World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Survey of IoT Platforms and Tools

Hanamanth B *

Lecturer, Department of Computer Science and Engineering, Government Polytechnic, karatagi -583229, Karnataka India.

World Journal of Advanced Research and Reviews, 2022, 13(01), 901-907

Publication history: Received on 09 January 2022; revised on 19 January 2022; accepted on 28 January 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.13.1.0064

Abstract

The Internet of Things (IoT) has revolutionized the way physical devices interact with digital systems, creating unprecedented opportunities for automation, monitoring, and intelligent decision-making across diverse domains. This survey paper provides a comprehensive examination of IoT platforms and tools available prior to 2020, analyzing both commercial and open source solutions that form the foundation of modern IoT ecosystems. The paper explores the architectural components essential to IoT platforms, including device management, data processing, communication protocols, security mechanisms, and analytics capabilities. Through detailed analysis of major commercial platforms such as AWS IoT Core, Microsoft Azure IoT, Google Cloud IoT, and IBM Watson IoT, alongside prominent open source alternatives including Eclipse IoT, Things Board, Node-RED, and FIWARE, this survey identifies the strengths, limitations, and appropriate use cases for different platform categories. The comparative analysis reveals that platform selection must align with specific organizational requirements regarding scalability, budget, technical expertise, security, and customization needs. Key findings indicate that commercial platforms offer advantages in managed infrastructure, global scalability, and professional support, while open source platforms provide flexibility, cost-effectiveness, and freedom from vendor lock-in. The survey also examines emerging trends including edge computing integration, artificial intelligence incorporation, blockchain applications, and standardization efforts that were shaping the future direction of IoT platforms. This comprehensive overview serves as a valuable resource for researchers, practitioners, and organizations navigating the complex landscape of IoT platform selection and implementation, providing insights that facilitate informed decision-making in IoT project planning and execution.

Keywords: Internet of Things; IoT platforms; IoT architecture; Cloud computing; Edge computing; Device management; MQTT protocol; IoT securityArtificial Intelligence; Machine Learning; Everyday Applications; Smart Systems; Human-Computer Interaction

1. Introduction

The Internet of Things (IoT) has emerged as a transformative paradigm that connects physical devices, sensors, and actuators to the internet, enabling intelligent decision-making and automated processes across various domains. The proliferation of IoT applications in smart cities, healthcare, industrial automation, agriculture, and home automation has necessitated the development of comprehensive platforms and tools that facilitate the design, deployment, and management of IoT systems. These platforms serve as the backbone infrastructure that bridges the gap between hardware devices and software applications, providing essential services such as device management, data processing, security, and integration capabilities. The complexity of IoT ecosystems, characterized by heterogeneous devices, diverse communication protocols, massive data volumes, and stringent security requirements, has driven both industry and academia to develop sophisticated platforms that address these multifaceted challenges. According to Gartner's predictions from 2017, the number of connected IoT devices was expected to reach 20.4 billion by 2020, highlighting the urgent need for scalable and efficient IoT platforms. The selection of an appropriate IoT platform significantly impacts the success of IoT deployments, as it determines the system's scalability, interoperability, security posture, and

* Corresponding author: Hanamanth B

overall operational efficiency. This survey paper provides a comprehensive analysis of prominent IoT platforms and tools available prior to 2020, examining their architectures, features, strengths, and limitations to guide researchers and practitioners in making informed decisions for their IoT implementations.

1. IoT Platform Architecture and Components

IoT platforms typically follow a layered architecture that encompasses the perception layer, network layer, middleware layer, and application layer, each serving distinct functions in the IoT ecosystem. The perception layer consists of physical devices, sensors, and actuators that collect data from the environment and perform actions based on received commands. These devices employ various communication protocols including MQTT, CoAP, HTTP, and AMQP to transmit data to upper layers. The network layer handles data transmission and routing, supporting multiple connectivity options such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, and cellular networks to accommodate different range and power requirements. The middleware layer, often considered the core of IoT platforms, provides essential services including device management, data storage and processing, security and authentication, API management, and integration capabilities with external systems. This layer abstracts the complexity of underlying hardware and network heterogeneity, presenting a unified interface to application developers. The application layer hosts end-user applications and services that leverage IoT data for monitoring, control, analytics, and decision-making purposes. Table 1 illustrates the key components found in typical IoT platform architectures and their primary functions.

Table 1 Core Components of IoT Platform Architecture

Component	Primary Function	Key Technologies
Device Management	Device provisioning, configuration, monitoring, firmware updates	OMA-DM, TR-069, LwM2M
Data Management	Data ingestion, storage, processing, analytics	Time-series databases, NoSQL, Apache Kafka
Security Layer	Authentication, authorization, encryption, access control	OAuth 2.0, TLS/SSL, PKI
Communication Layer	Protocol translation, message routing, publish-subscribe	MQTT, CoAP, AMQP, WebSocket
API Gateway	RESTful APIs, webhook support, third-party integrations	REST, GraphQL, gRPC
Analytics Engine	Real-time analytics, machine learning, predictive modeling	Apache Storm, Spark, TensorFlow
User Interface	Dashboards, visualization, configuration tools	Web frameworks, mobile applications

Modern IoT platforms incorporate edge computing capabilities to process data closer to its source, reducing latency and bandwidth consumption while enhancing privacy and reliability. Edge nodes can perform data filtering, aggregation, and preliminary analytics before forwarding relevant information to cloud infrastructure. The integration of artificial intelligence and machine learning algorithms within IoT platforms enables predictive maintenance, anomaly detection, and intelligent automation. Container technologies such as Docker and orchestration tools like Kubernetes have been increasingly adopted to facilitate platform deployment and scaling across distributed infrastructure. The platform architecture must address critical non-functional requirements including scalability to handle millions of concurrent devices, reliability to ensure continuous operation, security to protect against cyber threats, and interoperability to support diverse devices and standards. Research by Mineraud et al. (2016) emphasized that the absence of standardization in IoT platform architectures remains a significant challenge, as proprietary solutions often create vendor lock-in and hinder ecosystem development. The Open Source IoT Platform initiatives have gained traction as alternatives to commercial offerings, providing transparency, community-driven development, and customization flexibility.

2. Commercial IoT Platforms

The commercial IoT platform landscape prior to 2020 was dominated by major technology companies offering comprehensive cloud-based solutions with extensive service portfolios and global infrastructure. Amazon Web Services (AWS) IoT Core emerged as a leading platform, providing managed cloud services for device connectivity, data processing, and integration with AWS's extensive suite of cloud services including Lambda for serverless computing, S3 for storage, and SageMaker for machine learning. AWS IoT Core supports MQTT, HTTP, and WebSocket protocols, offering device shadows for state synchronization and a rules engine for data routing and transformation. Microsoft Azure IoT Suite presented a competitive offering with Azure IoT Hub serving as the central message hub, complemented by Azure Stream Analytics for real-time data processing, Azure Machine Learning for predictive analytics, and integration with Microsoft's enterprise software ecosystem. Azure IoT Edge extended cloud capabilities to edge devices, enabling local processing and offline operation capabilities. Google Cloud IoT Core focused on data analytics and machine learning integration, leveraging Google's expertise in big data processing through BigQuery and machine learning through TensorFlow and Cloud ML Engine. The platform emphasized seamless data pipeline creation from devices to analytics dashboards with minimal configuration overhead. IBM Watson IoT Platform differentiated itself through cognitive computing capabilities, integrating IBM Watson's artificial intelligence services for natural language processing, image recognition, and predictive analytics. The platform provided industry-specific solutions for sectors such as manufacturing, automotive, and insurance, incorporating blockchain technology for supply chain transparency and data integrity. Table 2 compares key features and characteristics of major commercial IoT platforms available before 2020.

Table 2 Comparison of Commercial IoT Platforms

Platform	Key Strengths	Primary Use Cases	Pricing Model	Notable Limitations
AWS IoT Core	Scalability, comprehensive AWS integration, strong security	Industrial IoT, smart home, connected vehicles	Pay-per-message, tiered pricing	Complex pricing structure, learning curve
Microsoft Azure IoT	Enterprise integration, hybrid cloud support, extensive tools	Smart buildings, predictive maintenance	Pay-as-you-go, enterprise agreements	Windows ecosystem bias
Google Cloud IoT	Data analytics excellence, machine learning integration	Retail analytics, environmental monitoring	Usage-based pricing	Smaller IoT-specific feature set
IBM Watson IoT	AI/cognitive capabilities, blockchain integration	Supply chain, asset tracking	Subscription-based, custom enterprise	Higher cost, complex configuration
Oracle IoT Cloud	Enterprise application integration, robust security	Manufacturing, logistics	Subscription-based	Limited developer community
SAP Leonardo IoT	ERP integration, business process automation	Enterprise asset management	License-based	Primarily enterprise-focused

Commercial platforms offered advantages including managed infrastructure, automatic scaling, global availability, comprehensive documentation, and professional support services, making them attractive for enterprises with substantial budgets and requirements for reliability and compliance. However, these platforms also presented challenges such as vendor lock-in, recurring costs that escalate with device volume and data usage, limited customization options, and data sovereignty concerns related to cloud storage locations. A study by Ray (2018) analyzing commercial IoT platforms highlighted that while cloud-based platforms excel in scalability and feature richness, they may not be suitable for applications requiring ultra-low latency, complete data privacy, or operation in environments with limited internet connectivity. The pricing models of commercial platforms typically combine device connection fees, message volume charges, and storage costs, which can become prohibitively expensive for large-scale deployments with millions of devices generating continuous data streams. Organizations must carefully evaluate total cost of ownership over multi-year periods and consider potential migration costs when selecting commercial IoT platforms. The competitive landscape drove continuous innovation, with platform providers regularly introducing new features, reducing prices, and expanding service portfolios to capture market share in the rapidly growing IoT industry.

3. Open Source IoT Platforms and Tools

Open source IoT platforms gained significant traction prior to 2020, offering cost-effective alternatives to commercial solutions with the added benefits of transparency, customizability, and community-driven development. Eclipse IoT projects represented a comprehensive ecosystem of open source tools and frameworks for IoT development, including Eclipse Mosquitto (an MQTT broker), Eclipse Paho (MQTT client libraries), Eclipse Kura (edge computing framework), and Eclipse Hono (messaging infrastructure for IoT). These modular components could be combined to build complete IoT solutions tailored to specific requirements. ThingsBoard emerged as a popular open source IoT platform providing device management, data collection, processing, and visualization capabilities through a unified interface. The platform supported MQTT, CoAP, and HTTP protocols, offered a rule engine for complex event processing, and included customizable dashboards for data visualization. ThingsBoard's architecture allowed deployment on-premises or in cloud environments, providing flexibility for organizations with varying infrastructure preferences and regulatory requirements. Node-RED, developed by IBM and contributed to the OpenJS Foundation, provided a flow-based programming tool for wiring together hardware devices, APIs, and online services. Its visual programming interface enabled rapid prototyping and development of IoT applications without extensive coding, making it accessible to developers with varying skill levels. Node-RED's extensive library of contributed nodes supported integration with numerous IoT devices, protocols, and cloud services. The FIWARE platform, supported by the European Union, offered a comprehensive framework for building smart city and smart industry applications, emphasizing standardized APIs and data models. FIWARE's context broker component, Orion, managed context information lifecycle, supporting NGSI (Next Generation Service Interfaces) for interoperable data exchange. Home Assistant and OpenHAB focused specifically on home automation, providing platforms for integrating diverse smart home devices and creating automation rules. These platforms supported hundreds of device integrations and offered flexible rule engines for customizing home automation logic. Figure 1 illustrates the typical architecture of an open source IoT platform deployment incorporating multiple components for edge and cloud processing.

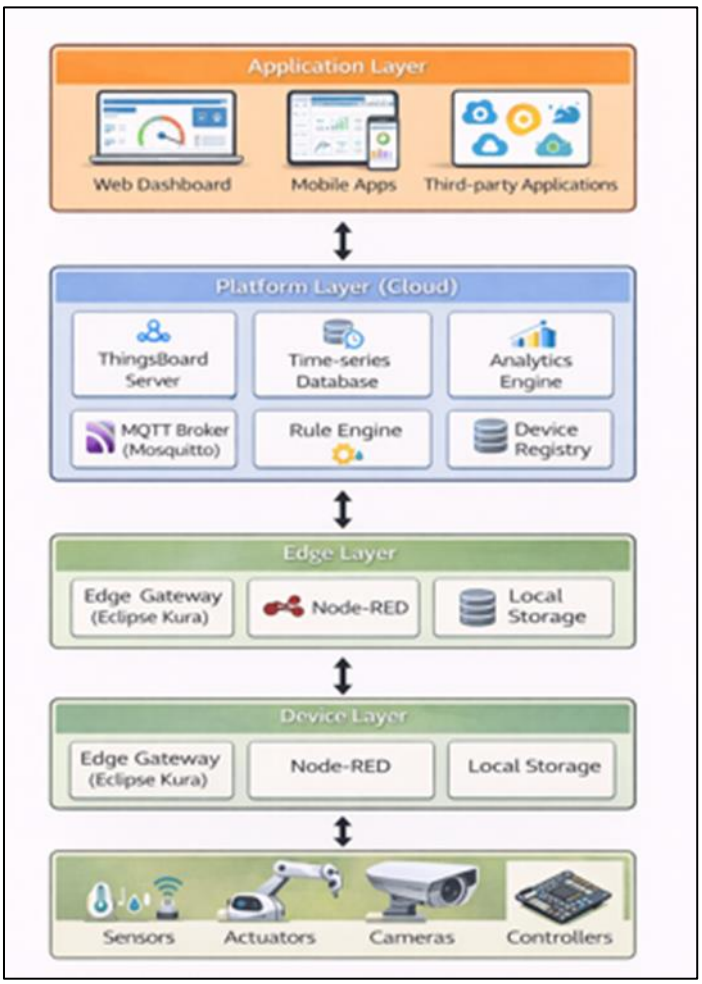

Figure 1 Open Source IoT Platform Architecture

Open source platforms provided distinct advantages including zero licensing costs, complete access to source code enabling customization and security auditing, active community support and contributions, and freedom from vendor lock-in. Organizations could modify platform components to meet specific requirements, integrate proprietary functionality, and maintain complete control over their IoT infrastructure and data. However, open source solutions also presented challenges such as the need for in-house expertise to deploy and maintain platforms, limited or community-based support compared to commercial offerings, potential security vulnerabilities if not properly maintained, and the responsibility for ensuring scalability and reliability. Research by Taivalsaari and Mikkonen (2018) examining IoT platform ecosystems noted that while open source platforms democratized IoT development and fostered innovation, they required organizational commitment to DevOps practices and continuous platform maintenance. The modularity of open source IoT tools allowed organizations to adopt incremental implementation strategies, starting with specific components and expanding functionality over time. Projects like EdgeX Foundry, initiated by the Linux Foundation, aimed to create vendor-neutral open source frameworks for edge computing in IoT, addressing interoperability challenges through standardized APIs and reference implementations. The success of open source IoT platforms demonstrated the viability of community-driven development models in addressing complex technical challenges while maintaining flexibility and cost-effectiveness for diverse use cases ranging from small-scale prototypes to large-scale industrial deployments.

4. Comparative Analysis and Future Directions

The comparative analysis of IoT platforms reveals that no single solution universally addresses all requirements, and platform selection must align with specific project constraints including budget, scalability requirements, technical expertise, security requirements, and integration needs. Commercial platforms excel in scenarios requiring massive scalability, global reach, comprehensive managed services, and integration with existing enterprise software ecosystems. Organizations with substantial budgets, limited in-house technical expertise, and requirements for high availability and professional support typically benefit from commercial platforms. The automatic scaling, managed security updates, and extensive documentation reduce operational overhead and accelerate time-to-market for IoT applications. Conversely, open source platforms suit organizations with strong technical capabilities, requirements for customization, budget constraints, or concerns about vendor lock-in and data sovereignty. The transparency of open source solutions enables security auditing, compliance verification, and optimization for specific use cases that may not be well-served by general-purpose commercial platforms. Hybrid approaches combining commercial and open source components have gained popularity, leveraging commercial platforms for core infrastructure while using open source tools for edge computing, data processing, or specialized functionality. For instance, organizations might use AWS IoT Core for device connectivity and cloud storage while employing Node-RED for edge processing and ThingsBoard for custom dashboards. This approach balances the benefits of managed services with the flexibility of open source components. The evaluation criteria for platform selection should encompass technical factors such as supported protocols, scalability limits, latency requirements, edge computing capabilities, and integration options, as well as business factors including total cost of ownership, vendor stability, licensing models, and exit strategies. Security considerations merit particular attention, as IoT systems often operate in critical infrastructure and handle sensitive data, requiring robust authentication, encryption, data privacy controls, and compliance with regulatory frameworks such as GDPR. Research by Atlam et al. (2018) examining security and privacy in IoT emphasized that platform security architectures significantly impact overall system security posture, with end-to-end security requiring comprehensive measures across device, network, platform, and application layers.

Looking toward future developments in IoT platforms, several trends were emerging by 2020 that would shape the next generation of platforms and tools. Edge computing integration was accelerating, driven by requirements for real-time processing, reduced bandwidth costs, enhanced privacy, and operation in connectivity-constrained environments. Platforms were increasingly incorporating edge intelligence capabilities, enabling sophisticated analytics and machine learning inference at the network edge. The convergence of IoT platforms with artificial intelligence and machine learning technologies was enabling predictive analytics, automated decision-making, and intelligent automation across diverse applications. Platforms were integrating pre-trained models and AutoML capabilities to democratize AI adoption in IoT applications. Blockchain technology was being explored for IoT platforms to address challenges related to device identity management, data integrity, supply chain transparency, and peer-to-peer device interactions without centralized intermediaries. Standardization efforts through organizations such as the Industrial Internet Consortium, OCF (Open Connectivity Foundation), and oneM2M were working to establish common frameworks, protocols, and data models to enhance interoperability across platforms and devices. The containerization and microservices architecture adoption was improving platform modularity, deployment flexibility, and resource efficiency. The emergence of specialized IoT platforms targeting specific verticals such as industrial IoT, smart agriculture, healthcare IoT, and smart cities reflected the maturation of the IoT market and recognition that generic platforms might not optimally address domain-specific requirements. The integration of digital twin technology with IoT platforms was enabling virtual

representations of physical assets for simulation, optimization, and predictive maintenance. As 5G networks began deployment, IoT platforms were preparing to leverage enhanced bandwidth, reduced latency, and support for massive device connectivity that 5G promises. The continued evolution of IoT platforms toward more intelligent, secure, interoperable, and specialized solutions will be essential to realizing the full potential of IoT across industries and applications, driving digital transformation and enabling new business models and services that were previously infeasible.

5. Conclusion

This survey has presented a comprehensive analysis of IoT platforms and tools available prior to 2020, examining the diverse ecosystem of solutions that enable the development, deployment, and management of Internet of Things applications. The investigation of IoT platform architectures revealed the complex layered approach required to bridge physical devices with software applications, incorporating essential components for device management, data processing, security, communication, and analytics. The comparative analysis of commercial platforms demonstrated that major technology companies including Amazon, Microsoft, Google, and IBM have developed sophisticated, feature-rich platforms optimized for scalability, reliability, and integration with enterprise ecosystems. These commercial offerings provide managed infrastructure that reduces operational complexity and accelerates deployment timelines, making them particularly attractive for organizations with substantial budgets and requirements for professional support and global availability. However, the survey also highlighted significant considerations including recurring costs that scale with device volume and data usage, potential vendor lock-in concerns, and limitations in customization capabilities that may constrain specialized implementations.

The examination of open source IoT platforms revealed a vibrant ecosystem of community-driven projects that offer compelling alternatives to commercial solutions, particularly for organizations with strong technical capabilities and requirements for customization, transparency, and cost control. Platforms such as Eclipse IoT, ThingsBoard, Node-RED, and FIWARE provide modular, extensible frameworks that can be tailored to specific use cases while maintaining complete control over infrastructure and data. The open source approach fosters innovation through community contributions, enables security auditing and compliance verification, and eliminates vendor dependencies that could constrain long-term strategic flexibility. However, successful adoption of open source platforms requires organizational commitment to platform maintenance, security updates, and continuous optimization, along with in-house expertise to manage deployment and operations effectively. The survey identified that hybrid approaches combining commercial and open source components represent an increasingly popular strategy, allowing organizations to leverage the strengths of both models while mitigating their respective limitations.

The analysis of platform selection criteria emphasized that no universal solution exists for all IoT applications, and successful implementations require careful alignment of platform capabilities with specific project requirements. Technical considerations including supported protocols, scalability limits, latency requirements, edge computing capabilities, and integration options must be balanced against business factors such as total cost of ownership, licensing models, vendor stability, and regulatory compliance requirements. Security emerged as a critical concern requiring comprehensive attention across all layers of the IoT stack, from device authentication and data encryption to access control and privacy protection. The survey highlighted that platform security architectures significantly influence overall system security posture, necessitating thorough evaluation of security features and compliance certifications during platform selection. The emergence of specialized vertical platforms targeting specific industries reflects the maturation of the IoT market and recognition that domain-specific requirements may not be optimally addressed by generic horizontal platforms.

Looking toward future developments, several transformative trends were identified that will shape the next generation of IoT platforms and tools. The integration of edge computing capabilities addresses critical requirements for real-time processing, bandwidth optimization, enhanced privacy, and operation in connectivity-constrained environments, enabling more distributed and resilient IoT architectures. The convergence of artificial intelligence and machine learning with IoT platforms promises to unlock new capabilities in predictive analytics, automated decision-making, and intelligent automation across diverse applications. Blockchain technology presents opportunities to address persistent challenges in device identity management, data integrity, and decentralized trust mechanisms. Standardization efforts by industry consortia working to establish common frameworks, protocols, and data models will be essential to achieving true interoperability and reducing fragmentation in the IoT ecosystem. The adoption of containerization and microservices architectures improves platform modularity and deployment flexibility, while the emergence of 5G networks promises to enable new classes of IoT applications requiring ultra-low latency and massive device connectivity.

In conclusion, the IoT platform landscape prior to 2020 represented a diverse and rapidly evolving ecosystem offering multiple viable approaches to IoT implementation. The coexistence of commercial and open source platforms provides organizations with options suited to different requirements, budgets, and technical capabilities. Successful IoT implementations depend not only on selecting appropriate platforms and tools but also on understanding the architectural principles, security requirements, and integration challenges inherent in IoT systems. As IoT technology continues to mature and penetrate new domains, platforms must evolve to address emerging requirements for intelligence, security, interoperability, and sustainability. The insights presented in this survey provide a foundation for understanding the current state of IoT platforms and inform strategic decisions regarding platform selection, architecture design, and implementation approaches. Future research should continue to monitor platform evolution, evaluate emerging technologies such as edge AI and blockchain integration, and develop frameworks for assessing platform suitability for specific application domains. The continued advancement of IoT platforms will be instrumental in realizing the transformative potential of IoT across industries, enabling innovations that improve efficiency, sustainability, and quality of life in an increasingly connected world.

References

[1] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Internet of Things: State-of-the-art, challenges, applications, and open issues. International Journal of Intelligent Computing Research, 9(3), 928-938.

[2] Gartner. (2017). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Gartner Press Release.

[3] Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. Computer Communications, 89, 5-16.

[4] Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.

[5] Taivalsaari, A., & Mikkonen, T. (2018). A roadmap to the programmable world: Software challenges in the IoT era. IEEE Software, 35(3), 53-58.