IDERA® | Database Tools Whitepaper

IS YOUR BUSINESS READY FOR THE INTERNET OF THINGS?

INTRODUCTION

The Internet of Things (IoT) is the term used to describe the connection of network-capable devices to the Internet and other connected devices.

The equipment that makes up the IoT go far beyond the computers that were connected to form the consumer Internet. IoT devices include such diverse items as industrial machinery, home appliances, automobiles, and blood-sugar monitors.

Many complementary technologies work together to enable the Internet of Things. Databases and the teams that support them are an integral component of a viable IoT implementation. They are instrumental in the storage, processing, and presentation of the information gathered by networks of IoT devices.

This paper will discuss the elements required to construct an IoT implementation. We will also look at how the IoT enables automation in many areas of society and how businesses can use it to their advantage. Also, we will investigate the critical role of databases and their support teams.

TWO FLAVORS OF THE IOT

A distinction needs to be drawn between IoT implementations primarily used by businesses and consumers and those used in industrial settings.

The consumer IoT encompasses smart devices used to perform functions related to individuals or segments of society.

This consumer IoT includes everything from health data gathered from wearable devices to smart traffic lights that streamline the daily commute in busy cities. The consumer IoT is usually referred to as the Internet of Things. It is primarily concerned with increasing society's quality of life and the way consumers interact with businesses.

Receiving less notoriety, yet arguably of at least equal importance, is the Industrial Internet of Things (IIoT). This concept refers to the use of IoT technology to facilitate automated industrial processes in such diverse sectors as power generation and assembly lines. Automation techniques using the IIoT promise to change the face of the workforce in the coming years as industry shifts to smart machines where possible.

COMPONENTS OF THE INTERNET OF THINGS

Both flavors of the IoT use the same underlying elements to accomplish their goals.

An IoT implementation depends on the convergence of five distinct components that interact to provide information to human operators or machines. They are sensors and actuators, networks, protocols, intelligent analysis, and intelligent action.

SENSORS AND ACTUATORS WITHIN THE IOT SYSTEM

Sensors measure and provide the raw information on which the system depends.

Based on the IoT system under review, the sensors may be measuring environmental conditions such as pressure, temperature, moisture or other essential characteristics.

They may also focus on actions taken by smart consumer devices. The information can be monitored and analyzed or used to start manual or automated processes. Sensors form the endpoints of an IoT system and provide the raw materials that are stored and processed in the databases associated with the system. Sensors can be broadly categorized based on their data gathering and processing capabilities.

- Base sensors are limited to transmitting the value of the entity they measure to the network layer of the IoT system. They cannot process the data.
- Smart sensors add functionality that enables them to perform some processing on the data before they pass the data to the rest of the system. Embedded software can augment the power of the sensors by transforming analog data readings into digital signals more easily processed by the rest of the system.
- Intelligent sensors ramp up the capabilities of the devices with the addition of the ability to perform self-validation and testing as well as adapting to changing conditions. An intelligent sensor can engage in activities in response to environmental changes it has detected. They use more advanced computing technologies, including machine learning, to increase their utility in IoT implementations.

Actuators are used to take action based on measurements made by the system's sensors. Actuators can be defined as devices that transform energy into motion. They may be used to trigger alarms, warning systems, or to perform critical tasks such as starting or stopping infrastructure components. They are more widely used in IIoT systems than those designed for the consumer IoT. Some examples are:

- Hydraulic devices responding to liquid measurements;
- Thermal actuators using a heat source;
- Pneumatic devices generating motion from compressed air;
- Electrical actuators that use external energy sources

The actuator used is necessarily dependent on the specifics of the IoT implementation. A common characteristic of actuators is that they need to be network-connected and remotely controlled.

Advances in sensor technology have been a significant factor in the growth of the IoT. Sensors are continually being manufactured to be smaller, smarter, and less expensive, which enables them to be used in new and innovative ways.

Limiting factors in using sensors include their interoperability and power consumption. Security is also of significant concern as each sensor is a potential entry point into IoT networks. They offer hackers an attractive target with which to gain unauthorized access to organizations' computing infrastructure and data assets.

NETWORK CHALLENGES AND CONSIDERATIONS FOR IOT

The network that connects the components of an IoT system is vital to its ability to perform its functions.

Communication failure in any area of the system can ripple through and cause the entire implementation to malfunction. Some basic questions need to be answered when planning the network with which the parts of an IoT will communicate.

The location of the hardware components is the deciding factor in how they will be connected. A self-contained solution involves monitoring and interacting with a controlled assembly line. Such a solution will, by necessity, demand different methods of connectivity than one that is concerned with a network of wind turbines or a fleet of smart vehicles.

Options need to be weighed before deciding on network topology. The reliability of directly cabled devices may be appropriate for some deployments. In other cases, equipment will be required that can withstand harsh conditions and connect with Bluetooth, radio-frequency identification (RFID), WiFi, or other wireless protocols. Smart consumer appliances are usually connected via a wireless router in individual homes.

All associated devices in the IoT system need to communicate with their designated hardware and software resources. This communication can involve transmitting data to a diverse set of on-premises and cloud assets that demand the flexibility to use various communication protocols. These assets include the databases that are used to derive usable information from the IoT implementation.

IoT networks are impacted by some of the same limiting factors that affect sensors. Power consumption and security need to be considered when implementing all aspects of an IoT system. The availability of the required network bandwidth to accommodate the tremendous growth in the number of connected devices poses a challenge. And that challenge needs to be addressed when designing an Internet of Things solution.

TECHNOLOGY AND REGULATORY STANDARDS FOR IOT

The handling, processing, and storage of the data obtained from sensors need to be standardized to increase its reliability and value. Two categories of standards are instrumental for the IoT to operate securely and efficiently.

Technology standards such as network and communication protocols are required to ensure that connected devices can talk to each other and IoT management tools. Data aggregation needs to be standardized so that the extraction and transformation of sensor output produces usable data for analysis.

Regulatory standards related to the privacy and security of collected data are also essential in viable IoT implementations. Consumers need to be confident that information obtained from their smart devices is not misused. Similarly, the security of IoT systems is critically important in maintaining the safety of their operation.

INTELLIGENT ANALYSIS: AI AND ML IN IOT

Once data has been aggregated using the appropriate standards, it needs to be analyzed. This analysis is done through a combination of traditional analytical techniques and newer methods such as cognitive technologies. Predictive and prescriptive analytics can be performed with data generated through natural language processing, speech recognition, and computer vision.

Artificial intelligence (AI) and machine learning (ML) are widely used technologies in the IoT. Real-time data processing and analysis is vitally important to produce the desired outcomes of IoT systems. Problems can arise because of flawed data models. Another cause of problems can be the inability of legacy systems to process the unstructured data that is collected from many of the connected devices that form the IoT. We will look more closely at IoT software shortly.

INTELLIGENT ACTION IN IOT IMPLEMENTATION

The ultimate result of all IoT implementations is the intelligent actions that the systems perform. Here again, machine learning and artificial intelligence play a significant role in performing the required actions quickly and correctly. Deep learning is employed to influence human actions and facilitate productive machine-to-machine interaction.

The quality of the actions taken by IoT systems is directly related to the quality of the data collection and analysis that precedes them. Incomplete or incorrect analysis can cause potentially dangerous actions. Slow connectivity can lead to delayed actions that negate the expected benefits of the system. IoT systems cannot function properly without all components operating efficiently. Failure in any area threatens the viability of the entire system.

SOFTWARE FOR THE INTERNET OF THINGS

There are several types of software required in the construction of a working IoT environment.

They can be broadly defined as providing these functions:

- Collecting data from IoT sensors;
- Storing the data;
- Processing the data;
- Allowing human interaction with the system.

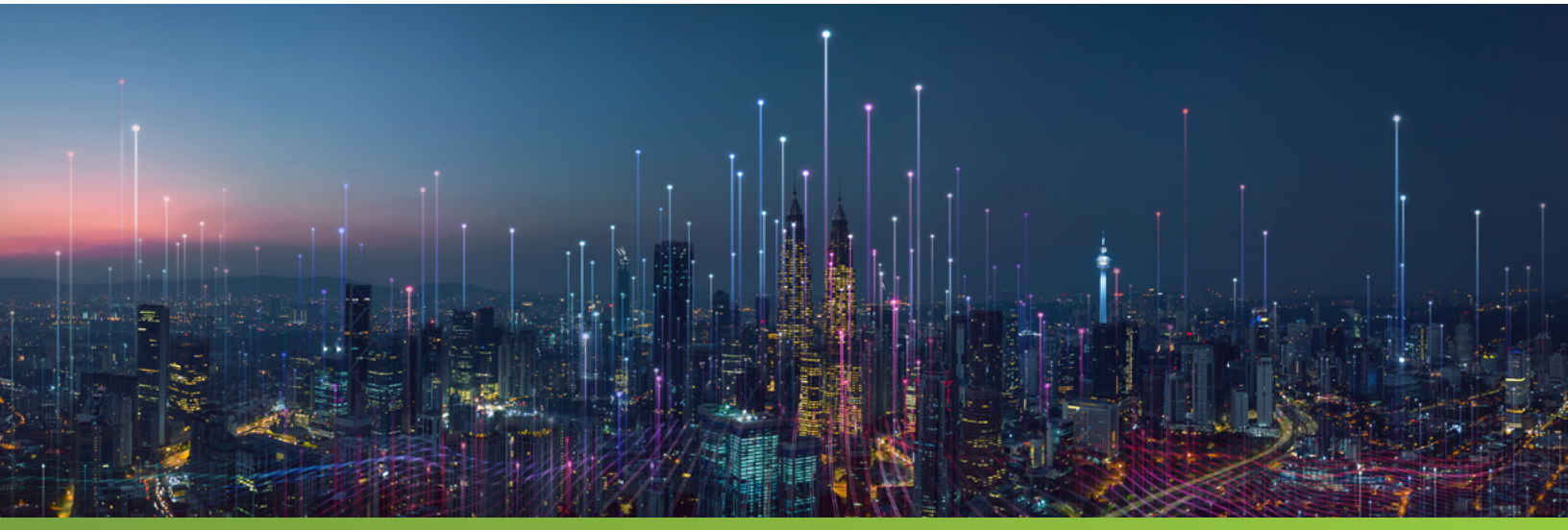
DATA COLLECTION

The sources of the information used in an IoT system are the sensors in the distributed network of connected devices.

The quality of data they provide is essential to the overall viability of the implementation. Ensuring this quality demands high-performing software at the data source.

Embedded software is primarily responsible for the flow of information from physical monitoring devices to the computer systems that process it. Embedded software can be seen as a system that is contained within a mechanical or electronic device. It comprises a sensor-based input system, output actuator, micro-controller, and a minimal amount of local memory.

Traditionally, embedded software has been proprietary, making interoperability with products from multiple vendors difficult or impossible. It also makes it hard to update the software to take advantage of technological breakthroughs. Recent moves toward using open-source embedded software promise to minimize this problem. Maintaining interoperability can limit the choices in hardware procurement.



DATA STORAGE

One of the defining characteristics of the IoT is the incredible volume of data that is generated by the connected-network of monitoring devices.

Collecting this data and putting it to productive use is the system's purpose. Storing it is an essential task in making the data available for further processing. It needs to be readily accessible for real-time and historical processes such as predictive analytics or capacity planning.

The cloud offers flexibility and scalability that fits well with the storage requirements of the IoT. Businesses can easily add storage capacity as their needs change without the complications and expense of adding on-premises resources. Cloud vendors often offer different performance and price options that provide a block, file, or object storage interface. The selected interface will coincide with the storage chosen for the cloud application.

DATA PROCESSING AND ANALYSIS

Software solutions are required to process the data collected from IoT devices. The information can be used for a wide variety of purposes based on the requirements of the IoT system it is supporting.

Data may be needed for use in real-time decision making, historical analysis, or both. Analytics is becoming an increasingly important technique in business and industry and can be put to good use with the data produced by the IoT. Dashboards that enable data to be disseminated and understood by non-technical personnel are useful both for monitoring and analysis. The specific software deployed needs to be fully integrated with the overall goals of the system and the storage methods used.

Databases straddle the line between data processing and storage software. They are vitally important in facilitating an effective IoT implementation. Compatibility between the databases and analytical software is essential when designing the system. The selected visualization tools need to interact with the chosen databases. Solutions that can be used with multiple platforms allow enhanced flexibility for database teams.

HUMAN-MACHINE INTERFACES (HMIS)

The ability to provide human interaction with the automated systems under the control of an IoT system is essential from a safety and security perspective. This human interaction is especially true in IoT implementations.

There needs to be a method for operators to assume control of the system in the event of unanticipated problems. HMIs can be implemented through software alone or as an embedded program built into IoT devices.

A higher degree of functionality is afforded by HMIs that are implemented as standalone software applications. They can provide operators the ability to view an entire installation and quickly drill down to isolate a specific component. Touch screen technology is used to enable staff members to access the HMI from tablet devices. Embedded HMIs are more limited and often control a single device or subsystem.

THE IMPACT OF THE IOT ON DATABASE PROFESSIONALS

Data is the currency of IoT implementations, making database professionals vitally important in creating successful systems.

Choosing the right database is an essential step that cannot be left to chance. Database platforms in use in an environment may not be appropriate for the way IoT data needs to be stored, accessed, and processed.

- Identifying the specific data needs of the IoT solution is the first step. Questions such as where the data should be processed and what it will be used for can inform the choice of databases. Different platforms, such as cloud-based solutions, may be more readily implemented with systems that are spread over larger geographic regions. If real-time responses or historical business analytics are required, the databases selected must be able to provide this functionality.
- Determining the requirements of database services is another step that needs to be taken when selecting the solution. The ability to handle high-speed read and writes as well as large volumes of data, is critical for IoT databases. In some cases, the stored data may need to be made available to supplemental tools for analytics and the creation of command-and-control dashboards. Understanding the characteristics and intent of the IoT system will help in making an informed decision about the underlying databases that it relies on.
- Multiple database solutions may be required to provide the functionality demanded by an IoT implementation. Hot and cold databases can be used to supply the features needed by different parts of the IoT system. In-memory databases deliver the highest data throughput and can be the perfect solution when real-time responses are part of system requirements. The volume of stored data used for analytics can quickly overwhelm the capacity of hot databases. Traditional solutions such as relational and NoSQL platforms are used as cold databases for long-term storage and processing.

Selecting the correct tools to extract the maximum amount of usable information from the chosen databases is another aspect of designing a viable IoT system. Here are some of the features to be considered when selecting database tools.

- The tools need to be compatible with the databases used in the system. This compatibility may require multiple tools if more than one database solution is in place. Flexible tools that can interact with various platforms are more attractive in this situation.
- Visualization capabilities in analytical tools can be a factor that determines their selection. Delivering real-time informative dashboards may require using different tools than those used for historical analytics. Comprehensive tools that afford users the ability to extract multi-format visualizations can streamline the processing of IoT data.
- Tools that can monitor databases and generate useful alerts are also crucial in developing successful IoT systems. Identifying processing bottlenecks and recommending performance-tuning guidelines can be the difference in developing a high-quality IoT implementation.

HOW THE INTERNET OF THINGS IMPACTS THE BUSINESS WORLD

The ability to automate processes is the primary benefit of the IoT in the world of business and industry.

Automation is used in many ways based on the focus of the organization implementing an IoT solution. Some examples include:

- Automated point-of-sale data collection for more efficient marketing and product placement;
- Better healthcare through the use of remote monitoring and microscopic sensors embedded in medical devices and pharmaceuticals;
- Smart automobiles that can request help in emergencies as well as controlling speed and reacting to changing traffic conditions;
- Increased assembly line productivity, efficiency, reliability, and safety by reducing the incidences of human error;
- Energy savings through smart lighting and heating systems for commercial and residential buildings;
- Micro-sensors embedded into construction materials to alert of impending structural failures.

This list of examples is just a brief sampling of the ways business, industry, and municipal planners are using the IoT to change the way we live and work.

MAINTAINING THE INTERNET OF THINGS AND YOUR IOT IMPLEMENTATION

Keeping the IoT running smoothly and producing its expected results requires vigilant security precautions.

As with all other instances of computing technology, security is an essential aspect of viable and useful systems. Here are some of the ways that security can be achieved in IoT implementations.

- Data encryption is a vitally important tool in securing IoT security. Every sensor, device, and network connection presents a potential security breach. Data needs to be encrypted at the source and throughout the storage and processing phases of an IoT system. System performance needs to be adequate to handle the overhead costs of processing encrypted information.
- Strict authorization and access controls are necessary to eliminate unscrupulous users from gaining entry into the system. These controls need to be implemented at the level of data collection and continue through every phase of an IoT system. Unauthorized entry at any point in the system can result in financial, privacy, and safety problems.

The Internet of Things is here to stay, and the number of connected devices is predicted to top 50 billion in 2020.

It is changing the way society, business, industry, and individuals function as we move through the 21st Century. The IoT will become an integral part of almost all aspects of our lives in the days to come.

Contact us to learn more.

IDERA