Towards Cloud Sensor Integration based on Fog Computing for the Internet of Things

Mridul, Rohit Vats, Mr. Rajesh Pandey,
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- mridul@shobhituniversity.ac.in, rohit.vats@shobhituniversity.ac.in, rajesh@shobhituniversity.ac.in

ABSTRACT: The Internet of Things (IoT) is a network of interconnected devices that allows for the sensing and monitoring of processes. In specifically, a Wireless Sensor Network (WSN) is created by connecting identifying devices to the internet, such as smart sensors, embedded CPUs, and low-power radios, through a gateway that connects WSN to the internet. To deal with the enormous quantity of data produced by devices in an IoT context, cloud infrastructure offers Sensing as a Service (SeaaS), which allows sensor data to be made accessible in cloud architecture for sensing and monitoring environmental conditions. The amount, diversity, and velocity of data generated by the IoT are unsuitable for today's cloud architectures. To deal with the amount, diversity, and velocity of IoT data, a new computing paradigm is required. In this article, we looked at several common Sensor Network applications that use cloud computing as a backbone, with a focus on fog computing to overcome some of cloud computing administration problems and to handle time-sensitive data. Because cloud computing offers a wide range of applications, platforms, and infrastructure over the Internet, it can be used in conjunction with sensor networks and fog computing in applications such as environmental monitoring, weather forecasting, transportation, healthcare, and military applications, among others.

KEYWORDS—*WSN, Cloud Computing, Fog Computing, Csaas, Internet of Things.*

1. INTRODUCTION

As more gadgets and sensors become linked to the internet, the Internet of Things (IoT) is becoming a hot subject. By 2020, several organizations expect billions of gadgets to be linked to the internet. By 2018, these gadgets and sensors will produce 403 zettabytes of data each year. The administration of these devices, networks, and produced data is critical in this fast-paced environment. Industry and academics must handle these linked devices since the administration and provisioning of such sensor devices and data offers up new commercial possibilities and poses new difficulties. The user's ability to construct their own IOT systems is limited due to the large investment and high maintenance costs of sensor networks. Due to advancements in the fields of ubiquitous computing and wireless sensor networks, the boundaries between the physical and digital worlds are becoming more blurred nowadays. Communication between sensor nodes over the Internet is often a difficult problem. As a result, integrating sensor networks with the Internet makes a lot of sense. At the same time, sensor network data should be accessible at any time and from any location. It may be difficult to give addresses to large numbers of sensor nodes; as a result, sensor nodes may not be able to connect to the internet alone and may be inefficient in terms of computation and storage [1] .

Cloud computing may be a superior option for resolving the issue. We can combine cloud computing with sensor networks to address the issue of limited calculation power and storage capacity since cloud computing offers massive computing power and storage. The cloud is linked with the sensor database system to offer a database for the cloud sensor network. Cloud computing may be used to alleviate WSN's compute limitation. WSN implementation is provider-specific, which means that each provider sets their own standard. Cloud is also linked to WSN to offer a single platform for data exchange and processing. The amount, diversity, and velocity of data generated by the IoT are unsuitable for today's cloud architectures. The current method, which involves transferring all data from the network edge to the data center for processing, adds delay to the system. The bandwidth capacity is also increased by traffic from thousands of devices. Fog Computing is a novel computing paradigm for dealing with the amount, diversity, and velocity of [2] IoT data. Fog computing may be integrated into the sensor-cloud architecture to mitigate the disadvantages of cloud computing. The fog brings the cloud closer to the objects that generate and act on IoT data, reducing latency by processing IoT data close to where it is gathered. It offloads terabytes of network traffic off the main network, reducing bandwidth capacity while keeping critical data safe inside the network. The following is a breakdown of the paper's structure: The first section discusses the development of different efficient computing paradigms in the Internet of Things. The second section gives an overview of cloud and fog computing. by the many gadgets that surround us. The Internet of Things (IoT) is created by the deployment of various devices in a communicating-actuating network, in which sensors and actuators blend in seamlessly with the world around us, and data is exchanged across platforms to build a common operational picture.

Internet of Things (IoT) is described as the sensing, identification, and transmission of object-specific data. Depending on the kind of sensors, the information is the detected data linked to temperature, direction, motion, vibration, acceleration, humidity, chemical changes in the air, and so on. A sensor network is made up of a large number of these sensors that are all linked wirelessly. These sensor networks may be used for a wide range of purposes. Natural-disaster prediction, industrial applications, water-scarcity monitoring, smart homes design, medical applications, agricultural applications, intelligent transport system design, smart-cities design, smart metering and monitoring, and smart security are just a few of the applications mentioned in .A wireless sensor network (WSN) is made up of geographically dispersed autonomous sensors that work together to monitor environmental and physical variables including sound, vibration, temperature, pressure, pollution, and mobility. Military uses like as battlefield monitoring prompted the creation of WSN. They are currently utilized in a variety of civilian and industrial applications, including industrial process management and monitoring, environmental and habitat monitoring, machine health monitoring, home automation, healthcare applications, and traffic [3] control, to name a few. In a WSN, each node is generally outfitted with a radio transceiver, a tiny microcontroller, or other wireless communications device, as well as an energy supply, which is commonly a battery.

Sensor node size and cost restrictions result in resource allocation rules for memory, energy, speed, and bandwidth Sensing, processing (including hardware, software, and algorithms), and communication technologies are all required for the development of WSN. As a result, WSN research has been driven by both combined and individual improvements in each of these areas. Communication paradigm: Individual node Identifiers (IDs) are unimportant in comparison to conventional communication networks. WSNs, on the other hand, are data-centric, which means that communication should be limited to nodes in a certain area or with specific data content. Application-specific: WSN is used to complete a specific job. Dynamic nature: Due to the severe operating circumstances in most WSNs, node platforms are prone to errors. Due to node faults, unreliable and simple modulations, node mobility, and environmental interferences, communication connections between nodes are unstable. Scale and density: When compared to other wireless networks [4] WSNs may have a large number of nodes. Furthermore, the node density may be increased. Physical constraints: A typical WSN node is modest in size and powered by batteries. This means that nodes have the bare minimum of communication, compute, and memory resources. Deployment: In large-scale WSNs, node deployment is haphazard, and maintenance and replacement are impractical. However, the deployed WSN's needs and applications may change, necessitating runtime reconfiguration and reprogramming. Longevity: The nodes are fueled by batteries or scavenged energy from the environment and their upkeep is tough. As a result, in the installation and design of WSN platforms, applications, and protocols, energy conservation and load balancing must be considered. Scalability: WSNs usually have a large number of nodes. As a result, WSN protocols must cope with very large node densities and numbers. Actual-time: Wireless sensor networks (WSNs) are intimately linked to the real world. As a result, WSNs have tight time restrictions for processing, sensing, and communication. Security: Security is critical in WSNs, particularly in security, health care, and military applications. The majority of the apps transmit data that is private or sensitive [5].

2. DISCUSSION

Cloud computing has emerged as the computing paradigm of the future. The National Institute of Standards and Technology (NIST) in the United States defines cloud computing as follows: Cloud computing is a paradigm for providing on-demand network access to a shared pool of customizable computing resources (e.g., networks, servers, storage applications, and services) that may be quickly provided and released with little administrative effort or service provider involvement .Cloud computing enables systems and users to access Platform as a Service (PaaS) (e.g. operating systems), Infrastructure as a Service (Iasi) (e.g. storages and servers), and Software as a Service (SAAS) (e.g. application level programs) and other services at a very low cost, which are provided by several cloud providers (e.g., Amazon, Google, and Microsoft) on a pay-per-use basis. Because the cloud has a lot of processing power and storage, it's a good idea to use it. We can combine it with sensor networks to address the issue of limited computing power and storage capacity, as demonstrated in International Journal of Computer Science and Engineering Communications, Volume.5, Issue.6 (2017): The following are the characteristics of cloud computing:

On-demand self-service: A customer may provide computer resources on demand, such as server time and network storage, without needing human contact with each service provider. Broad network access: Capabilities are accessible over the network and accessed through standard methods that allow heterogeneous thin and thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) to access them. Resource pooling: Using a multi-tenant approach, the provider's computing resources are pooled to serve many customers, with various physical and virtual resources dynamically allocated and reassigned based on demand. The client has no control or knowledge of the precise location of the supplied resources, but may be able to define location at a higher level of abstraction (e.g., country, state or datacenter). Storage, computation, memory, and network bandwidth are examples of resources. Rapid elasticity: Capabilities may be supplied and released elastically, in certain instances automatically, to scale outward and inward in response to demand. To the user, provisioning capabilities frequently seem to be limitless, and they may be used in any amount at any time. Measured service: Cloud systems employ a metering capability at some level of abstraction suitable to the kind of service to automatically manage and optimize resource usage (e.g., storage, processing, bandwidth and active user accounts). Resource consumption may be tracked, managed, and reported, giving both the supplier and the customer more transparency. Fog computing or fog networking, also known as fogging, is an architecture that uses one or more collaborative end-user clients or near-user edge devices to perform a significant amount of storage (rather than being stored primarily in cloud data centers), communication (rather than being routed over the internet backbone), control, configuration, measurement, and management (rather than being stored primarily in cloud data centers) [6]. By 2020, sensors will account for 40% of all data generated on the planet. Only in the past two years has 90 percent of the world's data been created. Every day, 2.5 quintillion bytes of data are produced. By 2020, the total cost of IoT devices will be $1.7 trillion. By 2020, there will be 250 million linked cars on the road globally. IoT devices will number in the billions. The quantity of information produced by IoT devices is enormous. Fog computing is not a replacement for cloud computing; rather, it is utilized to improve the efficiency of sensor-cloud infrastructure, as illustrated in and its architectural representation. The present cloud model's capacity to meet IoT needs is inadequate. Volume, Latency, and Bandwidth are all issues. Cloud sends data to be analyzed and stored, then returns with a command or action. Volume of Data: Around 50 billion gadgets will be connected to the internet by 2020. Every day, billions of gadgets generate Exabytes of data. Every day, the density of devices grows. This quantity of data is too large for the current cloud model to handle. Every day, private businesses, factories, and airline corporations generate massive amounts of data. The current cloud paradigm is incapable of processing this volume of data in a reasonable amount time. Figure 1 Discloses the Present Day Cloud Model [7].

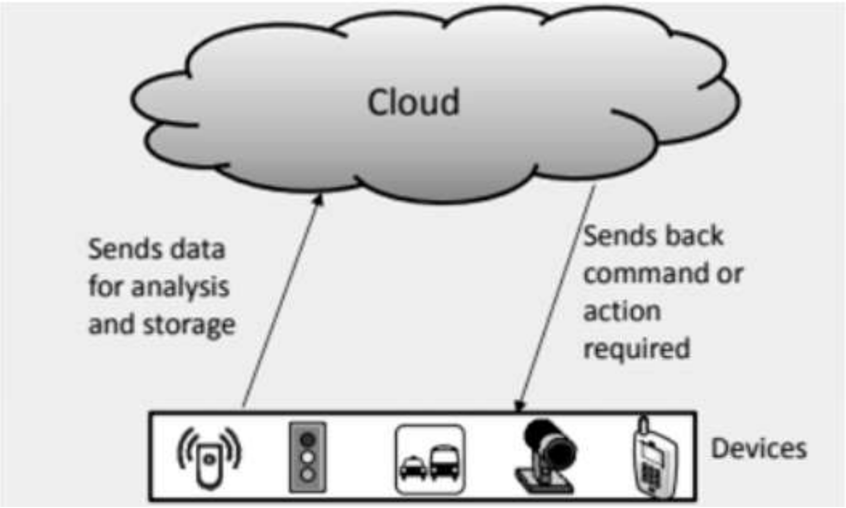
Cloud
Sends data for analysis and storage
Sends back command or action required
Devices

Figure 1: Present Day Cloud Model

As a consequence, data must be filtered; this may be accomplished by storing data using neural networks. Latency is the time it takes a data packet to complete a round trip. It's an essential consideration when dealing with time-sensitive data. If edge devices transmit time-sensitive data to the cloud for processing and then wait for the cloud to take action, it may lead to a slew of undesirable outcomes. By transferring time-sensitive data to the cloud for processing, a millisecond may make a big impact when dealing with time-sensitive data. Consider patient monitoring, where time-sensitive data must be evaluated in a fraction of a second or millisecond. However, if you use a conventional cloud architecture, your latency will rise. Latency = T from device to cloud + T data analysis + T from cloud to device is the formula T stands for time. As a result, by the time the action reaches the gadget, an accident may have happened. Bandwidth: A bitrate of data during transmission is defined as bandwidth. If all of the data produced by IoT devices is transmitted to the cloud for storage and analysis, the amount of data generated by these devices will be enormous. Because there are billions of devices using bandwidth, it takes almost all of it. Managing this kind of traffic will be very difficult. Even IPv6 will not be able to offer service to all of the devices if they all go online. It's possible that the information is private, and the companies don't want to disclose it online. The following are some of the benefits of fog computing: Reduce data latency: Major accidents, machine failure, and other problems may be avoided by taking the correct steps at the right time [6]. A split second of hesitation before making a choice may make all the difference. By evaluating data near to the data source, latency may be minimized. Data security: IoT data must be safeguarded from attackers and secured. Data must be checked 24 hours a day, seven days a week. Before the assault produces significant network damage, proper action should be done. Data accuracy: Data produced by IoT devices is utilized to address real-time problems. Figure 2 DISCLOSES THE. Architecture of Fog-Computing

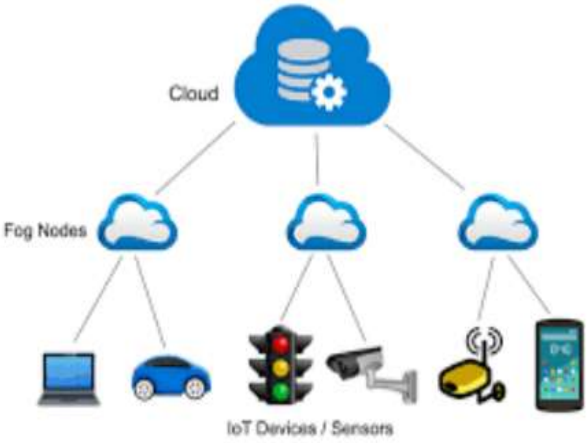

Figure 2: Architecture of Fog-Computing.

The data's integrity and availability must be ensured. Data manipulation and unavailability may be dangerous. Data processing at the appropriate location: Based on sensitivity, data may be classified into three categories: time sensitive data, less time sensitive data, and data that is not time sensitive. Data that is very time sensitive should be evaluated as soon as possible once it is collected. Data that isn't sensitive to time will be examined on the cloud [8].

2.1. WORKING:

Internal and external caching methods may be used to handle dynamic and adaptive data caching processes. This approach guarantees resource efficiency and adaptability to the varying pace of change in the physical environment. It is carried done in order to minimize the energy consumption that results from end-users requesting sensed information through a Web interface. The allocation of physical sensor nodes and virtualization cycle continues as needed. As a result, physical sensor nodes constantly detect and send data to the sensor cloud, resulting in increased energy usage. In practice, the change in environmental conditions may be very gradual in certain instances. Physical sensors' sensed data is unaffected by the gradual change in surroundings. Unnecessary sensing results in energy expenditure in this scenario. I External and Internal Caching Mechanisms: When an end user makes a request, the Internal Cache (IC) decides whether the data should be given directly to the end user or if it is necessary to recache the data from an external cache. External Cache (EC) is used to re-cache data after a certain amount of time has passed. Initially, just a small amount of data is sent to IC in order to process time-sensitive data. The cache-enabled design is compared to the current conventional architecture in Sensor-Cloud Infrastructure Dynamic Optimal Pricing: Because cloud computing offers different levels of service homogeneity , there is no scheme for sensing as a service (SeaaS).

There are two parts to the proposed pricing scheme: pricing ascribed to hardware (pH) and pricing attributed to infrastructure. I Hardware-based pricing (pH): This refers to the use of physical sensor nodes. Infrastructure pricing attribute: This characteristic is concerned with the cost of the virtual sensor node or sense-cloud infrastructure. The suggested scheme's aim is to maximize the profit of the sensor-cloud service provider while also maximizing the profit of the sensor owner and the pleasure of the end-user. Ubiquitous Healthcare Monitoring: Sensor-Clouds can be used for health monitoring by collecting patient health-related data for tracking sep activity pattern, blood sugar, body temperature, and other respiratory conditions using a variety of easily available and most often wearable sensors such as accelerometer sensors, proximity sensors, ambient light and temperature sensors, and so on.Military Applications: Sensor networks are used in the military for a variety of purposes, including monitoring friendly forces, ammunition, and equipment, battlefield surveillance, inspection of opposing forces, targeting, battle damage evaluation, and scouting for nuclear, biological, and chemical attacks, among others.For security reasons, 1771 requires top-level security, which may not be possible to deliver via standard internet connectivity. Agriculture and Irrigation Control System: Sensor-Cloud may be utilized in the agricultural sector to monitor crop fields and conserve them. A field server is being built for this purpose, which includes temperature sensors, camera sensors, air sensors, soil moisture sensors, CO2 concentration sensors, and temperature sensors, among other things. These sensors constantly send field data to the field owner through a Wi-Fi access point, allowing them to monitor the health of their crops. Growers, farmers, and agricultural organizations utilize these sensors to fit their requirements. An infinite number of field valves may be monitored and controlled with this dependable and powerful irrigation control system. Harvesting may also be done with this.

Earth Observation: A sensor grid is created to collect data from many GPS stations, as well as process, analyze, manage, and display the data. This GPS data would then be uploaded to the cloud for effective monitoring, early warning, and decision-making capacity for crucial circumstances such as volcanic eruptions, earthquakes, tsunamis, cyclones, and other natural disasters. Wildlife Monitoring: Sensor-Cloud may also be used to track wildlife sanctuaries, woods, and other places where endangered animals are routinely monitored in real time. Weather Forecasting: Weather forecasting is an application that predicts the condition of the atmosphere at a certain place and time in the future. Data gathering, data assimilation, numerical weather prediction, and forecast presentation are typical components of a weather monitoring and forecasting system. Assimilation is done because the data gathered from these sensors is large and difficult to preserve using conventional database methods. The equations that have been compiled control how the condition of the atmosphere changes [9].

3. CONCLUSION

Previously, most WSN systems that were used in a variety of calculating/monitoring methods were closed, had limited interoperability, were application-specific, and were not expandable. Integrating existing sensors with the cloud, on the other hand, will provide an open, scalable, extendable, interoperable, and re-constructible network of sensors for a variety of applications. We examined the usage and benefits of Sensor-Cloud architecture in the context of various applications using fog computing in this study. The Cloud Sensor architecture makes it possible to store, classify, and analyze sensor data in a manner that makes it timely, commercial, and readily accessible [10].

REFERENCES

[1] H. F. Atlam, R. J. Walters, and G. B. Wills, “Fog computing and the internet of things: A review,” *Big Data and Cognitive Computing*. 2018.

[2] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, “Fog Computing for the Internet of Things: Security and Privacy Issues,” *IEEE Internet Comput.*, 2017.

[3] A. V. Dastjerdi and R. Buyya, “Fog Computing: Helping the Internet of Things Realize Its Potential,” *Computer (Long. Beach. Calif).*, 2016.

[4] M. Aazam, S. Zeadally, and K. A. Harras, “Deploying Fog Computing in Industrial Internet of Things and Industry 4.0,” *IEEE Trans. Ind. Informatics*, 2018.

[5] J. Li, J. Jin, D. Yuan, and H. Zhang, “Virtual Fog: A Virtualization Enabled Fog Computing Framework for Internet of Things,” *IEEE Internet Things J.*, 2018.

[6] L. G. Jaimes, A. Chakeri, and R. Steele, “Localized cooperation for crowdsensing in a fog computing-enabled internet-of-things,” *J. Ambient Intell. Humaniz. Comput.*, 2018.

[7] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, “Fog computing: A platform for internet of things and analytics,” *Stud. Comput. Intell.*, 2014.

[8] R. Oma, S. Nakamura, D. Duolikun, T. Enokido, and M. Takizawa, “An energy-efficient model for fog computing in the Internet of Things (IoT),” *Internet of Things*, 2018.

[9] B. N. B. Ekanayake, M. N. Halgamuge, and A. Syed, “Review: Security and privacy issues of fog computing for the internet of things (iot),” in *Lecture Notes on Data Engineering and Communications Technologies*, 2018.

[10] U. Y. Khan and T. R. Soomro, “Envisioning Internet of Things using Fog computing,” *Int. J. Adv. Comput. Sci. Appl.*, 2018.