A Comparative study of cloud computing through IOT

Manoj Chopra, Vijay Dhote
Assistant Professor, IES College, Bhopal, INDIA

Abstract—Cloud computing and Internet of Things (IoT) are two very different technologies that are both already part of our life. The Internet of Things (IoT) is becoming the next Internet-related revolution. It allows billions of devices to be connected and communicate with each other to share information that improves the quality of our daily lives. On the other hand, Cloud Computing provides on-demand, convenient and scalable network access which makes it possible to share computing resources. Their adoption and use are expected to be more and more pervasive, making them important components of the Future Internet. A novel paradigm where Cloud and IoT are merged together is foreseen as disruptive and as an enabler of a large number of application scenarios.In this paper, we focus our attention on the integration of Cloud and IoT, which is call the Cloud-IoT paradigm. Many works in literature have surveyed Cloud and IoT separately and, more precisely, their main properties, features, underlying technologies, and open issues. However, to the best of our knowledge, these works lack a detailed analysis of the new Cloud-IoT paradigm, which involves completely new applications, challenges, and research issues. To bridge this gap. The vast number of resources available on the Cloud can be extremely beneficial for the IoT, while the Cloud can gain more publicity to improve its limitations with real world objects in a more dynamic and distributed manner.in this paper we provide a literature survey on the integration of Cloud and IoT. Starting by analyzing the basics of both IoT and Cloud Computing, we discuss their complementarity, detailing what is currently driving to their integration

Keywords—Cloud Computing, Internet of Things (IOT

INTRODUCTION:

Cloud computing:

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it.Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.

Understanding Cloud Computing

Cloud computing is named as such because the information being accessed is found remotely in the cloud or a virtual space. Companies that provide cloud services enable users to store files and applications on remote servers and then access all the data via the Internet. This means the user is not required to be in a specific place to gain access to it, allowing the user to work remotely.

Cloud computing takes all the heavy lifting involved in crunching and processing data away from the device you carry around or sit and work at. It also moves all of that work to huge computer clusters far away in cyberspace. The Internet becomes the cloud, and voilà—your data, work, and applications are available from any device with which you can connect to the Internet, anywhere in the world.

Cloud computing can be both public and private. Public cloud services provide their services over the Internet for a fee. Private cloud services, on the other hand, only provide services to a certain number of people. These services are a system ofnetworks that supply hosted services. There is also a hybrid option, which combines elements of both the public and private services. More information is outlined below.

Regardless of the kind of service, cloud computing services provide users with a series of functions including:

- Email
- Storage, backup, and data retrieval
- Creating and testing apps
- Analyzing data
- Audio and video streaming
- Delivering software on demand

Cloud computing is still a fairly new service but is being used by a number of different organizations from big corporations to small businesses, nonprofits to government agencies, and even individual consumers.

Cloud Computing Deployment Models

There are various types of clouds, each of which is different from the other. Public clouds provide their services on servers and storage on the Internet. These are operated by third-party companies, who handle and control all the hardware, software, and the general infrastructure. Clients access services through accounts that can be accessed by just about anyone.

Private clouds are reserved for specific clientele, usually one business or organization. The firm's data service center may host the cloud computing service. Many private cloud computing services are provided on a private network.

Hybrid clouds are, as the name implies, a combination of both public and private services. This type of model allows the user more flexibility and helps optimize the user's infrastructure and security.

Types of Cloud Computing

Cloud computing is not a single piece of technology like a microchip or a cellphone. Rather, it's a system primarily comprised of three services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

1. **Software-as-a-service (SaaS)** involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's 365.
2. **Infrastructure-as-a-service (IaaS)** involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure.
3. **Platform-as-a-service (PaaS)** is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Force.com and Heroku.

Advantages of Cloud Computing

Cloud-based software offers companies from all sectors a number of benefits, including the ability to use software from any device either via a native app or a browser. As a result, users can carry their files and settings over to other devices in a completely seamless manner.

Cloud computing is far more than just accessing files on multiple devices. Thanks to cloud computing services, users can check their email on any computer and even store files using services such as Dropbox and Google Drive. Cloud computing services also make it possible for users to back up their music, files, and photos, ensuring those files are immediately available in the event of a hard drive crash.

It also offers big businesses huge cost-saving potential. Before the cloud became a viable alternative, companies were required to purchase, construct, and maintain costly information management technology and infrastructure. Companies can swap costly server centers and IT departments for fast Internet connections, where employees interact with the cloud online to complete their tasks.

The cloud structure allows individuals to save storage space on their desktops or laptops. It also lets users upgrade software more quickly because software companies can offer their products via the web rather than through more traditional, tangible methods involving discs or flash drives. For example, Adobe customers can access applications in its Creative Suite through an Internet-based subscription. This allows users to download new versions and fixes to their programs easily.

DisadvantagesofCloudComputing

With all of the speed, efficiencies, and innovations that come with cloud computing, there are naturally risks.

Security has always been a big concern with the cloud especially when it comes to sensitive medical records and financial information. While regulations force cloud computing services to shore up their security and compliance measures, it remains an ongoing issue. Encryption protects vital information, but if that encryption key is lost, the data disappears.Servers maintained by cloud computing companies may fall victim to natural disasters, internal bugs, and power outages, too. The geographical reach of cloud computing cuts both ways: A blackout in California could paralyze users in New York, and a firm in Texas could lose its data if something causes its Maine-based provider to crash.As with any technology, there is a learning curve for both employees and managers. But with many individuals accessing and manipulating information through a single portal, inadvertent mistakes can transfer across an entire system.

The World of Business Cloud Computing

Businesses can employ cloud computing in different ways. Some users maintain all apps and data on the cloud, while others use a hybrid model, keeping certain apps and data on private servers and others on the cloud.

When it comes to providing services, the big players in the corporate computing sphere include:

- Google Cloud
- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Cloud
- Aliyun

Amazon Web Services is 100% public and includes a pay-as-you-go, outsourced model. Once you're on the platform you can sign up for apps and additional services. Microsoft Azure allows clients to keep some data at their own sites. Meanwhile, Aliyun is a subsidiary of the Alibaba Group.

internet of things (IoT)

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

History of IoT

Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999. Wanting to bring radio frequency ID (RFID) to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet. MIT professor Neil Gershenfeld's book, When Things Start to Think, also appearing in 1999, didn't use the exact term but provided a clear vision of where IoT was headed.

IoT has evolved from the convergence of wireless technologies, microelectromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silos between operational technology (OT) and information technology (IT), enabling unstructured machine-generated data to be analyzed for insights to drive improvements.

Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers embedded internet and pervasive computing.

The first internet appliance, for example, was a Coke machine at Carnegie Mellon University in the early 1980s. Using the web, programmers could check the status of the machine and determine whether there would be a cold drink awaiting them, should they decide to make the trip to the machine.

IoT evolved from machine-to-machine (M2M) communication, i.e., machines connecting to each other via a network without human interaction. M2M refers to connecting a device to the cloud, managing it and collecting data.

Taking M2M to the next level, IoT is a sensor network of billions of smart devices that connect people, systems and other applications to collect and share data. As its foundation, M2M offers the connectivity that enables IoT.

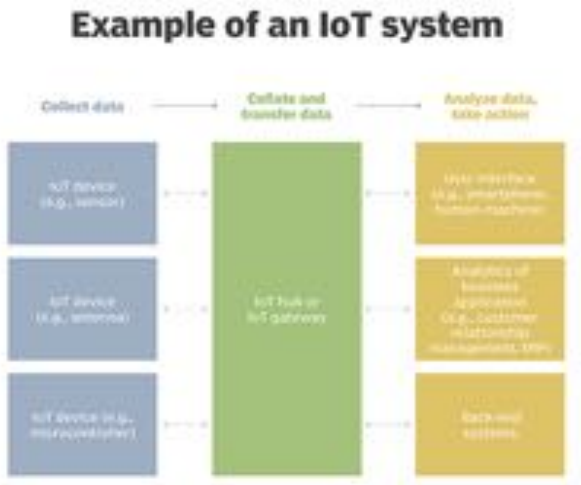
The internet of things is also a natural extension of SCADA (supervisory control and data acquisition), a category of software application program for process control, the gathering of data in real time from remote locations to control equipment and conditions. SCADA systems include hardware and software components. The hardware gathers and feeds data into a computer that has SCADA software installed, where it is then processed and presented it in a timely manner. The evolution of SCADA is such that late-generation SCADA systems developed into first-generation IoT systems.

The concept of the IoT ecosystem, however, didn't really come into its own until the middle of 2010 when, in part, the government of China said it would make IoT a strategic priority in its five-year plan.

How IoT works

An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed .



Benefits of IoT

The internet of things offers a number of benefits to organizations, enabling them to:

- monitor their overall business processes;
- improve the customer experience;
- save time and money;
- enhance employee productivity;
- integrate and adapt business models;
- make better business decisions; and
- generate more revenue.

IoT encourages companies to rethink the ways they approach their businesses, industriesand markets and gives them the tools to improve their business strategies.

Consumer and enterprise IoT applications

There are numerous real-world applications of the internet of things, ranging from consumer IoT and enterprise IoT to manufacturing and industrial IoT (IIoT). IoT applications span numerous verticals, including automotive, telco, energy and more.

In the consumer segment, for example, smart homes that are equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers, smartphones or other mobile devices.

Wearable devices with sensors and software can collect and analyze user data, sending messages to other technologies about the users with the aim of making users' lives easier and more comfortable. Wearable devices are also used for public safety -- for example, improving first responders' response times during emergencies by providing optimized routes to a location or by tracking construction workers' or firefighters' vital signs at life-threatening sites.

In healthcare, IoT offers many benefits, including the ability to monitor patients more closely to use the data that's generated and analyze it. Hospitals often use IoT systems to complete tasks such as inventory management, for both pharmaceuticals and medical instruments .

Smart buildings can, for instance, reduce energy costs using sensors that detect how many occupants are in a room. The temperature can adjust automatically -- for example, turning the air conditioner on if sensors detect a conference room is full or turning the heat down if everyone in the office has gone home.

In agriculture, IoT-based smart farming systems can help monitor, for instance, light, temperature, humidity and soil moisture of crop fields using connected sensors. IoT is also instrumental in automating irrigation systems.

In a smart city, IoT sensors and deployments, such as smart streetlights and smart meters, can help alleviate traffic, conserve energy, monitor and address environmental concerns, and improve sanitation.

IoT security and privacy issues

The internet of things connects billions of devices to the internet and involves the use of billions ofdata points, all of which need to be secured. Due to its expanded attack surface, IoT security and IoT privacy are cited as major concerns.

One of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. And manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

However, hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.

The future of IoT

1. By 2025, it is estimated that there will be more than to 21 billion IoT devices

A quick look back shows where IoT devices are going. Consider: In 2016, there were more than 4.7 billion things connected to the internet, according to IOT Analytics. Fast-forward to 2021? The market will increase to nearly 11.6 billion IoT devices.

2. Cybercriminals will continue to use IoT devices to facilitate DDoS attacks

In 2016, the world was introduced to the first "Internet of Things" malware — a strain of malicious software that can infect connected devices such as DVRs, security cameras, and more. The Mirai malware accessed the devices using default password and usernames.

What happened next? The malware turned the affected devices into a botnet to facilitate a Distributed Denial of Service (DDoS) attack, which aims to overwhelm websites with internet traffic. The attack ended up flooding one of the largest website hosting companies in the world, bringing a variety of major, well-known websites and services to a halt for hours.

This particular strain of malware is called "open source," which means the code is available for anyone to modify.

3. More cities will become "smart"

Consumers won't be the only ones using IoT devices. Cities and companies will increasingly adopt smart technologies to save time and money.That means cities will be able to automate, remotely manage, and collect data through things like visitor kiosks, video camera surveillance systems, bike rental stations, and taxis.

4. Artifici intelligence will continue to become a bigger thing

Smart home hubs, thermostats, lighting systems, and even coffee makers collect data on your habits and patterns of usage. When you set up voice-controlled devices, you allow them to record what you say to them and store those recordings in the cloud. In most cases, the data is collected to help facilitate what is called machine learning.

Machine learning is a type of artificial intelligence that helps computers "learn" without someone having to program them. The computers are programmed in a way that focuses on data that they receive. This new data can then help the machine "learn" what your preferences are and adjust itself accordingly. For instance, when a video website suggests a movie you might like, it's likely learned your preferences based on your past choices.

5. Routers will continue to become more secure and smarter

Because most consumer IoT devices reside in the home and can't have security software installed on them, they can be vulnerable to attacks. Why? A lot of manufacturers work to get their IoT products to market quickly, so security may be an afterthought. This is where the home router plays a very important role. The router is essentially the entry point of the internet into your home.

While many of your connected devices cannot be protected, the router has the ability to provide protection at the entry point. A conventional router provides some security, such as password protection, firewalls, and the ability to configure them to only allow certain devices on your network.

Router makers will likely continue to seek new ways to boost security.

6. 5G Networks will continue to fuel IoT growth

Major wireless carriers will continue to roll out 5G networks in 2019. 5G — fifth-generation cellular wireless — promises greater speed and the ability connect more smart devices at the same time.

Faster networks mean the data accumulated by your smart devices will be gathered, analyzed and managed to a higher degree. That will fuel innovation at companies that make IoT devices and boost consumer demand for new products.

7. Cars will get even smarter

The arrival of 5G will shift the auto industry into a higher gear. The development of driverless cars — as well as the connected vehicles already on the road — will benefit from data moving faster.

You might not think of your car as an Internet of Things device. But new cars will increasingly analyze your data and connect with other IoT devices — including other high-tech vehicles on four wheels.

8. 5G's arrival will also open the door to new privacy and security concerns

In time, more 5G IoT devices will connect directly to the 5G network than via a Wi-Fi router. This trend will make those devices more vulnerable to direct attack, according to a recent Symantec blog post.

For home users, it will become more difficult to monitor all IoT devices, because they will bypass a central router.

On a broader scale, the increased reliance on cloud-based storage will give attackers new targets to attempt to breach.

9. IoT-based DDoS attacks will take on more dangerous forms

Botnet-powered distributed denial of service (DDoS) attacks have used infected IoT devices to bring down websites. IoT devices can be used to direct other attacks, according to a Symantec blog post.

For instance, there may be future attempts to weaponize IoT devices. A possible example would be a nation shutting down home thermostats in an enemy state during a harsh winter.

10. Security and privacy concerns will drive legislation and regulatory activity

The increase in IoT devices is just one reason security and privacy concerns are rising.

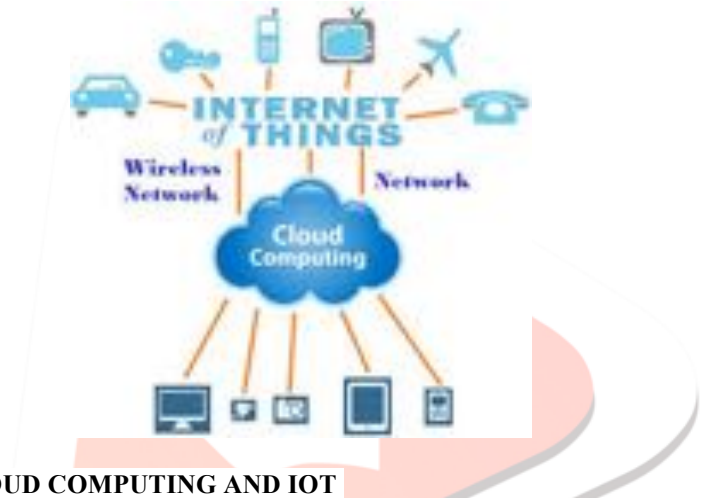
In mid-2018, the European Union implemented the General Data Protection Regulation. GDPR has led to similar security and privacy initiatives in several nations around the world. In the United States, California recently passed a tougher privacy law.

Gartner assesses that 20.8 billion connected things will be in use by 2020, with total spend on IoT devices and services to reach $3.7 trillion in 2018.

Cloud Computing Through IOT

The internet of Things is starting to transform daily tasks are completed. The Internet of Things (IoT) consists of everyday objects – physical devices, vehicles, buildings etc. with embedded electronics, software, sensors, and network connectivity, allowing them to collect, send and receive data. The IoT generates a vast amount of Big Data and this in turn puts a huge strain on Internet Infrastructure. As a result, this forces companies to find solutions to minimize the pressure and solve their problem of transferring large amounts of data.

Cloud computing has entered the mainstream of information technology, providing scalability in delivery of enterprise applications and Software as a Service (SaaS). Companies are now migrating their information operations to the cloud. Many cloud providers can allow for your data to be either transferred via your traditional internet connection or via a dedicated direct link. The benefit of a direct link into the cloud will ensure that your data is uncontended and that the traffic is not crossing the internet and the Quality of Service can be controlled.



DIFFERENCE BETWEEN CLOUD COMPUTING AND IOT

Cloud computing in simple terms means accessing data and programs from a centralised pool of compute resource that can be ordered and consumed on demand. Typically clouds deployments are described in 3 different models; Public, Private or Hybrid.

- **Private Cloud Services** is a secure cloud that only the specified organisation can access. The additional security offered by a private cloud model is ideal for any organisation, including enterprise, that needs to store and process private data or carry out sensitive tasks. For example, a private cloud service could be utilised by a financial company that is required by regulation to store sensitive data internally and who will still want to benefit from some of the advantages of cloud computing within their business infrastructure, such as on demand resource allocation.
- **Public Cloud Service** is like a Private cloud although the main differentiator is that resources used to process and store data can be shared with other organisations, and data transferred over a public network such as the internet. Third party providers will deliver cloud services over the internet and are normally charged by CPU cycles, storage, or bandwidth that they require.
- **Hybrid Cloud** is a cloud computing environment which uses a mix of on premise, private cloud and third party public cloud services. With the hybrid cloud model, IT decision makers have more control over both the private and public components than using a pre-packaged public cloud platform.

The internet of Things, meanwhile refers to the connection of devices other than the usual such as computers to the Internet. Cars, kitchen appliances and other sensors can be connected through the IoT. The IoT is an enabler for change. It enables systems and devices to be automated in a cost effective, intelligent manner supporting real-time control and monitoring. Having all the relevant information available (real time along with historical trend data) provides the ability to combine and process this data in an innovative manner resulting in more effective and efficient control or decision making.

HOW CLOUD COMPUTING COMPLEMENTS IOT INITIATIVES

Cloud computing and the IoT both serve to increase efficiency in everyday tasks and both have a complementary relationship. The IoT generates massive amounts of data, and cloud computing provides a pathway for this data to travel.

Many Cloud providers charge on a pay per use model, which means that you only pay for the computer resources that you use and not more. Economies of scale is another way in which cloud providers can benefit smaller IoT start-ups and reduce overall costs to IoT companies.

Another benefit of Cloud Computing for the IoT is that Cloud Computing enables better collaboration which is essential for developers today. By allowing developers to store and access data remotely, developers can access data immediately and work on projects without delay.

Finally by storing data in the Cloud, this enables IoT companies to change directly quickly and allocate resources in different areas. Big Data has emerged in the past couple of years and with such emergence the cloud has become the architecture of choice. Most companies find it feasible to access the massive quantities of Big Data via the cloud.

How IoT and cloud complement each other

Cloud computing, as well as IoT, work towards increasing the efficiency of everyday tasks and both have a complementary relationship. On one hand, IoT generates lots of data while on the other hand, cloud computing paves way for this data to travel. There are many cloud providers who take advantage of this to provide a pay-as-you-use model where customers pay for the specific resources used. Also, cloud hosting as a service adds value to IoT startups by providing economies of scale to reduce their overall cost structure.

In addition to this, cloud computing also enables better collaboration for developers, which is the order of the day in the IoT space. By facilitating developers to store as well as access data remotely, the cloud allows developers to implement projects without delay. Also, by storing data in the cloud, IoT companies can access a huge amount of Big Data. So, in a bid to lay down the relationship between IoT and cloud, here is a table that will let you know how they fit into each other like a glove.

Parameter	Internet of things	Cloud computing
Big Data	Acts as a source for big data	Acts as a way or a means to manage big data
Reachability	Very limited	Far spread, wide
Storage	Limited or almost none	Large, virtually never ending
Role of Internet	Acts as a point of convergence	Acts as a means for delivering services
Computing capabilities	Limited	Virtually unlimited
Components	Runs on hardware components	Runs on virtual machines which imitate hardware components

Why is Cloud essential to the success of IoT?

Just like cloud computing is built on the tenets of speed and scale, IoT applications are built on the principle of mobility and widespread networking. Hence, it is essential that both cloud and IoT form cloud-based IoT applications in a bid to make the most out of their combination. This alliance has led to the success of IoT. In addition to this, here are a few more pointers as to why the cloud is important from the point of view of IoT's success.

Provides remote processing power

Cloud as a technology empowers IoT to move beyond regular appliances such as air conditioners, refrigerators etc. This is because the cloud has such a vast storage that it takes away dependencies on on-premise infrastructure. With the rise of miniaturization and transition of 4G to higher internet speeds, the cloud will allow developers to offload fast computing processes.

Provides security and privacy

IoT's role in harnessing mobility is immense. However, its prowess would be incomplete without security. Cloud has made IoT more secure with preventive, detective and corrective controls. It has enabled users with strong security measures by providing effective authentication and encryption protocols. In addition to this, managing and securing the identity of users has been possible for IoT products with the help of biometrics. All of this is possible because of cloud's security.

Removes entry barrier for hosting providers

Today, many innovations in the field of IoT are looking at plug-and-play hosting services. Which is why the cloud is a perfect fit for IoT. Hosting providers do not have to depend on massive equipment or even any kind of hardware that will not support the agility IoT devices require. With the cloud, most hosting providers can allow their clients a ready-to-roll model, removing entry barriers for them.

Facilitates inter-device communication

Cloud acts as a bridge in the form of a mediator or communication facilitator when it comes to IoT. Many powerful APIs like Cloudflare, Cloud and Dropstr are enabled by cloud communications, allowing easy linking to smartphones. This eases devices to talk to each other and not just us, which essentially is the tenet of IoT cloud.

It would be fair to say that cloud can accelerate the growth of IoT. However, deploying cloud technology also has certain challenges and shortcomings. Not because the cloud is flawed as a technology but the combination of IoT cloud can burden users with some obstacles. If you ever go ahead with an IoT cloud solution, it is better if you know the kind of challenges you may face in advance.

What are the challenges posed by cloud and IoT together?

Handling a large amount of data

Handling a large amount of data can be overwhelming especially when there are millions of devices in the picture. This is because the overall performance of applications is at stake. Hence, following the NoSQL movement could be beneficial, but it is not tried and tested for the long run. Which is why there exists no sound or fool-proof method for the cloud to manage big data.

Networking and communication protocols

Cloud and IoT involve machine-to-machine communications among many different types of devices having various protocols. Managing this kind of a variation could be tough since a majority of application areas do not involve mobility. As of now WiFi and Bluetooth are used as a stop-gap solution to facilitate mobility to a certain extent.

Sensor networks

Sensor networks have amplified the benefits of IoT. These networks have allowed users to measure, infer and understand delicate indicators from the environment. However, timely processing of a large amount of this sensor data has been a major challenge. Though cloud provides a new opportunity in aggregating sensor data it also hinders the progress because of security and privacy issues.

Conclusion

The integration of cloud computing and IoT is indicative of the next big leap in the world of internet. New applications brimming from this combination known as IoT Cloud are opening newer avenues for business as well as research. Let us hope that this combination unveils a new paradigm for the future of multi-networking and an open service platform for users.

Reference:

[1] https://arxiv.org/ftp/arxiv/papers/1803/1803.02890.pdf
[2] https://pinaclsolutions.com/blog/2017/cloud-computing-and-iot
[3] https://www.investopedia.com/terms/c/cloud-computing.asp
[4] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[5] http://www.cs.umsl.edu/~pan/papers/iotsurvey2018.pdf
[6] https://www.esds.co.in/blog/cloud-computing-iot/#sthash.7YBHCDZx.dpbs
[7] https://stonefly.com/blog/role-cloud-computing-internet-things
[8] https://dzone.com/articles/10-cloud-platforms-for-internet-of-things-iot
[9] https://analyticstraining.com/how-cloud-computing-closely-relates-to-iot/