.15.4	Industrial IoT (6LoWPAN)	Ultra-low power, IPv6 compatibility.

Table 1. Comparison of PAN protocols based on use cases and key features

The Internet of Things (IoT)

IoT is a very vast system connected with the internet. This IoT is very important for many industries like healthcare, engineering, sports, transport, etc. Things are sensor-embedded with software, electronics, and networks. This technology helps to improve our work capacity, decision-making, real-time monitoring of our tasks, and automates different types of our work (2505).

EVOLUTION OF PAN TECHNOLOGIES AND IOT-ENABLED APPLICATIONS

Overview of traditional PAN technologies

Bluetooth

Bluetooth is a short-range wireless standard that allows electronic devices to connect wirelessly. The latest Bluetooth Low Energy technology has made exceptional enhancements, theoretically enabling connection with an infinite number of devices. The standard is very helpful for users and can be found nearly everywhere in small environments, like workplaces, homes, or vehicles. As many have discovered, Bluetooth is an extremely basic and helpful wireless innovation for connecting headsets, mobile phones, keyboards, and computers (ammattikorkeakoulu, 2010).

Industry Usages: Commonly found in consumer electronics, automotive, health care devices, wearables, and office peripherals for seamless cable-free connections.

Performance Data: Bluetooth Low Energy (BLE) enables low power consumption connections with range around 10 meters indoors (up to 100 meters for Class 1 devices). Data transfer rates achieve up to 1 Mbps for BLE and higher for classic Bluetooth, making it power efficient for frequently charged devices (Mitra, Brown, Huffman, & Hong, 2020).

Zigbee

ZigBee is an intelligent standard created for applications requiring low data rate remote networking, low battery consumption, and low operating costs. The standard provides exceptional flexibility compared to other network types, with robust and secure communication. Most advanced remote communications were designed to achieve higher data transmission with longer operating distances. However, components like sensors and controls in dynamic systems don't require high bandwidth but need extremely low battery consumption to conserve power. A ZigBee 802.15.4 system is designed to operate at 1mW of radio frequency power. It is the standard technology addressing applications like remote monitoring, control, and sensor network capabilities for short-distance communication.

Industry Application: Zigbee is aimed at home automation, industrial control, smart lighting, smart metering, and sensor networks requiring low-power operation and reliable secure communications.

Performance Data: Zigbee operates in the 2.4 GHz band at 250 kbps data rate. It supports mesh networking with up to 65,000 nodes, indicating much greater scale than Bluetooth. Zigbee reaches distances of 10-100 meters with good wall penetration. It can run on batteries for years due to extremely low power consumption and uses 128-bit AES encryption for security.

IEEE 802.15.4

Low-Rate Wireless Personal Area Networks (LR-PAN) have become popular in recent years. These networks can be implemented with minimal or no infrastructure. The first standardization step for LR networks was taken in 2003 when IEEE 802.15.4 was approved. An updated version was released in 2006 as IEEE 802.15.4-2006 (802.15.4b). Neither standard supported ranging capabilities between nodes in the network. To support distance and location information, IEEE 802.15.4-2007 (802.15.4a) was approved. Standardization continued with newer standards like IEEE 802.15.4c and 4d being authorized recently (Salman, Rasool, & Kemp, 2010).

Industry Use: Supplies the physical and MAC layers that Zigbee and others use. It is a low-rate wireless standard used in applications requiring long battery life and low data rates for wireless communications, including wireless sensor networks in industries and smart homes.

Performance Information: First published in 2003 with multiple iterations (802.15.4-2006/7, etc.) adding capabilities like ranging and location. Data rates range from 20-250 kbps over distances up to 100 meters under appropriate conditions. Low power consumption enables extended sensor operation. (Hardesty, 2024).

Integration of IoT with PAN standards

Enhancements in low-power communication

Low-power communication is now supported by these PAN standards, which are crucial for Internet of Things devices. Many devices are powered by small batteries and don't need recharging for extended periods. Low-power communication enables effective data transmission while conserving energy. Devices using these technologies can operate without frequent charging and are used in wearable technology, smart homes, and health monitoring, making systems more reliable and suitable for daily use.

Network topology adaptations

IoT networks are structured networks where constrained devices are organized in hierarchies called topologies. IoT networks consist of sensors and actuators operating in various fields. These constrained sensor and actuator nodes communicate with each other and with external devices on the wider Internet. A common network arrangement involves nodes that collect environmental measurements and send them to a gateway or border router. A gateway typically has multiple network interfaces: a wireless interface for the low-power wireless network and a wired interface connecting to a local computer or the internet. Mesh-based topologies are the most suitable and popular among IoT applications.

Applications for IoT-enhanced PANs

Healthcare and wearables

In healthcare, IoT wearables are increasingly tied to AI-powered analytics platforms that forecast health risks and customize treatment plans based on continuous data streams. Devices such as smart ECG monitors, glucose sensors, and pulse oximeters connect through wireless PANs to mobile devices or gateways that securely transmit data to cloud-based health systems. This connectivity strengthens telemedicine, remote patient monitoring, and emergency response systems, ultimately reducing hospital utilization and operating costs. Healthcare providers can leverage 5G networks for low latency and reliable real-time data transfer, supporting critical monitoring during surgery or in intensive care units. An emerging example are FDA-approved wearable devices like the Apple Watch that detect atrial fibrillation, giving patients health insights while enabling a proactive approach to healthcare (Thottempudi, Konduru, Valiveti, Kuraparthi, & Kumar, 2025).

Smart homes and IoT appliances

Smart houses have numerous features. For example, automated lights detect the presence in a room and switch on automatically, or they can be voice-activated. Smart homes increasingly use integrated IoT ecosystems that combine PAN protocols such as ZigBee, Z-Wave, and Bluetooth Low Energy with cloud platforms, providing real-time interactions across devices through built-in automation and user configuration. An example is a smart thermostat that uses real-time occupancy and weather data to optimize its heating and cooling strategy, minimizing energy consumption without affecting occupant comfort. Smart security systems use facial recognition cameras and AI tools for immediate emergency response through detection capabilities and provide remote management for entry and lockdown. Market leaders like Philips Hue and Google Nest demonstrate smart home technology integration that improves user experience and operational efficiency. The integration of smart home technologies enhances user experience while supporting energy sustainability goals and adding property value.

Fitness monitoring and body sensor networks

Fitness monitoring in IoT-enhanced PANs uses smart devices like fitness bands or smartwatches to track physical activities including steps, heart rate, sleep patterns, and burn calories. These devices create complex Body Sensor Networks (BSNs) that operate using wireless low-power communication protocols **to** gather health data from multiple sensors including accelerometers, gyroscopes, and heart rate monitors on or inside the body. BSNs support continuous monitoring with long battery life by combining collected data for biometric profiling (Peng, Zhang, & Pang, 2025).

Data can be processed locally on the device or offloaded to cloud platforms using machine learning algorithms to assess early warning signs of health abnormalities and provide fitness coaching. This enables real-time health monitoring, fitness routine improvement, and early detection of health issues by individuals and medical professionals. Commercial BSN implementations like Fitbit, Garmin, and WHOOP achieve adoption rates as high as 95% for activity recognition. APIs enables BSNs to connect with third-party health and nutrition applications, providing a comprehensive healthcare approach. Professional sports and healthcare providers use BSN data for performance optimization and rehabilitation.

Comparative Analysis

The evolution of PANs from traditional to IoT-based systems has brought changes in performance, energy consumption, and communications. (The ZigBee Alliance, 2015).

Table 2. Comparison between traditional PANs and IoT-enhanced PANs

Feature	Traditional PANs	IoT-Enhanced PANs
Example Technologies	Bluetooth Classic, Zigbee, IR	Bluetooth low energy (BLE), Zigbee Pro, Thread and 6LoWPAN
Power Consumption	Moderate to high	Optimized for ultra-low power operation
Data Rate	Moderate (up to 1 Mbps for Bluetooth)	Application-specific, optimized (125 kbps to 2 Mbps for BLE)
Range	Limited (10–30 meters)	3 Extendable to mesh networks (100+ meters)
Topology Support	Mostly star	Mesh, star, tree (dynamic and saleable)
Protocol Stack Complexity	Simple, often single purpose	Modular stack with IPv6 (e.g. 6LoWPAN) support
Application Scope	Device pairing (e.g., phones to headsets)	Health Care, Smart Home, Industrial IoT, Wearables
Security	Basic pairing encryption	Multiple layers of security (AES, ECC, session keys)
Interoperability	Often vendor-specific	Designed for multi-vendor IoT ecosystems

Diagram: Protocol Stack Comparisons

The following diagram shows the difference in stack architecture between traditional PAN and IoT-enhanced PAN implementations (Ala Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015):

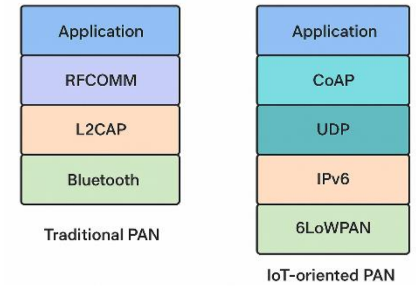

Figure 10. Protocol Stack Comparisons

CRITICAL ANALYSIS OF IOT-ENHANCED PANS

Key Challenges in IoT-Enhanced PANs

Security and privacy issues

According to (Aqeel-ur Rehman, Khan, Moiz, & Rehman, 2016) and, (Kumar, Zymbler, & Tiwari, 2019), major security issues include identification, authentication, data management, cyber-attacks, risks, and vulnerabilities. Many IoT devices have weak security because they are small and lack the power to support strong security methods, making them easily accessible to hackers. Data management is problematic because updating and managing numerous devices securely is difficult. Privacy is important for user comfort and security. IoT devices often collect personal data without user knowledge, creating significant problems. Better regulations, stronger but simpler security systems, and increased awareness about data protection in IoT environments are needed.

Power consumption and Energy efficiency

The discussion of power consumption and energy efficiency is crucial because many IoT devices run on batteries and are used in remote areas. Many IoT devices, such as sensors and cameras, need to work for extended periods without frequent charging or maintenance. Constant data transmission, sensing, and processing can quickly drain device power, creating significant problems in IoT environments. It is necessary to reduce power usage while keeping devices active and reliable. Techniques such as low-power communication protocols, energy harvesting, and smart sleep modes can improve energy efficiency (Mahmoud & Mohamad, 2016).

Quality of Service

According to (Kumar, Zymbler, & Tiwari, 2019), Quality of Service is another important challenge in the IoT environment. We can define it as a measure of the quality, efficiency, and performance of IoT devices. We can identify several problems with the quality of service: there are limited bandwidth, unreliable wireless connections, and power constraints. IoT devices should transfer data on time without delay. Some applications need real-time responses. For example, a health monitoring application needs to send data quickly and without delay. Also, managing these different requirements while many devices are connected simultaneously is challenging. IoT devices often can't fulfill these Quality-of-Service requirements because IoT devices are low-cost and have limited processing power. This makes it difficult to implement advanced QoS techniques. To improve the IoT environment, there is a need for a robust environment that includes reliable and high-speed connections; devices should be energy efficient, and capable of processing data quickly.

Heterogeneity

We can simply define the IoT environment as working with different types of devices, networks, platforms, and data formats. Additionally, IoT systems include a wide range of devices like sensors and cameras. These devices are manufactured by different manufacturers using different technologies. Apple vs Android is one of the best examples of different technologies. However, in an IoT environment, every device should share data and communicate, and connectivity is necessary. Therefore, IDRA (Integrated Data Routing Architecture) is a more suitable solution for this problem (Aqeel-ur Rehman, Khan, Moiz, &

Rehman, 2016). If the IoT environment does not implement such solutions, it cannot build scalable, reliable, and efficient IoT systems.

Scalability

On the Internet of Things context, scalability can be simply described as the ability of a system to manage a growing number of users, devices, and data while maintaining optimal performance levels (Asad Yasin, Maqbool hussain, 2024). Data overload, storage issues, and data quality are several challenges related to data volume and management. Bandwidth limitations, latency, and interference are challenges in network communications. Security, deployment, and maintenance are challenges in device management and configuration. To achieve good scalability, the system should use flexible architecture, cloud or edge computing, and efficient data management techniques.

FUTURE DIRECTIONS AND OPEN ISSUES

Emerging PAN standards for IOT

BLE Mesh

Bluetooth Low Energy, otherwise known as BLE, is a special kind of wireless technology that is meant for low-energy communication. The technology finds its application in a wide range of IoT applications. Meanwhile, BLE also finds usefulness in heart rate monitors for sending data to smartphones for health monitoring. BLE's working range is typically 10 to 100 meters. Apart from this, BLE possesses the capability of making multiple connections simultaneously.

Thread

Thread is also low power and wireless technology. It is suitable for larger and more complex networks. Thread is very good at security. It uses strong encryption. So, this helps to keep the network protected from hackers. Thread is an excellent choice for extensive smart home networks.

Trends in Miniaturization and Edge computing for PANs

Miniaturization

As technology advances, we can optimize electronics into compact parts, such as smartwatches, medical sensors and fitness trackers. These devices can now easily be placed onto the body or into everyday objects. Enhancements in the field of semiconductors, improved efficiency, reduced energy expenditure, and reduced overall expenditure are advantages of miniaturization.

Edge computing

Edge computing is unlike cloud computing. Edge computing means small devices can process data without the internet. The focus of edge computing is to decrease latency and increase responsiveness when processing data that requires real-time results. At the same time, it is used for autonomous cars, industrial automation, and real-time virtual environments.

The use of new technologies such as BLE Mesh and Thread will mark new advances in IoT-enabled PANs. Also, as devices become more advanced and smaller in size, and as edge computing becomes increasingly important in the enhancement of responsiveness, these IoT-enabled PANs will become more effective.

Potential of Artificial Intelligence and Machine Learning in PAN Management

The Artificial Intelligence (AI) system oversees how PAN devices communicate with each other through their networks. Every PAN includes multiple devices like sensors, fitness bands, and smartwatches. These devices need to work together while exchanging information. PANs require strong security measures when they handle health information and location data. Machine Learning (ML) also helps on the security side, as when a hacker tries to connect and access data, ML processes can handle unauthorized access by blocking access or sending warning messages. Since many PAN devices are powered by small batteries, saving energy is very important in the PAN system. Therefore, AI applications can help reduce the power usage of IoT-enhanced PANs.

Research Gaps and Future Exploration Areas

The innovative part of IoT-PAN integration is its potential to evolve traditional short-range networks into intelligent ecosystems which are applicable in healthcare, smart homes, and wearable technologies, enabling real-time applications. Future studies need to focus on creating uniform security standards for low power PAN devices, as the existing approaches are fragmented and limited to specific vendors. One more potential contribution is the AI and ML powered PAN management systems that automatically tune energy consumption, load balancing, and intrusion detection in heterogeneous networks. There are also gaps in cross vendor interoperability testing as most of the research is conducted in controlled laboratory environments as opposed to large-scale, real-world, uncontrolled settings. Other emerging technologies focus on integrating edge computing into PAN protocols, which would decrease latency and facilitate real-time IoT decision-making. In summary, the primary contribution is offering a roadmap showing how IoT-enabled PANs can evolve toward scalable, secure, and adaptive systems to drive the next generation of pervasive computing.

CONCLUSION

The combination of IoT and PANs has radically transformed the landscape of short-range communication, facilitating a new generation of networked devices that support smart, real-time applications across various fields such as healthcare, home automation, and fitness monitoring. By integrating protocols like Bluetooth, ZigBee, and IEEE 802.15.4, IoT-enhanced PANs demonstrate significant improvements in energy efficiency, data transmission rates, device interoperability, and automation capabilities. However, this development brings new challenges. Security and privacy remain primary concerns because the typically constrained processing power of IoT devices makes them vulnerable to attacks. Additionally, factors such as energy constraints, scalability, heterogeneity, and Quality of Service (QoS) limitations underscore the need for highly resilient adaptive solutions. Overcoming these challenges requires a multi-faceted approach based on sophisticated encryption techniques, standardized protocols, energy-aware design, and intelligent resource management methods. This research provides a comprehensive analysis of IoT-PAN integration by assessing proposed solutions for building secure and efficient PANs, conducting detailed protocol analysis, and identifying the primary obstacles and specific challenges in IoT-PAN integration. Furthermore, the comparison between traditional and IoT-enhanced PANs offers valuable insights for system designers regarding improvements in system efficiency, interoperability, and application scope. As the IoT ecosystem expands, PANs will become fundamental pillars of pervasive and secure communication between adjacent devices. Future research must therefore focus on designing scalable and interoperable architectures that provide security, privacy, and resilience while maintaining the lightweight and power-efficient characteristics of PANs. This will ultimately enable the development of sustainable, intelligent, and user-centric IoT applications that enhance quality of life.

REFERENCES

1. Ala Al-Fuqaha, Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015, June 15). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 2347–2376. doi:10.1109/COMST.2015.2444095
2. ammattikorkeakoulu, M. (2010). Retrieved from https://www.theseus.fi/handle/10024/15812
3. Aqeel-ur Rehman, A.-u., Khan, I. U., Moiz, M., & Rehman, S. u. (2016, December). Security and Privacy Issues in IoT. *International Journal of Communication Networks and Information Security (IJCNIS), x*, 147-157.
4. Asad Yasin, Maqbool hussain. (2024). Scalability Challenges and Solutions in Massive IoT Networks. *International Journal of Advanced Engineering Technologies and innovations, 10*.
5. Hardesty, G. (2024, November 08). ZigBee Compared to Bluetooth and Wi-Fi for IoT Applications. Retrieved August 12, 2025, from https://www.data-alliance.net/blog/zigbee-antennas-frequencies-types-applications/

6. Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. h., & Hosen, S. (2023, April 28). Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics*, 1-19. Retrieved Agust 12, 2025
7. Kumar, S., Zymbler, M., & Tiwari, P. (2019). Internet of Things is a revolutionary. *Journal of Big data*, December.
8. Li, M., Gu, W., Chen, W., He, Y., Wu, Y., & Zhang, Y. (2023). Smart Home: Architecture, Technologies and Systems. *131*, 393-400. Retrieved August 12, 2025, from https://www.sciencedirect.com/science/article/pii/S1877050918305994
9. Mahmoud, M. S., & Mohamad, A. (2016, January). A study of efficent power consumption Wireless communication Techniques. *Advances in Internet of Things, 6*, 19-29.
10. MarketsandMarkets. (2024, August). Retrieved August 12, 2025, from MarketsandMarkets: https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html
11. Mitra, R., Brown, G., Huffman, M., & Hong. (2020). Telecommunications and Networking. Retrieved August 12, 2025, from UTSA Pressbooks: https://utsa.pressbooks.pub/networking/chapter/short-range-wireless/
12. Pangarkar, T. (2025, January 14). Retrieved August 12, 2025, from Market.us: https://scoop.market.us/enterprise-iot-statistics/
13. Paraskevopoulos, D. (2024, April 25). (I. Analytics, Editor) Retrieved August 12, 2025, from https://iot-analytics.com/challenges-iot-product-launches-why-time-to-market-has-increased-80-percent-in-4-years/
14. Peng, Y., Zhang, G., & Pang, H. (2025, march 12). Impact of Short-Duration Aerobic Exercise Intensity on Executive Function and Sleep. Retrieved from arxiv.org: https://arxiv.org/abs/2503.09077
15. Salman, N., Rasool, I., & Kemp, A. (2010). Overview of the IEEE 802.15.4 standards family for Low Rate Wireless Personal Area Networks. *7th International Symposium on Wireless Communication Systems.* York, UK: IEEE.
16. The ZigBee Alliance. (2015). *ZigBee Specification.* 508 Second Street ,Suite 206 ,Davis, CA 95616, USA: ZigBee Alliance, Inc.
17. Thottempudi, P., Konduru, R. M., Valiveti, H. B., Kuraparthi, S., & Kumar, V. (2025, February 25). Digital health resilience: IoT solutions in pandemic response and future healthcare scenarios. *6*. Retrieved August 12, 2025, from https://link.springer.com/article/10.1007/s43621-025-00886-7
18. Yasar, K. (2024, september 04). Retrieved 05 21, 2025, from https://www.techtarget.com/searchmobilecomputing/definition/personal-area-network