Journal of Advanced Research in Computer Graphics and Multimedia Technology
Volume 11, Print Issue 1 - 2024, Pg. No. 5-11
Peer Reviewed Journal

Review Article

Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review

Shubh Dave

Research Scholar, MCA, Thakur Institute of Management Studies, CareerDevelopment & Research (TIMSCDR) Mumbai, India.

I N F O

E-mail Id:
daveShubh3@gmail.com
Orcid Id:
https://orcid.org/0009-0002-8662-1731
How to cite this article:
Dave S. Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review. *J Adv Res Comp Graph Multim Tech.* 2024; 11(1): 5-11.

Date of Submission: 2024-03-01
Date of Acceptance: 2024-04-03

A B S T R A C T

The rise of the Internet of Things (IoT) marks a revolutionary shift, transforming our everyday existence into a high-tech tapestry. From the interconnected brilliance of smart cities and homes to the meticulous management of pollution, energy, transportation, and industries, IoT has been the catalyst for these groundbreaking changes. Countless research endeavors have tirelessly worked to elevate IoT technology, but amidst the progress lie numerous unresolved challenges yet to be surmounted. In this landscape, the quest for IoT's full potential demands a holistic approach, encompassing its applications, hurdles, enabling technologies, and social and environmental impacts. This review article endeavors to delve deep into these facets, painting a comprehensive picture that straddles both the technological and societal realms. It meticulously dissects the challenges and pivotal issues that confront IoT, elucidating its architecture and significant application domains. Moreover, it shines a spotlight on existing literature, meticulously detailing their contributions across various dimensions of IoT. Furthermore, the article amplifies the significance of big data and its analysis concerning IoT—a critical junction that warrants profound exploration. Its overarching aim? To serve as a guiding beacon for readers and researchers alike, illuminating the intricate landscape of IoT and its tangible implications in the real world.

Keywords: IoT, Remote Sensor, Data storage

Introduction

The Internet of Things (IoT)[1] emerges as a transformative paradigm, bridging devices and sensors through the internet to enhance our daily lives. Leveraging smart technology and the internet, IoT pioneers' innovative solutions across diverse industries worldwide. Its omnipresence underscores its burgeoning significance in our lives. Essentially, IoT amalgamates a vast array of intelligent systems, frameworks, and sensors in Figure 1, harnessing quantum and nanotechnology for previously inconceivable storage, sensing, and processing capabilities.

An extensive corpus of research, spanning scientific articles, online reports, and printed materials, showcases the profound efficacy and applicability of IoT transformations. It serves as a groundwork for innovative business endeavors, prioritizing security, assurance, and interoperability.

IoT's pervasive influence is unmistakable, reshaping our routines with the proliferation of IoT devices and technologies. One such evolution is the advent of Smart Home Systems (SHS) and appliances, integrating internet-based devices and energy-efficient management systems.[2] Notably, Smart Health Sensing Systems (SHSS) epitomize another milestone in IoT, employing intelligent devices to monitor human health indoors and outdoors, revolutionizing healthcare practices in hospitals and wellness centers.

IoT pioneers actively engage in enhancing the lives of the elderly and differently-abled through cost-effective, easily accessible smart devices, facilitating a more independent lifestyle. Transportation, too, undergoes a paradigm shift, employing intelligent sensors and drone devices to regulate traffic and suggest alternate routes for congestion-free travel.

The vast scope of IoT extends to technology augmentation and human facilitation, impacting

economic and industrial growth. Its significance in trade and stock markets marks a revolutionary step forward. However, data security remains a paramount concern, with IoT striving to combat cyber threats and fortify information security.

Addressing these concerns, IoT developers are diligently crafting secure pathways for collaboration between social networks and privacy safeguards, a pivotal topic in IoT.[3] The subsequent sections of this article delineate the current landscape, IoT architecture, key challenges, burgeoning applications, and the pivotal role of big data analytics. Finally, drawing together these insights, the conclusion underscores the multifaceted impact and potential trajectory of IoT.

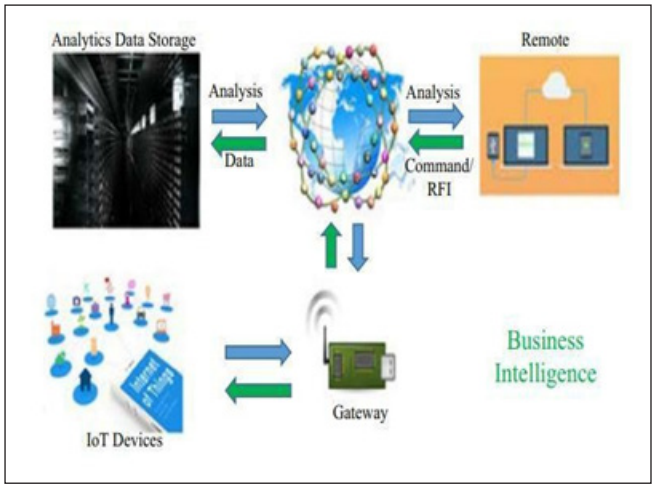

Figure 1.General architecture of IoT

Literature Survey

The Internet of Things (IoT) embodies a multifaceted vision, extending its benefits across various domains like environmental conservation, industrial enhancement, public and private sectors, medical advancements, and transportation optimization [4]. Diverse perspectives from researchers have illuminated IoT's spectrum, each tailored to specific interests and facets. This breadth of potential and power manifests vividly across several application domains, as depicted in Figure 2, showcasing IoT's expansive capabilities.

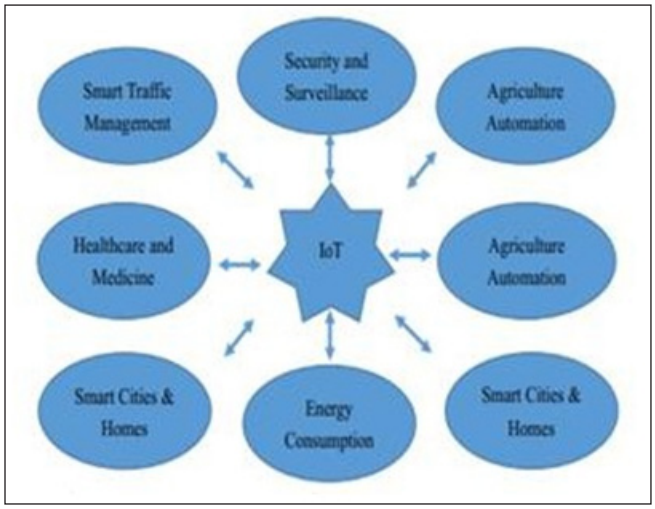

Figure 2.IoT's capabilities

In recent years, pivotal IoT projects have surged into the market, shaping landscapes and dynamics. Figure 3 outlines some key projects that have carved significant market space. This global distribution, as illustrated in Fig. 3, delineates how the Americas spearhead healthcare and smart supply chain initiatives, while Europe takes the lead in the realm of smart city projects.[5]

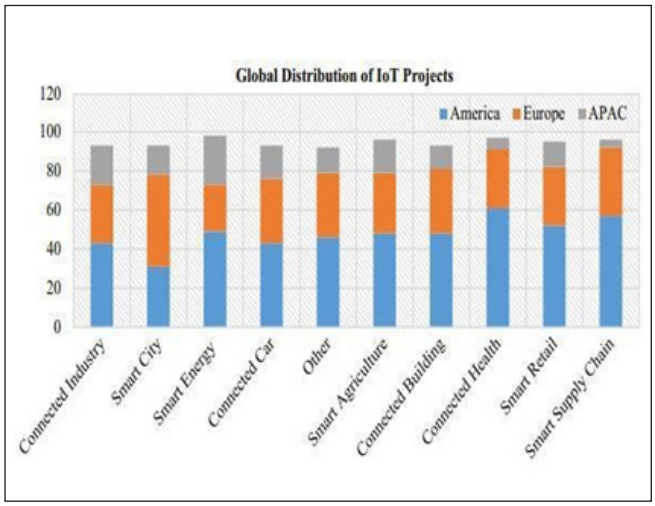

Figure 3.Global Distribution of IoT Projects

An intriguing insight emerges in Figure 4, portraying the global market share of IoT projects worldwide. Industries, smart cities, energy optimization, and intelligent vehicular systems dominate this space, holding substantial market stakes compared to other sectors. The allure of the smart city concept within the IoT ecosystem has burgeoned, encompassing the integration of smart homes. These homes host a plethora of IoT-enabled appliances, heating/cooling systems, entertainment devices, and security mechanisms, fostering seamless communication aimed at optimizing.[6]

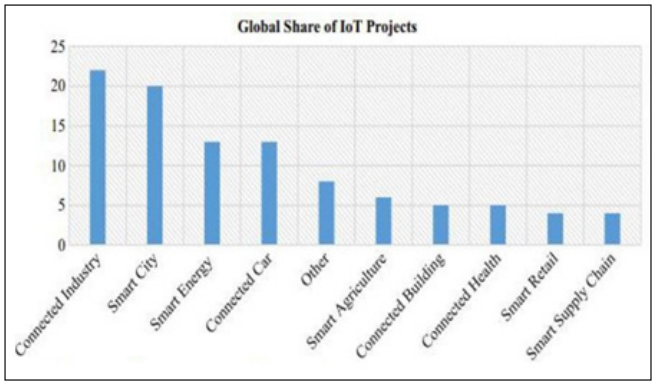

Figure 4.Global Share of IoT Projects

Comfort, security, and energy conservation. The trajectory of smart city evolution, especially in smart homes, is poised to surpass the $100 billion mark by 2022, not just amplifying in-house comfort but also driving cost efficiencies through reduced energy consumption.[7]

In parallel, smart vehicles within the smart city framework showcase a paradigm shift in automotive technology. Modern cars, equipped with intelligent sensors and devices, regulate various components, offering an amalgamation of predictive maintenance and enhanced safety through wireless communication between vehicles and drivers.

The convergence of IoT and smart energy control, as investigated by Khajenasiri, underscores the nascent yet potent role of IoT in revolutionizing energy management for smart city applications [8]. The current deployment of IoT in selected arenas hints at its vast potential to encompass myriad sectors, emphasizing energy efficiency and cost savings. However, challenges loom, particularly in the form of immature IoT hardware and software, necessitating resolution for a robust, efficient, and user-friendly IoT ecosystem.

Addressing the burgeoning urbanization challenge, advocate for IoT's pivotal role in developing smart solutions for mobility, energy, healthcare, and infrastructure within smart cities. The gamut of issues from traffic management to public safety, underscore the criticality of IoT- enabled technologies in sculpting sustainable and efficient urban landscapes.[9]

Security and privacy in IoT form critical focal points, as emphasized by Weber, urging private organizations leveraging IoT to embed robust data authentication, access controls, and privacy measures, fortifying their business operations against potential threats.[10] Furthermore, IoT's relevance extends to environmental and agricultural spheres. Their survey delineates IoT's instrumental role in fortifying agro-industrial and environmental facets, benefitting farmers and society at large

IoT Architecture and Technologies

The foundation of IoT architecture is built upon five essential layers, each defining the functionalities integral to IoT systems: the perception layer, network layer, middleware layer, application layer, and business layer as shown in Figure 5.

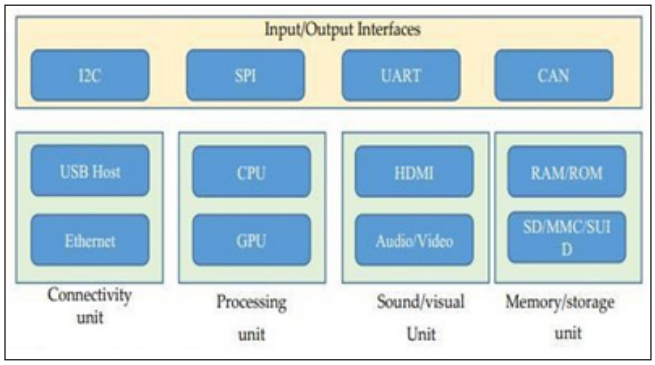

Figure 5.Frame work of IoT Devices

At the core lies the perception layer, housing physical devices like sensors, RFID chips, and barcodes interconnected within the IoT network.[11] These devices gather vital information for transmission to the network layer. The network layer serves as the conduit, employing various mediums—wired or wireless, including 3G/4G, Wi-Fi, Bluetooth—to convey data from the perception layer to the information processing system.

Moving up, the middleware layer undertakes the processing of data received from the network layer, leveraging ubiquitous computing to make informed decisions. Subsequently, the application layer utilizes this processed information for global device management. At the apex rests the business layer, steering the entire IoT system, its applications, and services as shown in Fig.6. It visualizes and utilizes insights derived from the application layer to strategize and set future targets.

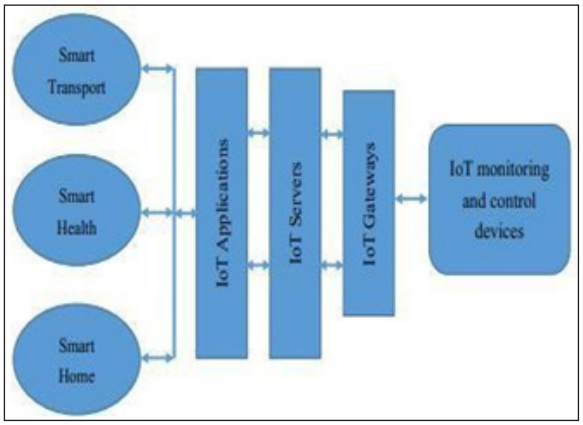

Figure 6.Working structure of IoT devices

Beyond the layered framework, the IoT system comprises functional blocks supporting various operations such as I/O, connectivity, processing, audio/video monitoring, and storage management. The synergy of these blocks forms an efficient IoT system, critical for optimal performance.

While reference architectures with technical specifications exist, a standardized global IoT architecture remains a work in progress.[12] Designing a suitable architecture that aligns with global IoT needs

remains a challenge. Scalability, modularity, interoperability, and openness emerge as pivotal design considerations in heterogeneous environments.

A robust IoT architecture should cater to cross- domain interactions, multi-system integration, scalable management functions, big data analytics, and user-friendly applications. Moreover, it should imbue intelligence and automation among IoT devices, accommodating the increasing influx of data generated by IoT sensors and devices.

Dealing with massive amounts of streaming data in IoT systems necessitates efficient architectures like cloud and fog/edge computing. These architectures facilitate handling, monitoring, and analyzing vast data volumes. A modern IoT architecture could be a four-stage model.[13]

In Figure 7, the initial stage, sensors and actuators play a pivotal role in collecting real-world data for subsequent analysis. Stage two involves aggregating and structuring the amassed data from stage one, collaborating with gateways and data acquisition systems for optimization.

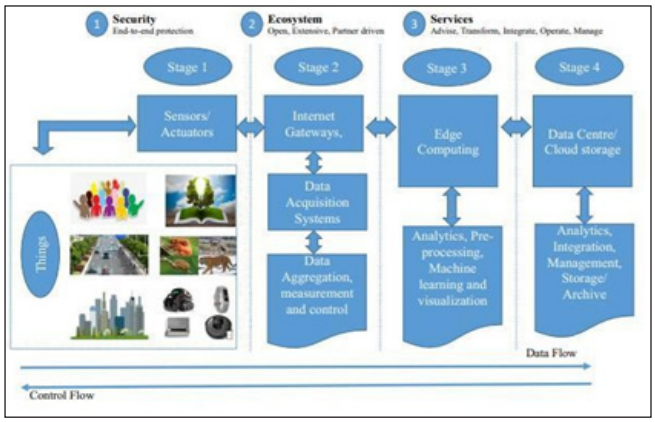

Figure 7.Fourstages of IoT architecture

Stage three, edge computing, utilizes distributed architectures to process vast data volumes efficiently, offering functionalities like visualization and machine learning-based analysis. Finally, the last stage involves in-depth processing and analysis, potentially employing cloud servers or data centers. Big data frameworks like Hadoop and Spark aid in handling large streaming data, while machine learning enhances prediction models for a more accurate and reliable IoT system.

Major Key Issues and Challenges of Iot

The involvement of IoT based systems in all aspects of human lives and various technologies involved in data transfer between embedded devices made it complex and gave rise to several issues and challenges. These issues are also a challenge for the IoT developers in the advanced smart tech society. As technology is growing, challenges and need for advanced IoT system is also growing. Therefore, IoT developers need to think of new issues arising and should provide solutions for them.

Enhancing Security and Privacy in IoT Systems

Within the realm of the Internet of Things (IoT), paramount challenges loom large in the form of security and privacy concerns. This landscape is rife with threats, vulnerabilities, and the looming specter of cyber-attacks. At the heart of device-level privacy issues lie inadequate authorization, insecure software and firmware, vulnerable web interfaces, and the lamentably poor encryption at the transport layer. To instill confidence in IoT systems across various spectrums, robust security mechanisms need embedding at every stratum of the IoT architecture to thwart potential threats and attacks. Diverse protocols have been meticulously devised and deployed across communication layers to fortify security and privacy within IoT-based systems. Notably, the implementation of Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) among others has fortified cryptographic protocols, particularly between the transport and application.[14] layers, safeguarding numerous IoT systems. However, the diversification of IoT applications necessitates distinct methods to ensure communication security between devices. Moreover, wireless communication within IoT systems amplifies susceptibility to security risks, mandating the deployment of proactive measures to detect malicious activities and ensure self-healing capabilities.

Preserving privacy is equally pivotal, fostering a sense of security and comfort among IoT users. It's imperative to uphold authorization and authentication over secure networks to establish communication between trusted entities. The issue further extends to varying privacy policies governing objects communicating within IoT systems. Thus, each object must verify the privacy policies of others before transmitting data, ensuring a seamless and secure exchange.

Tackling Interoperability and Standards

Interoperability, the seamless exchange of information among diverse IoT devices and systems irrespective of software and hardware disparities, remains a persistent challenge. The heterogeneous nature of technologies used in IoT development spawn's interoperability hurdles across technical, semantic, syntactic, and

organizational levels. Alleviating these challenges demands innovative functionalities within IoT systems to facilitate communication across diverse environments. Merging disparate IoT platforms based on functionalities emerges as a viable strategy to cater to varied user needs. While numerous handling approaches have alleviated some pressures on IoT systems, challenges persist, underscoring the need for future studies.

Ethical, Legal, and Regulatory Imperatives

The ethical, legal, and regulatory landscape presents another daunting challenge for IoT developers. As IoT resolves real-world problems, it simultaneously spawns critical ethical and legal quandaries.[15] Issues spanning data security, privacy protection, trust, and usability emerge as pivotal concerns. The lack of trust in IoT devices among users underscores the necessity for stringent norms and regulations to fortify data protection, privacy, and safety, thereby enhancing user trust in IoT devices and systems.

Ensuring Scalability, Availability, and Reliability

Scalability, the ability to expand services, devices, and equipment without compromising performance, remains a cornerstone for IoT systems.[28] Accommodating a plethora of devices with varying memory, processing power, storage, and bandwidth remains a challenge. Coupled with scalability, ensuring availability becomes pivotal. Cloud-based IoT systems exemplify scalability by adeptly supporting network scaling through the addition of devices, storage, and processing power as required.[16] However, this globalized distributed IoT network introduces a research paradigm to craft a seamless framework that caters to global needs. The challenge of resource availability across locations and timeframes in a distributed IoT environment necessitates an uninterrupted and reliable data transmission channel.

Quality of Service (QoS) Benchmarks

Quality of Service (QoS) stands as a crucial criterion for evaluating IoT devices, systems, and architectures, gauging their efficiency and performance. Vital QoS metrics for IoT applications encompass reliability, cost, energy consumption, security, availability, and service time. An astute IoT ecosystem must adhere to QoS standards and define metrics to ensure reliability. Deploying quality models such as ISO/IEC25010 and OASIS-WSQM becomes imperative to assess the approaches used for QoS evaluation. These models offer a comprehensive array of quality factors suitable for assessing IoT services

Major Iot Application

IoT's Societal Impact: Emerging Economy, Environment, and Healthcare IoT stands as a dedicated force, enriching society with public and financial benefits while fostering development as shown in Figure 8. From bolstering economic growth and maintaining water quality to promoting well-being and industrialization, its scope is vast. Efforts are directed towards aligning with the United Nations' goals for social, health, and economic advancements. Notably, environmental sustainability takes precedence. Addressing the environmental impact of IoT systems is crucial, particularly in managing escalating energy consumption from internet-enabled services and cutting-edge devices. Research endeavors aim to develop eco-friendly materials for IoT devices and adopt green technologies to lower energy consumption rates. Engineers also focus on crafting highly efficient IoT devices, pivotal in monitoring health concerns like diabetes, obesity, and depression.

Transforming Cities and Transport: IoT's Influence on Smart Structures

IoT catalyzes a shift from conventional society to smart cities, homes, and transportation networks. With advancements in machine learning and natural language processing, technology assimilates seamlessly into everyday life. Cloud server technology and wireless sensor networks, when integrated with IoT servers, optimize the framework for smart cities. Environmental considerations are paramount in smart city planning, urging the integration of energy-efficient and green technologies. IoT-incorporated devices in vehicles detect congestion and suggest alternate routes, easing city gridlocks.[17] Furthermore, monitoring engine activities in vehicles and the potential of self-driving cars communicating through intelligent sensors promise enhanced traffic flow. While widespread implementation takes time, IoT devices detecting congestion remain vital. Transportation manufacturers embedding IoT devices in vehicles present tangible societal benefits.

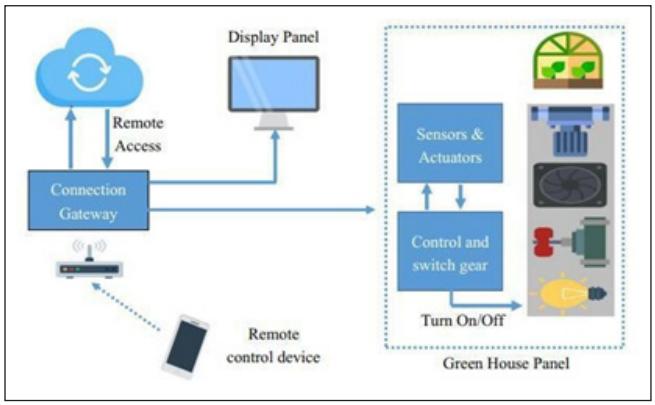

Figure 8.Application of IoT

Agriculture and Industry: Revolutionizing Production and Automation

To meet the needs of an estimated 10 billion global populations by 2050, agriculture requires a technological overhaul. Combining technology with agriculture,

greenhouse technology emerges as a promising avenue for precision control of environmental parameters, boosting yields. However, manual management proves less effective, demanding high efforts, costs, and resulting in energy loss.

IoT Advancements, Employing Smart Devices

and sensors, transform agriculture by facilitating seamless climate control and monitoring processes. This not only conserves energy but also significantly amplifies production yields. Additionally, IoT's role in industry automation proves transformative, revolutionizing digitalization in factories, inventory management, quality control, logistics, and supply chain optimization.

Importance of Big Data Analytics in IoT

An IoT system encompasses an extensive array of devices and sensors interconnected to communicate seamlessly. As the IoT network undergoes rapid expansion, the sheer number of these devices and sensors increases significantly. These devices continually exchange vast volumes of data over the internet, earning the classification of 'big data' due to its immense size and constant streaming. This continuous growth of IoT networks presents complex challenges, including data management, storage, processing, and analytics.

A framework integrating IoT and big data proves invaluable in addressing multifaceted issues within smart buildings. From managing oxygen levels to monitoring hazardous gases and luminosity, this framework efficiently gathers data from building-installed sensors, enabling informed decision-making through data analytics. Similarly, in industrial settings, leveraging an IoT-based cyber-physical system with information analysis and knowledge acquisition techniques significantly enhances production capabilities.

The issue of traffic congestion in smart cities finds resolution through real-time traffic information collected by IoT devices and sensors installed in traffic signals. This data is pivotal for analysis within IoT-based traffic management systems. In healthcare, IoT sensors continuously generate voluminous patient health data, necessitating integration into a unified database for real-time, accurate decision-making where big data technology emerges as the optimal solution.

Moreover, the amalgamation of IoT and big data analytics revolutionizes traditional methodologies in manufacturing industries, utilizing sensor-generated data for informed decision-making. Cloud computing and analytics emerge as allies in energy development and conservation, effectively reducing costs while enhancing customer satisfaction.

The copious streaming data generated by IoT devices necessitates effective storage and real-time analysis for informed decision-making. Deep learning emerges as a powerful tool to handle such massive datasets, delivering high-precision results Thus, the convergence of IoT, big data analytics, and deep learning stands as a cornerstone in fostering a highly advanced society.

Conclusions

Recent advancements in IoT have captured the global attention of both researchers and developers. This collaborative effort aims to propel the technology to new heights, intending to maximize its societal impact. However, achieving substantial improvements necessitates a critical examination of existing technical approaches and addressing prevalent issues and shortcomings.

In our comprehensive survey article, we shed light on numerous challenges and hurdles that IoT developers confront, emphasizing the imperative need to refine the existing models. Additionally, we delve into pivotal application domains where IoT developers and researchers are actively involved, recognizing that IoT not only delivers services but also generates vast troves of data.

The sheer volume of data generated by IoT systems underscores the paramount importance of big data analytics. By harnessing this analytical prowess, we can derive precise insights crucial for augmenting IoT systems and making informed decisions that significantly enhance their functionality.

References

1. Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 F e b . 2017. https://doi.org/10.1109/sm2c.2017.8071828.
2. Gatsis K, Pappas GJ. Wireless control for the IoT: power spectrum and security challenges. In: Proc. 2017 IEEE/ACM second international conference on internet-of-things design and implementation (IoTDI), Pittsburg, PA, USA, 18–21 April 2017. INSPEC Accession Number: 16964293.
3. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https://doi.org/10.1109/MCOM.2017.1600363CM.
4. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118
5. Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017.https://doi.org/10.1109/ccnc.2017.7983271.

6. Gaona-Garcia P, Montenegro-Marin CE, Prieto JD, Nieto YV. Analysis of security mechanisms based on clusters IoT environments. Int J Interact Multimed Artif Intell. 2017;4(3):55–60.
7. Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. Sustainability. 2019;11(3):763. IoT application areas. https://iot-analytics.com/top- 10-iot-project-application-areas-q3-2016/. Accessed 05 Apr 2019.
8. Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities. IEEE IoT-J. 2014;1(1):22–32.
9. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. A review on internet of things for intelligent energy control in buildings for smart city applications. Energy Procedia. 2017; 111:770–9. Internet of Things. http://www.ti.com/technologies/internet-of- things/overview.html. Accessed 01 Apr 2019.
10. Liu T, Yuan R, Chang H. Research on the internet of things in the automotive industry. In: ICMeCG 2012 international conference on management of e-commerce and e-Government, Beijing, China. 20–21 Oct 2012. p. 230–3.
11. Alavi AH, Jiao P, Buttlar WG, Lajnef N. Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement. 2018; 129:589–606.
12. Weber RH. Internet of things-new security and privacy challenges. Comput Law Secur Rev. 2010;26(1):23–30.
13. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP based internet of things. Wirel Pers Commun. 2011;61(3):527–42.
14. Liu J, Xiao Y, Philip-Chen CL. Authentication and access control in the internet of things. In: 32nd international conference on distributed computing systems workshops, Macau, China. IEEE xplore; 2012. https://doi.org/10.1109/ icdcsw.2012.23.
15. Kothmayr T, Schmitt C, Hu W, Brunig M, Carle G. DTLS based security and two-way authentication for the internet of things. Ad Hoc Netw. 2013; 11:2710– 23.