A Systematic Review of IoT Middleware Frameworks: Investigating Architecture, Implementation, and Performance

Mahendra Kumar Verma[1*], Nirmal Dagdee[2] and Preeti Saxena[3]

[1,2,3] School of Computer Science & Information Technology, DAVV, Indore, MP, India
[*]mahendraverma2610@gmail.com, [2]nirmal_dagdee@rediffmail.com,
[3]preeti_ms@rediffmail.com

Abstract. As the Internet of Things (IoT) environment keeps growing, there is a rising demand for middleware solution that can help in connecting devices in a way that is both efficient and reliable. Due to the diverse nature and capabilities of IoT devices and their usage in complex data exchange, middleware framework is a key aspect of the IoT. Also middleware functionalities and services are highly required by a variety of IoT applications. Across the existing literature, very few authors have discussed about underlying architecture of IoT middleware, the challenges of implementing them, and how well they perform according to their application requirements. This review paper aims to investigate the architecture, implementation, and performance of existing IoT middleware frameworks, emphasizing on their suitability across diverse application domains. This review can be helpful for the researchers to identify how IoT middleware framework can be improved and in selecting the most suitable Framework according to different application domains for developers of different varieties of IoT applications.

Keywords: IoT, Middleware, Framework, Architecture, Implementation, Performance.

1 Introduction to Internet of Things (IoT)

The Internet of Things (IoT) have changed everything including how we interact with the world around us over the time [1]. Internet of Things (IoT) is a network of physical objects or things connected to the internet [4]. The Internet of Things is connecting everyday things to the internet and enabling them to do tasks together. For example smart phones, smart watches, smart refrigerator and smart television etc. Each these machines were designed to talk to each other via the internet, which was supposed to make our lives a little easier.

IoT consists of a network connecting physical objects, or "things" to the internet [2]. It is connecting everyday objects to the network so they can share information and work together. These types of devices are capable to communicate with each other and many others over the internet. This technology has become widely adopted in industries as it renders physical devices, sensors, actuators and software applications

S. Bhalerao et al. (eds.), *Proceedings of the International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2025),* Advances in Intelligent Systems Research 192,
https://doi.org/10.2991/978-94-6463-716-8_50

interconnected thus enabling these things to gather process which helps decision making automate simple tasks [7].

The structure of this research document is described as:

-Section 1 provides an overview of Internet of Things (IoT) and their significance in the IoT ecosystem.

-Section 2 gives an overview of the existing work related to IoT middleware frame Works.

-Section 3 provides research objectives to be incorporated in this paper.

-Section 4 covers importance of IoT middleware frameworks and detailed comparison of existing IoT Middleware Frameworks based on architecture, implementation and performance.

-Section 5 examines the suitability of different IoT Middleware Framework for vari ous application domains.

-Section 6 discusses criteria for selecting an appropriate IoT Middleware Framework
-Finally, Section 7 concludes the paper with key findings for future directions for research.

2 Literature Review

In this section, we will discuss about some studies carried out about IoT middleware frameworks.

Kushwah, R. et al. (2020) [1], provided a comprehensive overview of the architectural components of IoT. They have discusses the significant challenges faced in its implementation, and also suggested future research directions for enhancing the effectiveness and security of IoT systems. They have divided the IoT challenges into four categories (aspect related to networking and gateway, aspects related to architecture, addressing and mobility of object, aspects related to traffic characterization issues and security and aspects related to management of huge number of devices and huge amount of data). Goumopoulos, C. et al. (2024) [2], explored current middleware solutions and proposes a framework that specifies functional and non-functional requirements i.e. scalability, data privacy, and real-time processing capabilities etc. They have also identified some challenges in using middleware for smart city applications and suggested a conceptual framework for smart city middleware to fulfill challenges and requirements identified in existing middleware solutions.

Venanzi, R. et al. (2021) [3], introduced a middleware designed to emphasis on interoperability and integration challenges in Industrial Internet of Things (IIoT)

middleware framework. The highlighted the requirement of middleware solution that can connect different IIoT platforms to seamless functionality across industrial ecosystem. Agrawal, P. et al. (2020) [4], compared IoT middleware platforms for various applications. They examined their features according to the general IoT architecture. This research work can help further developers in choosing the right platform according to their requirement based on the application to be developed. Bellini, P. et al. (2022) [5], discussed key technologies of IoT middleware and their benefits for improving urban life through its applications in transportation, energy, and healthcare in Smart City. Idoko, P. et al. (2024) [6], analyzed IoT implementation strategies in Ghana and the USA. They have performed comparative analysis of architecture, and infrastructure.

Mauro A.A. et al. (2021) [7], addressed key challenges in existing IoT middleware, such as complex device integration, insufficient security for protocols like MQTT, and performance issues due to frequent database access. They proposed a secure and scalable middleware solution for IoT applications named as In.IoT that focuses on response times, error rates, and packet sizes.

Toutsop, O. et al. (2021) [8], explored challenges such as interoperability, scalability, and available security vulnerabilities that can affect the integration of new devices against potential threats. They suggested future middleware that can incorporate machine learning for predictive analytics and robust security protocols, against potential threats.

These research studies have discussed only about the parameters that give general overview of different IoT middleware. The authors of these research articles have not compare the features of IoT middleware based on architecture, implementation and performance. Our investigation compares various IoT middlewares based on architecture, implementation and performance.

3. Research Objectives

We are comparing the existing IoT middleware frameworks based on their architecture, implementation and performance features. Selecting the right IoT middleware framework is a very challenging task. It is very much important for development of scalable, secure, and interoperable IoT applications according to the need. In this review paper, we are focusing on the research objectives as given below:

-To explore the architecture, implementation and performance of existing IoT Frameworks.

-To analyze suitability of different IoT middleware frameworks for various appli cation domain.

Our work carried out in this review article can be helpful for selecting suitable IoT middleware framework for a particular application domain.

4. IoT Middleware Framework

IoT provides effective communication between the interconnected devices and make it possible to have the data exchange between various IoT applications [3]. The number of IoT devices continuously increasing, therefore the need for effective and efficient communication between these devices is fulfilled by IoT middleware [5]. IoT middleware is basically software which is available in the form of a framework that is specially designed to provide interaction among the IoT devices, data management, data storage, and data processing required to build smart application [4][8]. It is something that can play a role of bridge between the smart devices of IoT ecosystem and the IoT applications [17].

4.1 Importance of IoT Middleware Framework

Middleware frameworks play a key role in IoT environments by acting as a communication bridge between a variety of IoT devices, networks, and applications. Middleware is something which is available in between the IoT devices and IoT applications. The responsibility of IoT middleware is to avail effective data exchange between a wide variety of IoT devices and underlying IoT applications [6].

IoT middleware frameworks provide the following significant functions:

-Communication: The IoT middleware ensures efficient and reliable data communication between the IoT devices and underlying IoT applications, focusing on underlying hardware and communication protocols which are the key need of IoT ecosystem [9].

-Data management: Middleware frameworks facilitate cross-layer communications and flexible management of data. It provides efficient acquisition of data, its pre-processing and storage over the cloud. It integrates data from different platforms and also supports real-time data analytics [11].

-Security: Security is crucial for the IoT ecosystem as unsecure devices increase vulnerabilities. Many IoT subsystems face security breaches, unauthorized access, and data breaches [15]. Real-time middleware frameworks offer encryption and authentication and provide secure cloud for security.
-Interoperability: Device heterogeneity is considered one of the major challenges within IoT and another challenge is the fact that different groups of devices might use different communication standards [28]. Interoperability refers to the capacity that enables middleware to work as a link between different systems and organizations that could possibly use different formats and technologies [13]. Middleware has to be interoperable with different systems if it wants to work properly within the IoT ecosystem.

4.2 Layered Architecture of IoT Middleware

The IoT is a multilayer architecture, divided into the four layers as given in fig. 1. All layers are discussed with their components and functions.

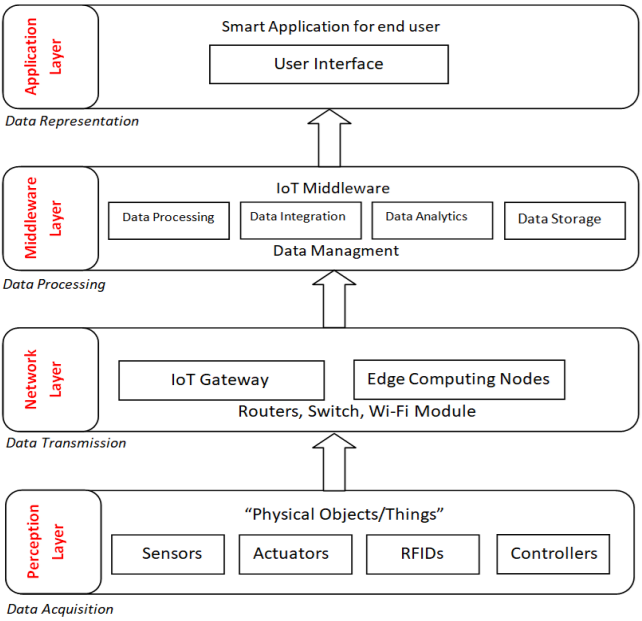

Fig. 1: Layered Architecture of IoT

a. Perception Layer

It serves as the "sensing" layer, responsible for detecting, collecting, and data acquisition from the physical environment through various sensors and smart devices of IoT environment. This layer basically prepares real-world data for the use across the IoT ecosystem [14].

Components at Perception Layer

Main components at Perception Layer are sensors, actuators, RFIDs, Controllers etc. Sensors are responsible to detect some changes in the environment of IoT and convert this information into signals that can be read and processed by other devices or systems in the IoT ecosystem [27]. Sensor can measure the physical properties or For example: light sensors, temperature sensors, pressure sensors, humidity sensors, and motion sensors etc. Actuators can receive commands and perform physical actions or movements in response to these commands e.g. motor, valves, relay, heating elements etc [10].

Functions of Perception Layer

Data collection and initial processing are the important functions of the Perception Layer. It helps IoT devices in sensing their surroundings and taking actions based on based on environmental changes.

b. Network Layer

The layer above Perception Layer is the network layer. This layer performs the initial processing of data and its transmission from perception layer to the next layer i.e. middleware layer of the IoT.

Components at Network Layer

Communication Protocols, Gateway, Routers and Edge computing nodes are main components of Network Layer of IoT middleware. The role of an IoT Gateway is to act as a bridge between IoT devices (like sensors and actuators) and the cloud. Edge devices are computing units located at the network's edge [26].

Functions of Network Layer

Data transmission, routing and forwarding of data and connection management are the main functions of the Network Layer of IoT.

c. Middleware Layer

This layer provides the abstraction for the things in IoT. Middleware layer sits in between the hardware (sensors, actuators, devices) and the application layer (software and user interfaces). It receives information from the Network Layer and performs further information processing. It analyzes how to fetch the data whenever required to complete the desired task, and also supports the storage of data through cloud [12].

Components at Middleware Layer

Data Management System, Real Time Data Processing Tools, API Management i.e. Interface for communication between IoT devices and IoT applications are the main components of IoT middleware Layer.

Functions of Middleware Layer

Device management, Data Processing and Storage, Interoperability and Security are the important functions of the middleware layer of IoT.

d. Application Layer

Application layer implements the working of IoT with the help of an application with corresponding device. It provides the services as per the user demand. Developers

create the specific application at the application layer using frameworks, and development tools [24].

Components at Application Layer

User interface and business applications are main components of IoT Application Layer.

Functions of Application Layer

Data Visualization, Decision Making and Control and Specific Service Delivery are the important functions of the Application Layer of IoT Ecosystem [16].

4.3 Comparison of existing IoT Middleware Frameworks

Investigating architecture, implementation, and performance are important key aspects to review different IoT middleware frameworks. In this paper, we are comparing existing IoT middleware frameworks based on their architecture, implementation and performance.

-Architecture: examining the underlying design principles, components, and interactions within the middleware frameworks.

-Implementation: assessing how these frameworks are built, deployed, and integrated within IoT ecosystems.

-Performance: evaluating the efficiency, scalability, reliability, and other performance metrics of the middleware frameworks under various conditions and workloads

Some popular IoT middleware frameworks includes Microsoft Azure IoT Hub [29], AWS IoT [30], Google Cloud IoT [31], IBM Watson IoT Platform [32], Oracle IoT [33], ThingSpeak [34], Particle Cloud [35], Kaa IoT Platform [36], Cisco IoT Cloud Connect [37] and ThingWorx IIoT Platform [38]. Table 1 provides the description and key features of some popular IoT middleware frameworks:

Table 1: Key features of some popular IoT Middleware Framework

IoT Middleware Framework	Device Management	Data Analytics	Security Features	Open Source	Cloud Integration	Real-Time Processing	Interoperability
Microsoft Azure IoT Hub	Yes	Yes	Yes	No	Yes	Yes	Yes
AWS IoT Core	Yes	Yes	Yes	No	Yes	Yes	Yes
Google Cloud IoT	Yes	Yes	Yes	No	Yes	Yes	Yes
IBM Watson IoT Platform	Yes	Yes	Yes	No	Yes	Yes	Yes

Oracle IoT	Yes	Yes	Yes	No	Yes	Yes	Limited
ThingSpeak	Limited	Yes	Limited	Yes	Yes	Limited	Yes
Particle Cloud	Yes	Yes	Yes	No	Yes	Yes	Yes
Kaa IoT Platform	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IoT Cloud Connect	Yes	Yes	Yes	No	Yes	Yes	Yes
ThingWorx IIoT Platform	Yes	Yes	Yes	No	Yes	Yes	Yes

a. Architecture

The architectural characteristics of IoT middleware frameworks are important elements that define the structure and overall design of the IoT middleware framework [23]. These characteristics ensure the efficient and effective operation of IoT systems. The right architectural design ensures that the IoT middleware can meet diverse application needs, provide robust performance, and support the seamless operation of IoT systems [17]. Key architectural characteristics of IoT middleware framework include:

-Architectural Characteristics

The architectural characteristics of IoT middleware specify how the middleware structured and organized focusing on adaptability, modularity, and overall layout. These characteristics define how IoT middleware manages data communication, data processing, and data storage over the cloud [24].

-Edge Computing Mechanism:

IoT middleware support the edge computing to process, analyze, manage and store the IoT data near to its source. This is basically the location available at the edge device itself or the edge of the network. With the edge computing, latency can be minimized and network's bandwidth consumption can be reduced [18].

-Device Management

Device Management is the efficient supervision (i.e. control, monitoring, and maintenance) for achieving secure and effective functioning of smart IoT devices with the help of smart tools and services of IoT middleware [21].

-Data Processing

Data Processing within an IoT environment is to assess, control, and monitor data collected from various IoT devices. Data involves data acquisition, data filtering, and processing of data in real time, as well as analyzing it for further decision-making task.

-Scalable

IoT devices are continuously increasing. IoT middleware should be scalable (i.e. expand and adapt) so that it can accommodate increasing numbers of devices, users, and data, without compromising the performance. With the scalability feature, IoT middleware can support larger IoT deployments as per the requirements according to the particular application [22]. The architectural characteristics of different IoT middleware frameworks are compared in table 2:

Table 2: Architectural Characteristics of different IoT Middleware Frameworks

IoT Middleware Framework	Architecture	Edge Computing	Device Management	Data Processing	Scalability
Microsoft Azure IoT Hub	Cloud and Edge	Yes (Azure IoT Edge)	Yes	Yes	Yes
AWS IoT Core	Cloud and Edge	Yes (AWS Greengrass)	Yes	Yes	Yes
Google Cloud IoT	Cloud and Edge	Yes (Cloud IoT Edge)	Yes	Yes	Yes
IBM Watson IoT	Cloud and Edge	Limited (Edge with IBM Edge Application Manager)	Yes	Yes	Yes
Oracle IoT	Cloud	No	Yes	Yes	Yes
ThingSpeak	Cloud	No	Limited	Yes	Limited
Particle Cloud	Cloud and Edge	Yes (Particle Edge)	Yes	Yes	Yes
Kaa IoT Platform	Cloud and Edge	Yes (Customizable)	Yes	Yes	Yes
Cisco IoT Cloud	Cloud	Limited	Yes	Yes	Yes
ThingWorx IIoT	Cloud and Edge	Yes (Edge MicroServer)	Yes	Yes	Yes

b. Implementation

The implementation characteristics of IoT platforms include ease of deployment, development tools, integration complexity, customization, vendor lock-in and cost of implementation. Each characteristic is described as follows:

-Ease of Deployment

While deploying an IoT middleware framework, it should be simple to configure. The ease of deployment of middleware depends on appropriate documentation, availabili ty of pre-configured setups, automated deployment tools, and user-friendly interfaces. These can help in reducing the deployment complexity and the time required to start the IoT middleware for a particular application [11].

-Development Tools

Efficient development of middleware required some important development tools for example Software Development Kits, Integrated Development Environments, Application Programming Interfaces and some kind of simulation and debugging tools for IoT [23].

-Integration Complexity

IoT application developers can experience the difficulty of connecting the IoT middleware framework with other devices, systems, or services. These difficulties may arise due to compatibility requirements of middleware with different software and hardware platforms, support of more than one communication protocols needed, and integrating existing systems into the new middleware framework easily [19].

-Customization

Sometimes IoT middleware framework is required to be change add, or organize according to system's capabilities, interfaces, and user requirements to accomplish technical required of a particular IoT application. IoT middleware should support such customization.

-Vendor Lock-In

When we rely on single vendor of IoT middleware, for products and services, it is difficult to go with the different vendors. This is because of the data formats or pro gramming interfaces of applications which cannot be compatible with some different system. This restriction is of using specific middleware is considered as vendor lock-in.

-Cost of Implementation

Cost of implementation of IoT middleware includes the costs to establish and cost to maintain a particular middleware. There are so many costs associated with it for example licensing fees at initial level, expenses related with subscriptions, expenses related with hardware and infrastructure, cost associated with development and customization, and expensed on training, and support. Table 3 provides the Implementation Characteristics of different IoT middleware frameworks:

Table 3: Implementation Characteristics of different IoT Middleware Frameworks

Platform	Ease of Deployment	Comprehensive Development Tools	Low Integration Complexity	High Customization	Vendor Lock-In	Low Cost of Implementation
Microsoft Azure IoT Hub	No	Yes	No	Yes	Yes	No
AWS IoT Core	Yes	Yes	Yes	Yes	Yes	No
Google Cloud IoT	No	Yes	No	Yes	Yes	No
IBM Watson IoT	No	Yes	No	Yes	Yes	No
Oracle IoT	No	Yes	No	No	Yes	No
ThingSpeak	Yes	No	Yes	No	No	Yes

Particle Cloud	Yes	Yes	Yes	Yes	No	Yes
Kaa IoT Platform	No	Yes	Yes	Yes	No	Yes
Cisco IoT Cloud	No	Yes	No	No	Yes	No
ThingWorx IIoT	No	Yes	No	Yes	Yes	No

c. Performance

The performance aspects of IoT middleware frameworks are important for ensuring efficient and effective operation of IoT systems. Key performance aspects include latency, throughput, reliability, data processing speed, real time capabilities, edge computing performance, data ingestion rate and bandwidth utilization. These aspects significantly impact the overall functionality and responsiveness of the IoT platform. Each performance characteristic is described as follows:

-Latency

Latency refers to the time delay that is taken into the consideration between the point of time when data is generated by an IoT device in the IoT environment and the moment when these data is being processed by the IoT middleware. Real-time communication systems, such as industrial automation require low latency. High latency can lead to performance issues and can fail to meet user requirements and can affect the quality of content.

-Throughput

Throughput refers to data processing capacity of IoT middleware. As the IoT middleware handles large volumes of data volumes, it requires high throughput to manage data traffic. Overall system throughput is important for understanding component interaction.

-Reliability

Reliability is a crucial performance metric in evaluating middleware performance and signifies how consistent a system can operate. The term itself is defined as the ability of a system to perform its intended function under specified conditions for a specified period [7]. IoT middleware should function correctly despite various environmental changes, connectivity issues in the network and some challenges faced during data transmission.

-Data Processing Speed

Data Processing Speed is an important performance metric of an IoT middleware. It is the rate at which the IoT middleware can process incoming data from various smart devices connected in IoT environment. High data processing speed is an important issue for handling large volumes of data with required efficiently [14].

-Real-Time Capabilities

The ability of an IoT middleware framework to process and respond to data and events in real-time that can enable instant action. Real-time capabilities are essential for applications that require immediate action, such as automated control systems, precise and real time monitoring etc. real-time processing can improve IoT middleware performance with great extent [4]. Therefore, IoT middleware should capable to process in real-time to enable instant decision-making.

-Edge Computing Performance

Edge computing is an important performance metrics that measures the efficiency and performance of processing data locally on edge devices itself or nearby nodes in the IoT ecosystem. IoT middleware can reduce latency, minimize bandwidth usage, and accelerate response times with edge computing. Edge computing is an essential consideration for time-sensitive applications requiring instant results [7].

-Data Ingestion Rate

For an IoT middleware, data ingestion rate is the rate at which data is gathered from various sources and injected into the middleware for further processing. A high data ingestion rate of IoT middleware can ensures that it can handle large volumes data which is coming from different smart devices of IoT without any delay. It makes possible to have timely processing of data and its analysis [4][21].

-Bandwidth Utilization

An IoT environment is consist of different smart devices, nodes available at the edge and centralized system. IoT middleware is responsible to communicate between these components of the IoT ecosystem. These communications may consume some amount of network bandwidth. This is considered as Bandwidth Utilization [11]. Efficient bandwidth utilization by IoT middleware can reduce network congestion, minimizes costs, and can enable seamless communication within the environment which can have limited network capabilities. Table 4 highlights the performance aspects of different IoT middleware frameworks:

Table 4: Performance Characteristics of different IoT Middleware Frameworks

Platform	Low Latency	High Through-put	High Reliability	Fast Data Processing	Real-Time Capabilities	Strong Edge Computing	High Data Ingestion Rate	Efficient Bandwidth Utilization
Microsoft Azure IoT Hub	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS IoT Core	Yes	Yes	Yes	Yes	Yes	Yes (Greengrass)	Yes	Yes

Google Cloud IoT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IBM Watson IoT	Yes	Yes	Yes	Yes	Yes	Limited	Yes	Yes
Oracle IoT	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
ThingSpeak	No	No	No	No	No	No	No	No
Particle Cloud	Moderate	Moderate	Yes	Moderate	Moderate	Yes	Moderate	Yes
Kaa IoT Platform	Moderate	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IoT Cloud	Yes	Yes	Yes	Yes	Yes	Limited	Yes	Yes
ThingWorx IIoT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5 Suitability of different IoT Middleware Framework for various application domains

Different IoT middleware frameworks are designed with specific features and characteristics that make them suitable for various application domains. The table 5 provides the suitability of different IoT middleware frameworks with their application domain and examples.

Table 5: Suitability of different IoT Middleware Frameworks

IoT Middleware Framework	Application Domain	Example	Suitability Reasoning
Microsoft Azure IoT Hub	Healthcare	Remote patient monitoring	Support Secure data connectivity and real time monitoring.
AWS IoT	Agriculture	Soil moisture monitoring in farms	Provide tools for remote monitoring and support Scalable data collection, data analytics and automation.
Google Cloud IoT	Energy Management	Optimizing energy usage in buildings	Robust infrastructure and optimization of energy consumption and distribution systems.
IBM Watson IoT Platform	Manufacturing	Optimizing manufacturing processes	Provide improved efficiency, minimized failure time and enhanced quality of product with automation.
Oracle IoT	Smart Grid	Smart grid monitoring	Efficiently manages and analyzes data from smart grid devices, enabling utilities to improve grid performance and resource management.
ThingSpeak	Environmental Monitoring	Air quality monitoring in urban areas	Helps to gather data from IoT sensors, making it easy to track factors like temperature, humidity, and air quality. Provide Visualization and analytics for environmental data

Particle Cloud	Wearable Devices	Fitness tracker development	Provides a platform for connecting, managing, and securing wearable devices, simplifying development and deployment.
Kaa IoT Platform	Agriculture	Greenhouse monitoring	Offers features for collecting data from sensors in fields, monitoring crop conditions, and optimizing irrigation and fertilization processes helping farmers make informed decisions to improve crop yield and efficiency.
Cisco IoT Cloud Connect	Smart Cities	Street lighting management	Offers a platform for managing sensing devices and facilitating data acquisition and its analysis for better city management.
ThingWorx IIoT Platform	Industrial Automation	Predictive maintenance	Helps to monitor, control, and optimize industrial processes, reducing downtime and improving productivity. Supports Real-time data analysis for predictive maintenance

6 Criteria for selecting an appropriate IoT Middleware Framework

Each IoT middleware framework offers different features and different services. Selecting the appropriate one according to the application will depend on some specific criteria. You can select the right IoT middleware platform that meets your requirements and enables the development of scalable, secure, and interoperable IoT applications. We have discussed some key criteria to consider:

-Scalability

Scalability is an important parameter for application requirement. An efficient IoT middleware framework should effectively handle the increasing number of IoT devices and data volumes without performance degradation.

-Availability

Availability of IoT middleware ensures its ability to be accessible whenever required and operational as per the need. Availability of IoT middleware should be high to ensure its reliability and continuous service without any failure. For example, Smart healthcare application usually available all the time to monitor patient medical data continuously (24*7), whereas, if we take the example of smart industry, its timing restricted is limited for few hours only.

-Interoperability

The IoT middleware should support a wide range of heterogeneous smart devices and should support communication protocols like HTTP, MQTT, CoAP etc. It should also provide seamless integration with different IoT devices of IoT ecosystem.

-Security

The IoT middleware should be secure enough. It should support secure data transmission, data encryption, authentication mechanism and access control to provide protection for sensitive data and IoT devices against unauthorized access and a variety of security threats.

-Reliability

The IoT middleware should be highly reliable. It should include fault tolerance mechanisms to ensure uninterrupted functionalities of IoT applications.

-Flexibility

The IoT middleware should be flexible enough so that it can support customization in terms of data processing, data storage, and communication protocols as per the application requirements.

-Data Management and Analytics

The IoT middleware should have data management capabilities such as data collection, data processing, data analysis and data storage. It should support real-time data processing and data analytics at advance level to achieve desirable insights from data generated with IoT environment.

-Performance

The IoT middleware should deliver high performance and low latency so that we can achieve real-time data processing and fast response.

-Ease of Integration

The IoT middleware framework should be user friendly in terms of integration with available system, applications and components of infrastructure. It should provide seamless integration tools, APIs, SDKs, and other software and hardware components of IoT ecosystem along with well documentation.

-Vendor Support

The vendors of IoT middleware should have a fair track record in delivering reliable and high-quality IoT solutions. It should support responsive customer support. The vendor must have a good history of successful implementations and positive feedback of customers.

7 Conclusion

In this paper, we have discussed the architecture, implementation and performance features of some popular IoT middleware frameworks. This thorough investigation of

existing IoT middleware frameworks aims to contribute to the advancement of IoT technology and its widespread adoption across industries by offering useful insights and guidance for comparing different IoT middleware frameworks. At the last we have discussed the criteria for selecting the appropriate IoT middleware framework for application developers for design, development, and deployment of a particular IoT application. Overall, such a systematic review would likely contribute to the understanding of the current landscape of IoT middleware frameworks, identify trends, gaps, and best practices, and provide insights for researchers, developers, and practitioners in the IoT domain.

References

1. Kushwah, R., Batra, P.K., Jain, A.: Internet of things architectural elements, challenges and future directions. In: Proceedings of the 2020 6th International Conference on Signal Processing and Communication (ICSC), pp. 1–5. IEEE (2020).
2. Goumopoulos, C.: Smart city middleware: A survey and a conceptual framework. IEEE Access 12, 4015–4047 (2024).
3. Venanzi, R., Cavalucci, A., Foschini, L., Bellavista, P.: MIINT: Middleware for IIoT platforms integration. In: 2021 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2021).
4. Agarwal, P., Alam, M.: Investigating IoT middleware platforms for smart application development. In: Smart Cities—Opportunities and Challenges, pp. 231–244. Springer (2020).
5. Bellini, P., Nesi, P., Pantaleo, G.: IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Applied Sciences 8(12), 2663 (2018).
6. Idoko, I.P., Ijiga, O.M., Agbo, D.O., Abutu, E.P., Ezebuka, C.I., Umama, E.E.: Comparative analysis of Internet of Things (IoT) implementation: A case study of Ghana and the USA - vision, architectural elements, and future directions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology 5(1), 245–256 (2020).
7. Cruz, M.A.A., Rodrigues, J.J.P.C., Lorenz, P., Korotaev, V.V., de Albuquerque, V.H.C.: In.IoT—A new middleware for Internet of Things. IEEE Internet of Things Journal 8(10), 8116–8131 (2021).
8. Deohate, A., Rojatkar, D.: Middleware challenges and platform for IoT—A survey. In: 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1–6. IEEE (2021).
9. Toutsop, O., Kornegay, K., Smith, E.: A comparative analyses of current IoT middleware platforms. In: 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 1–7. IEEE (2021).
10. Wasswa, S., Matinkhah, S.M., Asadi, M., Ahmadi, Z., Hadiyan, Z.: A study on Internet of Things performance evaluation. Journal of Communications Technology, Electronics and Computer Science 28 (2020).
11. Mesmoudi, Y., Lamnaour, M., El Khamlichi, Y., Tahiri, A., Touhafi, A., Braeken, A.: A middleware based on service-oriented architecture for heterogeneity issues within the Internet of Things. Journal of King Saud University – Computer and Information Sciences (2020).
12. Thenmozhi, S., Bala Ranjitha, J., Anu, S., Jasmine Soniya, A.: Light weight security framework for IoT. In: International Conference on Advanced Computing & Communication Systems (ICACCS), 15-16 March 2019.

13. Thapliyal, S., Gupta, H., Khatri, S.K.: An innovative model for the enhancement of IoT device using lightweight cryptography. In: Amity International Conference on Artificial Intelligence (AICAI), 4-6 February 2019.
14. Li, C., Palanisamy, B.: Privacy in Internet of Things: From principles to technologies. IEEE Internet of Things Journal 6(1) (2019).
15. Goyal, K.K., Garg, A., Rastogi, A., Singhal, S.: A literature survey on Internet of Things (IoT). International Journal of Advanced Networking and Applications 9(6), 3663–3668 (2018).
16. da Cruz, M.A.A., Rodrigues, J.J.P.C., Al-Muhtadi, J., de Albuquerque, V.H.C.: A reference model for Internet of Things middleware. IEEE Internet of Things Journal 5(2) (2018).
17. Ansari, A.M., Hussain, M.: Middleware based node authentication framework for IoT networks. In: Proceedings of IEEE ICIRCA (2018).
18. Ammar, M., Russello, G., Crispo, B.: Internet of Things: A survey on the security of IoT frameworks. Elsevier Journal of Information Security and Applications (2018).
19. Sandescu, C., Grigorescu, O., Rughinis, R., Deaconescu, R., Calin, M.: Why IoT security is failing: The need for a test-driven security approach. In: RoEduNet Conference: Networking in Education and Research, 6-8 September 2018.
20. Prathibha, L., Fatima, K.: Exploring security and authentication issues in Internet of Things. In: International Conference on Intelligent Computing and Control Systems (ICICCS), 14-15 June 2018.
21. Assiri, A., Almagwashi, H.: IoT security and privacy issues. In: International Conference on Computer Applications & Information Security (ICCAIS), 4-6 April 2018.
22. Lomotey, R.K., Pry, J., Sriramoju, S., Deters, R.: Middleware framework for IoT services integration. International Journal of AI & Mobile Services (2017).
23. Hagag, A., Imam, M., Azer, M.A.: Internet of Things security framework. In: International Computer Engineering Conference (ICENCO), 27-28 December 2017.
24. Chow, R.: The last mile for IoT privacy. IEEE Security & Privacy Journal 15(6), 73–76 (2017).
25. Naru, E.R., Saini, H., Rathee, G.: Proposed IoT framework using third party with enhanced security. In: International Conference on Signal Processing, Computing and Control (ISPCC), 21-23 September 2017.
26. Josyula, S.K., Gupta, D.: A new security methodology for Internet of Things. In: International Conference on Computing, Communication and Automation (ICCCA), 5-6 May 2017.
27. Challa, S., Wazid, M., Das, A.K., Kumar, N.: Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Journal 5 (2017).
28. Sridhar, S., Smys, S.: Intelligent security framework for IoT devices: Cryptography-based end-to-end security architecture. In: International Conference on Inventive Systems and Control (ICISC-2017), 19-20 January 2017.
29. Azure.microsoft.com. (2019). IoT Hub | Microsoft Azure. [online] Available at: https://azure.microsoft.com/en-in/services/iot-hub/ [Accessed 24 September, 2024].
30. Amazon Web Services, Inc. (2019). IoT Applications & Solutions | What is the Internet of Things (IoT)? | AWS. [online] Available at: https://aws.amazon.com/iot/ [Accessed 24 September, 2024].
31. Google Cloud. (2019). Google Cloud IoT - Fully managed IoT services | Google Cloud. [online] Available at: https://cloud.google.com/solutions/iot/ [Accessed 24 September, 2024].
32. Ibm.com. (2019). IBM Watson Internet of Things (IoT). [online] Available at: https://www.ibm.com/internet-of-things [Accessed 24 September, 2024].

33. Cloud.oracle.com. (2024). Internet of Things | Oracle Cloud. [online] Available at: https://cloud.oracle.com/iot [Accessed 24 September, 2024].
34. Thingspeak.com. (2019). IoT Analytics - ThingSpeak Internet of Things. [online] Available at: https://thingspeak.com/ [Accessed 24 September, 2024].
35. Particle. (2019). Particle Company News and Updates. [online] Available at: https://www.particle.io/ [Accessed 24 September, 2024].
36. Kaa IoT platform. (2019). Kaa Enterprise IoT platform. [online] Available at: https://www.kaaproject.org/ [Accessed 24 September, 2024].
37. Cisco. (2024). Cisco IoT Cloud Connect. [online] Available at: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-cloud-connect.html [Accessed 24 September, 2024].
38. PTC. (2024). ThingWorx IIoT Platform. [online] Available at: https://www.ptc.com/en/products/iiot/thingworx [Accessed 24 September, 2024].