Survey of Platforms for Massive IoT

Devananda
School of Electrical and Informatics Engineering
Bandung Institute of Technology
Bandung, Indonesia
devanandakrn@gmail.com

***Abstract*—IoT platform technology developments has increased due to emerging of the Internet of Things (IoT) technology. IoT platform are utilized to facilitate IoT development. Furthermore, IoT systems are now gaining traction in the market. Each platform offers unique and valuable services and features. Therefore, this paper aims to do a survey to determine the parameters and criteria to compare a massive IoT platform. Additionally, it surveys and analyzes using several parameters or criteria to compare several IoT platforms that refer to a few types of research such as a review of 20 different IoT platforms by Hamdan Hejazi et al., the specific survey of IoT cloud platforms by Partha Pratim Ray, and Comparison of IoT platforms for cyber-physical systems (CPS) by Yohanes Yohanie Fridelin Panduman et al. The results of comparing IoT platforms show that some IoT platforms, such as KAA platform and Microsoft Azure IoT, have met these criteria because they have used Digital Twin technology to virtualize physical entities from the device to the server and be able to know the conditions of the device for its environment. Moreover, this paper explains several problems that exist in today's IoT platform, which is standardize, heterogeneity, middleware, IoT node identity, energy management, context awareness, and fault tolerance. As a result of this research, a study of IoT-valued large data clouds will be conducted in the near future. Future studies could include a full comparison and description of cloud platforms, Standardized Protocols for the Internet of Things, and IoT platform kinds.**

Keywords—Internet, IoT, Platforms, Comparison

I. INTRODUCTION (*HEADING 1*)

We can now have quick access to information about the real world and its items because of the Future Internet. As a result, the Internet of Things (IoT) has been embraced to integrate digital information with the real world of devices. Watches, televisions, automobiles, machinery, and other devices can all connect to the Internet. The IoT industry's rapid expansion necessitates robust IoT platforms that fulfill renewal requirements, such as in smart city applications, where a massive volume of data must be handled.

The Internet of Things (IoT) is a network of connected objects in the real world, such as sensors, vehicles, and devices, that can be monitored, detected, and controlled. Sensors are integrated in the objects, allowing them to detect their surroundings and communicate with other objects [12]. The environment is monitored, and items have the ability to perceive, be uniquely identified, and perform any specified action. Users can use the internet to access the items, receive notifications, and take action to regulate the environment.

Emerging industrial IoT and the fourth industrial revolution (Industry 4.0) give flexibility for planners and implementers, resulting in better decision-making. Furthermore, in addition to the apps given, machine monitoring and cloud services assist to growth and production.

Finding an acceptable IoT platform for a specific field of application is a challenge that any firm faces when trying to choose the right platform from a large number of options. Although IoT platforms provide comparable or even identical capabilities, their implementation and underlying technologies differ. The platform selection procedure is sometimes carried out without a thorough examination of the requirements [4].

Current IoT platforms have a market share and provide clients with competitive benefits and features that drive them to choose them. It offers a variety of services and applications, including data collection and analytics, device management, integration, security, operational intelligence, and the capacity to identify and control devices. There are several IoT models, including as on-premise models that are operated on the same premises or companies, and platform as a service models that are operated off premises and often involve cloud computing. Companies frequently make decisions based on these models.

The remaining paper is written out as follows. Comprehension of IoT Platform Parts is introduced in Section II. Conparison of IoT by afew type of reseach are discussed in Section III. In Section IV, I highlight Problem of the Existance IoT Platforms.

II. COMPREHENSION OF IOT PLATFORM PARTS

A. Concetual of IoT platform

IoT platforms are made up of a large number of linked objects all across the world. It connects cloud services and applications to the edge of devices, gateways, and data networks. The objects may be surrounding or separated by large distances in diverse contexts, but they are all managed by the centralized administration that serves as the IoT platform's processing unit. To better understanding IoT attitude and absolute sense, it is necessary to research and identify the elements/components/blocks that make up IoT platforms. Because each block of IoT platforms becomes an appealing topic of research, they create a loosely interconnected system, and all of the blocks are influential in the competition between IoT providers, the important blocks of IoT platforms are described as components in this study. Sensing, communication, and identification components, computing and cloud components, and lastly services and applications components make up the components. The strengths and limitations of all the platforms are determined by the IoT protocols in the communication and identification component, as well as the average processing speed in the computing and cloud element, as well as the offered services and applications given. This study includes numerous aspects of IoT platform comparison, resulting in a comprehensive survey of platforms for massive IoT.

Platforms for the Internet of Things (IoT) are a fascinating topic in the information and communication technology (ICT) business. The majority of studies and researchers in the literature focus on presenting IoT solutions. In the Internet of Things, standardization refers to the necessity of enhancing interoperability between diverse apps, services, and consumers. Furthermore, the Web of Things (WoT) is linked

to the Internet of Things (IoT) [5], as data visualization and applications offered to users are based on IoT platforms in the web world. The majority of IoT platforms provide a web browser-based graphical frontend for human communication and control of Internet-connected devices.

The Internet of Things platform is a system that provides a set of services or features that are used to develop IoT, such as communication between devices or sensors, data storage, and application service environments in general. The IoT platform is typically hosted on a cloud server [11]. Device management, integration, security, data collecting protocols, and analytics types are among the characteristics of an IoT platform, according to a study conducted by Rusu Liviu in 2017 [11].

B. An IoT platform elements

IoT functionality is divided into six parts, as explained in [9] [10].

- Identification block, which means each IoT object must be uniquely defined within the network of objects, such as with an assigned unique ID;
- Sensing block, which includes actuators that act when required;
- Communication block, which defines IoT communication technologies;
- Computation block, which is responsible for the IoT's processing and computational ability;
- Services block, which represents all of the many types of services offered by IoT platforms, and
- Semantics block, which shows how to extract data and work with various devices to give the needed services using web technologies.

Figure II.1depicts the IoT reference platform as a four-part architecture[1].

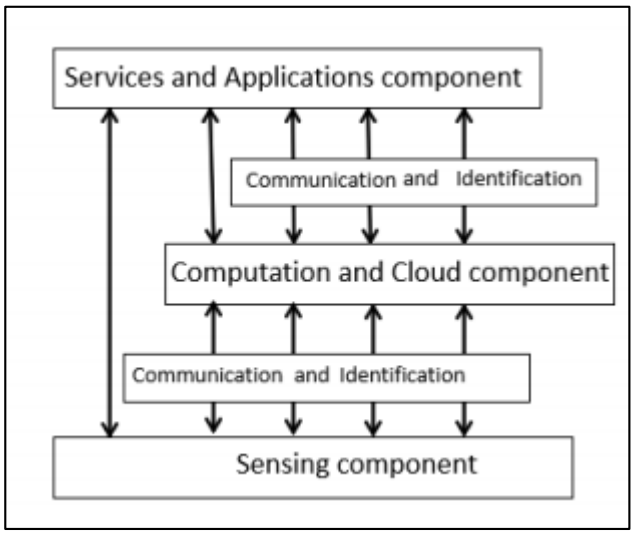

Figure II.1 An IoT Platform Elements

a. Sensing component that includes sensors, actuators, and devices

The sensor, which monitors the physical environmental condition, is one of the most important elements on the IoT platform. The sensor's job is to take measurements and sense the physical world before translating them into an electrical signal. It captures precise sensory data from IoT devices and sends it to a designated location, such as a database with data management or cloud computing for analysis. Actuators are hardware mechanical devices that perform the requested response to changes. They are also employed in IoT platforms such as switches. They generate electrical signals and turn them into physical actions. It works in the opposite direction as a sensor. Any hardware component that handles data from sensors and controls actuators and is connected by wires or wirelessly is referred to as a device.

b. A communication and identification component

IoT objects that require communication with the top system manage the data acquired. A gateway that connects devices and operates in the condition of a device that is not capable of direct communication with other systems. When a device is unable to interact via a specific protocol, for example, the gateway is employed. It can send and receive data via IoT communication protocols. In real-world IoT systems, the entire IP protocol stack is implemented on the end devices. Despite the fact that it will load the end device, it will allow for “gateway-less” end-to-end communication. IoT connection protocols such as CoAP and MQTT are included in the Communication component to link multiple IoT objects and transfer data to the management system [4]. In networks and operations of sensors, actuators, and devices, identification in addition to authentication delivers considerable performance advantages. It aids in the discovery of process errors that have reappeared. Unique identifiers are assigned to each object by specialized identifying technologies. Sensors and gadgets with suitable communication technologies connected to the Internet.

c. A computation and cloud component that represents the tasks of the IoT's "processing unit,"

The majority of today's IoT platforms are cloud-based. There are numerous technologies and techniques to choose from. The data from sensors and devices is collected and processed on the IoT platform's cloud. This component is known as IoT integration middleware because it serves as a combination layer for various types of sensors, actuators, devices, and applications. It represents the processing unit and offers the computational capabilities of the IoT. It uses appropriate communication technologies and transport protocols, such as WebSockets, to communicate with devices and platforms. Messages are sent in the appropriate payload format, such as JSON or XML.

d. The services and applications component

The services and applications component, which represents the services and capabilities available to the user through the IoT platform to connect and control the environment. Data collecting and data analytics, assistance for data visualizations, management, incorporation, and security are just a few of the services provided by IoT platforms. By enabling free access to devices, connectivity is provided as a service. Analytical tools based on data collected by sensors and devices can be employed in application development.

C. IoT protocols

Machine-to-machine (M2M) systems are created by the Internet's massive number of connected objects or devices. It is a form of IoT system, and the other parts of the system must be set, maintained, and monitored throughout their lifetime in order to provide service and device management. Lightweight M2M is a communication protocol that allows M2M devices, such as client software, to communicate with M2M management and service enablement platforms contained in server software. Lightweight M2M has a number of capabilities, including interfaces for bootstrapping, registration, management, and services, and services reporting. It is built on efficient and secure IETF standards, such as Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS).

a. Constrained Application Protocol (CoAP)

The Constrained Application Protocol (CoAP), which is based on the Hypertext Transfer Protocol (HTTP) and uses one-to-one communication, is a new communication protocol built specifically for IoT hardware. CoAP does not support TCP/IP connection because it is used for IoT hardware, which must be lightweight, small, and generate as little traffic as reasonable. Brandon Cannaday [7] examines a performance comparison between HTTP and CoAP in terms of energy usage and response time. CoAP includes a Discover functionality for locating devices in the immediate vicinity. Furthermore, a typical IoT platform may offer a number of connection protocols from which the device manufacturer can select the most appropriate.

b. MQTT

MQTT (Message Queue Telemetry Transport) is a published subscribe lightweight communication protocol that is implemented over TCP/IP. In the center of communication between devices, it uses a message broker server. Subscriber, publisher, and broker are the three components. The clients then use the broker to publish and subscribe to subjects. MQTT supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for security (TLS).

D. The importance of IoT platforms

The Internet of Things (IoT) is a popular technology. It is a collection of devices, sensors, software, and networks that work together to release the Internet of Things' beneficial and valuable data. All of these elements will be combined to make an IoT platform. As a result, the following are the primary goals of using IoT platforms:

a. IoT networks and multi-network connectivity

Various forms of network technology have recently been applied to connect IoT devices. However, the optimal networking solution is determined by how and where it will be deployed, as long as the required service quality is met. As a result, an all-encompassing IoT platform should facilitate communication and supply all necessary IoT kinds in order to provide the greatest flexibility for current and future projects.

b. IoT service management

Using an IoT platform is an important aspect to gain better management of the activity and business and also to enhance the capacity, and optimize operations. To keep on IoT solutions consistently running, IoT platforms should supply administration for accessing the user-controlled software tools to maintain the endpoints and the connections via the networks as a component of IoT solution. In addition, an appropriate on-demand service management implementation enables control of the IoT network by allowing for the addition, relocation, removal, or modification of IoT device reporting functions.

c. IoT data management and application enablement

Most IoT solutions have an impact on a variety of sensors that can generate a large amount of data over time, such as condition, position, and status. Each data point is typically brief, although the volume of information collected is typically large, owing to the frequency with which IoT devices report. The ability to secure and standardize data from many IoT endpoints, virtually any sensor, and any device reading is supported by an IoT platform. Multiple methods are utilized to convey streams of data, and after receiving the data, fragmentation is performed so that the gathered data can be efficiently processed, used, or reacted to based on the data received by executing the commands.

d. Accurate data analytics

Analytics, statistic computation, and data management using a variety of data sources and technology must yield an usable outcome with correct data analytics. The ultimate goal of data collection is to improve business outcomes by increasing visibility and understanding. An IoT platform could provide complete data and analytics views, as well as ability to extract data and retain business from shipwrights of fresh information that might be poorly organized. Analysis will be performed on the IoT platform, as well as the ability to access third-party analytics tools via secure APIs and services.

e. Security with multiple layers

One of the most important factors to consider for every IoT organization is security with several levels. As mentioned in the study [6], centralized and distributed low-level protocols for IoT, including privacy and security. Following the required safeguards and standards to decrease the risk and maximize the benefits of utilizing new sets of linked devices.

E. The function of IoT platforms

Many aspects of our activities are impacted by IoT platforms. As a component of IoT platforms, connectivity services are provided, and there are distinct connectivity platforms that connect consumers and their devices. In IoT platforms, security entails transferring trusted data to the cloud and maintaining ongoing value through analytics. Authentication, authorization, content integrity, and data security are all additional functions that must be provided.

F. Discovering the optimal solution of IoT platform

Each source has unique features and services that set it apart from the others. Several elements are taken into consideration, including hardware type, protocols, data visualization, and the desired service, among others. As a result, according to LinkLabs [8], before investing in a certain IoT platform, the organization must explore these choices

a. The platform’s tability

There is a potential that certain platforms will fail despite the fact that there are several on the market. It is critical to select a platform with high availability, i.e., the likelihood of staying operational with no interruption for several years; otherwise, the investment may be lost if the platform provider fails. In order to determine whether the chosen platform is good or not, inquire about current and previous consumers.

b. The platform's scalability and flexibility

Ascertain that the platform will function not only for a limited number of endpoints at first, but also with expanding demand over time. In addition to scalability, the platform should be adaptable to rapidly changing protocols, technologies, or features. The platform must also be network agnostic.

c. The consideration of pricing model and business case

There are various platforms that provide introductory costs, and after choosing and subscribing to them, numerous features that are not required or are essential are discovered. Furthermore, platforms focused with saving time have more expensive operations, but platforms focused with saving money may not have all of the competitive features. In general, the company that provides more features will last longer.

III. Platform Comparison for Internet of Things (IoT)

Earlier studies and research have compared many IoT platforms to define the parameters of the IoT platform. Furthermore, there is a scarcity of support for analysis of created IoT data in terms of both visualization and computing. The majority of IoT platforms included real-time support analytics, which is a must in any IoT framework. On the other hand, the visual interface of data via graphical frontends was mostly centered on simple web site layouts. These panels grant permission to control the IoT ecosystem.

This section presents a few types of study [1][2][3] that compare IoT platforms based on their suitability in specific application sectors. There are obviously plenty more platforms on the market, but according to technical and time constraints, just a few of these are chosen to provide realistic information about how they work, what their strengths and shortcomings are, and in which domain they are appropriate.

A. Review of 20 different IoT platforms by Hamdan Hejazi et al.

Hamdan Hejazi et al. provide 20 various IoT platforms based on their suitability for specific application sectors. Twenty distinct categories are chosen and presented alphabetically, based on where the majority of IoT platforms are currently evolving in the IT sector. When comparing platforms, consider the following parameters: integration, security, a data gathering mechanism, and types of analytics assistance for visualization.

This part also includes Table 1, which compares IoT based on their acceptability and appropriateness in the mandated application domain division. Platforms with open-source properties are thought to be more promising than proprietary alternatives for the following reasons.

Identify applicable funding agency here. If none, delete this text box.

B. Specific survey of IoT cloud platforms by Partha Pratim Ray

Partha Pratim Ray assesses 26 IoT cloud platforms based on their suitability for certain application categories. There are obviously many more platforms on the market, but owing to technical and time constraints, 26 of them are chosen to provide detailed information about how they function, what their strengths and drawbacks are, and which domains they are good for. Management-wise, a few technological domains are envisioned where these platforms fit well, such as Device, System, Heterogeneity, Data, Deployment, and Monitoring. Similarly, the domains of Analytics, Research, and Visualization are chosen as possible destinations for the rest of the platforms.

This part also includes Table 2, which compares IoT based on their acceptability and appropriateness in the mandated application domain division. Tabel 2 shows that Data management-based platforms are now trending in the industry, accounting for 19.2 percent of the 26 IoT cloud platforms. Device and application management domains are performing similarly in the IoT industry, with a value of 11.5 percent. 7.6 percent is assigned to heterogeneity, analytics, monitoring, visualization, and research domain. Deployment management has the lowest importance at the moment, accounting for 3.8 percent. Monitoring management is currently in first place, with a score of 42.3 percent. Application development, device management, and visualization are ranked second, third, and fourth, with scores of 38.4 percent, 30.7 percent, and 19.2 percent, respectively.

C. Comparison of IoT platforms for cyber-physical systems (CPS) by Yohanes Yohanie Fridelin Panduman et al.

Yohanes Yohanie Fridelin Panduman et al. conducted studies by comparing and assessing many IoT platforms based on factors and criteria required by an IoT platform, where criteria have a correlation to produce an IoT platform that is a solution for CPS problems. This section presents the comparison results of the IoT platform studied in this study. The research shows that CPS has a basic architecture such as the IoT architecture for smart factories combined with twin digital technology [yohan].

Table 3 indicates that most IoT platforms provide device management for credentials and events, however this research reveals that Azure IoT and Thingsboard have employed digital twin technology to construct smart factories or CPS systems. Because of its supremacy with little computational power, MQTT is a communication protocol utilized by all IoT platforms. Because it is capable of storing enormous amounts of heterogeneous data, practically all IoT systems have given NoSQL BigData services for data storage. This is also pertinent to the requirements of a smart manufacturing system and CPS, both of which require enormous volumes of data storage.

Table 4 highlights that all IoT platforms have features to provide feedback to the device as a trigger to move the actuator; this feature is critical for the development of CPS platforms that interact with devices on a regular basis. The comparison results illustrate that numerous platforms can collaborate on actions by integrating with other platforms or applications. Because all IoT platforms use SSL security and fulfil the scalability requirements, this is the criterion required to construct a CPS platform capable of connecting billions of devices.

IV. Problem of the Existing IoT Platforms

This section discusses the few major prospects of these applications to improve the existing solutions [2], which are listed below, whereas the following sections will illustrate the road to enhance the current situation point by point.

A. Standardization

Standardization is a key component that can be used to accelerate the development of IoT-centric apps. Standardization in the IoT cloud means lowering the initial barriers for service providers and active consumers, improving interoperability concerns across different applications or systems, and fostering greater competition among established products or services at the application level.

Table 1 Review of 20 different IoT platforms by Hamdan Hejazi et al.

IoT Software Platform	Device management?	Integration	Security	Protocols for data collection	Types of analytics	Support for visualizations?
AirVantage	Yes (Needs gateway)	REST API	*Unknown	MQTT, CoAP	Real-time analytics	Yes (User Interface Integrator)
Appcelerator	No	REST API	Link Encryption (SSL, IPsec, AES-256)	MQTT, HTTP	Real-time analytics (Titanium [1])	Yes (Titanium UI Dashboard
AWS IoT Platform	Yes	REST API	Link Encryption (TLS), Authentication (SigV4, X.509)	MQTT, HTTP1.1	Real-time analytics (Rules Engine, Amazon Kinesis, AWS Lambda)	Yes (AWS IoT Dashboard)
Bosch IoT Suite – MDM IoT Platform	Yes	REST API	*Unknown	MQTT, CoAP, AMQP, STOMP	*Unknown	Yes (User Interface Integrator)
Carriots	Yes	REST API	Unknown	MQTT	Real-time analytics	Yes (User Interface Integrator)
Ericsson Device Connection Platform (DCP) - MDM IoT Platform	Yes	REST API	Link Encryption (SSL/TSL), Authentication (SIM based)	CoAP	*Unknown	No
EVRYTHNG - IoT Smart Products Platform	No	REST API	Link Encryption (SSL)	MQTT, CoAP, WebSockets	Real-time analytics (Rules Engine)	Yes (EVRYTHNG IoT Dashboard)
Eurotech Device Cloud	Yes	REST API	Unknown	MQTT	Real-time analytics	Yes (Everyware™ Software Framework)
Exosite	Yes	REST API	Link Encryption (SSL)	CoAP, WebSocket	Real-time analytics	Yes (Web portal)

IBM IoT Foundation Device Cloud	Yes	REST and Real-time APIs	Link Encryption (TLS), Authentication (IBM Cloud SSO), Identity management (LDAP)	MQTT, HTTPS	Real-time analytics (IBM IoT Real-Time Insights)	Yes (Web portal)

IoT Software Platform	**Device management?**	**Integration**	**Security**	**Protocols for data collection**	**Types of analytics**	**Support for visualizations?**
Microsoft Azure IoT Suite	Yes	REST API	Link Encryption (SSL/TSL),	HTTP, AMQP, MQTT	Real-time analytics	Yes (Web Portal)
Litmus Loop	Yes	REST API	*Unknown	MQTT	Real-time analytics	Yes (Web portal)
ParStream - IoT Analytics Platform***	No	R, UDX API	*Unknown	MQTT	Real-time analytics, Batch analytics (ParStream DB)	Yes (ParStream Management Console)
PLAT.ONE - end-to-end IoT and M2M application platform	Yes	REST API	Link Encryption (SSL), Identity Management (LDAP)	MQTT, SNMP	*Unknown	Yes (Management Console for application enablement, data management, and device management)
Samsung ARTIK Cloud	Yes	REST API	Link Encryption (SSL)	LWM2M, CoAP, MQTT, IPv6	Real-time analytics	Yes (Web portal)
Temboo	Yes	REST API	*Unknown	MQTT, CoAP	Real-time analytics	Yes (Web portal)
ThingWorx - MDM IoT Platform	Yes	REST API	Standards (ISO 27001), Identity Management (LDAP)	MQTT, AMQP, XMPP, CoAP, DDS, WebSockets	Predictive analytics (ThingWorx Machine Learning), Real-time analytics (ParStream DB)	Yes (ThingWorx SQUEAL
Xively- PaaS enterprise IoT platform	No	REST API	Link Encryption (SSL/TSL)	HTTP, HTTPS, Sockets/ Websocket, MQTT	*Unknown	Yes (Management console)
Intel® IoT Platform	Yes	REST and Real-time APIs	Unknown	MQTT	Unknown	Yes (Web portal)

Lelylan	Yes	REST API	Link Encryption (SSL/TSL), Authentication (SIM-based)	MQTT, WebSocket	Real-time analytics	Yes (Web portal) "Apache License, Version 2.0"

Table 2 Specific survey of IoT cloud platforms by Partha Pratim Ray

IoT cloud platforms	**Domain**									
	Application development	**Device management**	**System management**	**Heterogeneity management**	**Data management**	**Analytics**	**Deployment management**	**Monitoring management**	**Visualization**	**Research**
Aercloud			applicable			applicable		suitable		
Arkessa		applicable			suitable					
Arrayantconnect	applicable	applicable		suitable	applicable					
Axeda		applicable			suitable			applicable		
Ayla's clous fabric		applicable	suitable						applicable	
Carrots	suitable	applicable						applicable		
Echelon	applicable	applicable					suitable			
Etherios		suitable						applicable		
Exosite		applicable	suitable					applicable		
GroveStreams	applicable							applicable	suitable	
IBM IoT		applicable								suitable
InfoBright					applicable	suitable				
Jasper Control Centre	applicable					suitable		applicable		
KAA	suitable				applicable					suitable
Microsoft research lab of things	applicable									
Nimbits					suitable	applicable				
Oracle IoT cloud			applicable	applicable	suitable		applicable		applicable	
OpenRemote	applicable			suitable						
Plotly						applicable		applicable	suitable	
SeeControl IoT		suitable				applicable			applicable	
SensorCloud		suitable						applicable	applicable	
Temboo	suitable									
Thethings.io	applicable		suitable					applicable		
ThingSpeak	applicable							suitable	applicable	
ThingWorx	applicable				suitable			applicable		
Xively	applicable	suitable						applicable		

Table 3 Result I of Comparison of IoT platforms for cyber-physical systems (CPS) by Yohanes Yohanie Fridelin Panduman et al.

IoT Platform			**Parameters and Criteria**			
	Thing management	***Connectivity***	***Data Storage***	***Data Abstraction***	***Interface***	***Analytical***
KAA Platform	Manage devices and credentials, Enable digital twins.	MQTT	MongoDB, Cassandra, PostgreSQL & Maria DB	Apache Thrift	Dashboard, Real-time visualization in gauges, charts, maps, tables, etc	Real-time analytics, pattern analysis.

Thingspeak	No, Manage the channel and credentials	MQTT, HTTP	Not-mention	No	Real-time visualization in plots, charts, and gauges with MATLAB	Analysis with MATLAB
Microsoft Azure IoT	Management in plans, provisioning, configuration, monitoring, firmware updates. Enable digital twins	MQTT, AMQP. HTTPS	Azure Storage	Azure Stream Processing Service	Azure Sphere, Time Series or Maps Services	Real-time analytics through Machine Learning
Thingsboard	Manage devices credentials and event	MQTT, CoApor HTTP	Cassandra	Thingsboard Core Services	Dashboard, Real-time visualization gauges, charts	Apache Spark
AWS IoT	Manage device in plans, provisioning, configuration, monitoring, firmware updates	HTTP, MQTT, WebSockets	MongoDB, Amazin DynamoDB, Other Database	Amazon Kinesis	Dashboard, Real-time visualization gauges, charts	Real-time analytics

Table 4 Result II of Comparison of IoT platforms for cyber-physical systems (CPS) by Yohanes Yohanie Fridelin Panduman et al.

IoT Platform	**Parameters and Criteria**				
	Feedback & Collaboration	***Security***	***Scalability***	***Microservices***	***Plug and Play***
KAA Platform	Yes, Feedback to the device, Integrations with business tools (SAP, Salesforce)	Link encryption SSL	Yes	Yes	Yes
Thingspeak	Yes, Trigger a reaction on the device using TalkBack app	Link encryption SSL	Yes	No	No
Microsoft Azure IoT	Yes, Feedback to the device, Integrations with another service	Link encryption SSL	Yes	Yes	Yes
Thingsboard	Yes, Integration to other systems such as the AWS IoT and Azure Event Hub	Link encryption SSL	Yes	No	Yes
AWS IoT	Yes, Feedback to the device, Integrations with another service	Link encryption SSL	Yes	Yes	No

B. Heterogeneity

The Internet of Things (IoT) is a highly complex heterogeneous network platform. However, the few clouds described above are unable to interface with diverse modules or communication technologies. This, in turn, increases the intricacy among various sorts of devices via various communication methods, revealing the network's impolite behavior to be false and delayed. Bandyopadhyay et al. have stated unequivocally that managing connected objects by facilitating collaborative work among various things (hardware components or software services) and administering them after providing addressing, identification, and optimization at the architectural and protocol levels is a serious research issue.

C. Middleware

Middleware facilitates the horizontal flow of information across devices, protocols, and applications in relation to itself. Applications can be run throughout the entire data set, and queries can be handled centralized on the connected devices. IoT clouds demand the adoption of a greater number of middleware to function.

D. IoT node identity

The Internet of Things is expected to have a massive number of nodes. All attached devices and data must be retrievable; in this case, a unique identity is required for efficient point-to-point network configuration. As it is well known that the availability of IPv4 numbered addresses is fast reducing, with the possibility of approaching zero in the next years, new addressing policies must be implemented, where IPv6 is a strong candidate. The presented systems primarily communicate over IPv4. However, a futuristic network may be so densely populated that imposing a distinct identity on the nodes becomes challenging. Improved techniques to be combined with the current strategy.

E. Energy management

While operating in energy harvesting, system components such as IoT devices, network antennas, and other dependent passive modules, as well as the fundamental algorithms, should be correctly addressed. Otherwise, non-traditional energy collecting methods such as solar power, wind, biomass, and vibration cloud should be tested while creating IoT-based cloud systems. As a result, researchers may become involved in the future to work on alternative sources.

F. Context Awareness

Context-aware computing approaches must be used more effectively to help determine what data needs to be processed. This appears to establish the negation of information validation in the form of a constantly disturbed process. Surrounding environmental characteristics and self-assessment may communicate the localized context to others while creating a self-contained, periphery-aware IoT cloud ecosystem.

G. Fault tolerance

The preceding solutions are mainly devoid of fault tolerance. To create a perfect system, the fault tolerance level of the system should be kept very high so that the system continues to function even if there is a technological issue. Hardware modules can fail for a variety of reasons, including a low battery. Similarly, erroneous value production by the sensor, improper calibration, and communication failure can all lead to a problem condition. While searching for a solution, solar power may provide an alternative to battery-powered modules. The use of numerous communication protocols may increase power consumption, but it always provides seamless connectivity.

V. Conclusions

The conducted surveys and analyses to compare many IoT platforms using parameters or criteria such as Thing management, Connectivity, Data Storage, Data Abstraction, Interface, Analytical, Feedback & Collaboration, Security, Scalability, Microservices, Plug and Play. The study covers a wide range of topics, including device management, integration, security, data gathering protocols, analytics kinds, and visualization capabilities. This, in turn, may broaden the foundation of understanding the architecture and the roles of many components and protocols that comprise the IoT.

The results of comparing IoT platforms show that some IoT platforms, such as KAA platform and Microsoft Azure IoT, have met these criteria because they have used Digital Twin technology to virtualize physical entities from the device to the server and be able to know the conditions of the device for its environment. Another key factor is the IoT platform's capacity to give action, such as feedback to control the device or interface with other system services, such as those on Thingsboard.

Beside comparing IoT platforms, this study reveals the problem that exist in today's IoT platform, which is standardization, heterogeneity, middleware, IoT node identity, energy management, context awareness, fault tolerance. As a result of this research, a study of IoT-valued large data clouds will be conducted in the near future. Future studies could include a full comparison and description of cloud platforms, Standardized Protocols for the Internet of Things, and IoT platform kinds.

VI. References

[1] H. Hejazi, H. Rajab, T. Cinkler and L. Lengyel, "Survey of Platforms for Massive IoT," *IEEE*, 2018.

[2] P. P. Ray, "A survey of IoT cloud platforms," *Future Computing and Informatics Journal*, pp. 35-46, 2016.

[3] Y. Y. Fredelin, S. Sukaridhoto and A. Tjahjono, "A Survey of IoT Platform Comparison for Building Cyber-Physical System Architecture," *IEEE Xplore*, 2019.

[4] J. Guth, "Comparison of IoT Platform Architectures: A Field Study based on a Reference Architecture," pp. 1-6, 2016.

[5] V. Trifa and D. Guinard, "Towards the Web of Things," pp. 1-4, 2009.

[6] M. A. Rajan, P. Balamuralidhar, K. P. Chethan and M. Swarnahpriyaah, "A Self-Reconfigurable Sensor Network Management System for Internet of Things Paradigm," *2011 Int. Conf. Devices Commun*, pp. 1-5, 2011.

[7] B. Cannaday, "Top 3 Connectivity Platforms For Your IoT," Losant Entreprise IoT Platform, [Online]. Available: https://www.losant.com/blog/top-3-connectivity-platforms-for-youriot-devices. . [Accessed 1 June 2021].

[8] LinkLabs, "IoT Platforms: What They Are & How To Select One," LinkLabs, 03 August 2016. [Online]. Available: https://www.linklabs.com/blog/what-is-an-iot-platform. [Accessed 1 June 2021].

[9] S. Agrawal and D. Vieira, "A survey on Internet of Things," *Abakós*, vol. 1, 2013.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[11] R. L. Dumitru, "IoT Platforms: Analysisi for Building Projects," *Informatica Economica*, vol. 21, no. 2, pp. 44-53, 2017.

[12] M. Sruthi and B. R. Kavitha, "A Survey on IoT Platform," vol. I, no. 1, pp. 468-473, 2016.