Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19278-6

Internet of things technology, research, and challenges: a survey

Amit Kumar Vishwakarma[1] · Soni Chaurasia[2] · Kamal Kumar[3] · Yatindra Nath Singh[4] · Renu Chaurasia[5]

Received: 18 October 2023 / Revised: 13 March 2024 / Accepted: 18 April 2024

Abstract
The world of digitization is growing exponentially; data optimization, security of a network, and energy efficiency are becoming more prominent. The Internet of Things (IoT) is the core technology of modern society. This paper is based on a survey of recent and past technologies used for IoT optimization models, such as IoT with Blockchain, IoT with WSN, IoT with ML, and IoT with big data analysis. Suppose anyone wants to start core research on IoT technologies, research opportunities, challenges, and solutions. In that case, this paper will help me understand all the basics, such as security, interoperability, standards, scalability, complexity, data management, and quality of service (QoS). This paper also discusses some recent technologies and the challenges in implementation. Finally, this paper discusses research possibilities in basic and applied IoT Domains.

Keywords Semantic intelligence · IoT protocol · IoT application · Research possibilities · IoT Platforms · IoT optimization models

✉ Soni Chaurasia
soni28sep@gmail.com

Amit Kumar Vishwakarma
Amit.vishwakarma@ku.ac.ae

Kamal Kumar
kamalkumar@igdtuw.ac.in

Yatindra Nath Singh
ynsingh@iitk.ac.in

Renu Chaurasia
renu.chaurasia14@gmail.com

1 Management science and technology, Khalifa University, Abu Dhabi, UAE

2 Computer science & Engineering, SGT University, Gurugram, India

3 Department of Information Technology, IGDTUW, New Delhi, India

4 Electrical Engineering, IIT Kanpur, Kanpur, India

5 Computer science & Engineering, AIT, Rooma, Kanpur, India

Published online: 02 May 2024

1 Historical background of IoT (Internet of Things

The basic idea of the Internet started around 1970 when DARPA initiated work to build a communication network to share costly computer resources. In modern life, where we are entirely dependent on technology and use many gadgets, the idea of the Internet extended naturally to them, leading to the concept of the Internet of Things (IoT). IoT is expected to be very helpful in home automation, transportation, lifestyle, healthcare, and many other applications. The IoT is changing our lives, making day-to-day processes more efficient. It is changing the work style of almost everyone in the society. Consequently, academics and industry have shown immense interest in this domain. The term IoT has been used for nearly 20 years; earlier, it was known as “Pervasive Computing" or “Embedded Internet." In 1991, Mark Weiser stated in his article - “Computers will weave themselves into the fabric of everyday life until they are indistinguishable from it”; this article can be seen as the first version of ubiquitous computing [1].

Kevin Aston first used the word “Internet of Things," or IoT, in his 1999 presentation to Proctor and Gamble. Later, Kevin co-founded the Auto-ID lab at MIT and used RFID (Radio Frequency Identification) for the first time in supply chain management [2], which can be considered an initial implementation of IoT. The Internet of Things is a system of connected computing devices, electronic machines, mechanical devices, objects, etc. Each one of them provided a unique identifier and had the capability of transferring data over a network, i.e., machine-to-machine communication. IoT systems integrate with existing internet and lead to automation and analytical abilities in the system.

Figure 1 shows the network technology evolution. Network technology has evolved from basic teleprocessing to desktop computers, Ethernet, and WiFi, and now we are going toward 4G and 5G, which will provide faster internet. As shown in Fig. 2, the technological development of IoT increases per year. According to the 2013 report of international data corporation, IoT device connectivity will reach up to 200 billion in 2025 with a 20 trillion USD market [3]. According to the CCS 2020 report, the number of IoT-connected objects will reach up to 250bn by 2025, and it would be nearly 3 percent of total devices worldwide. Both reports predict different numbers, but the order of magnitude is the same.

2 Introduction

There are already a lot of survey papers and basic tutorials about the Internet of Things (IoT). As we searched the Internet for documentation on IoT, we found a lot of papers explaining IoT and its different applications. Seeing it from the research point of view, we found very few papers about the challenges and improvisations that need to be explored in the IoT domain

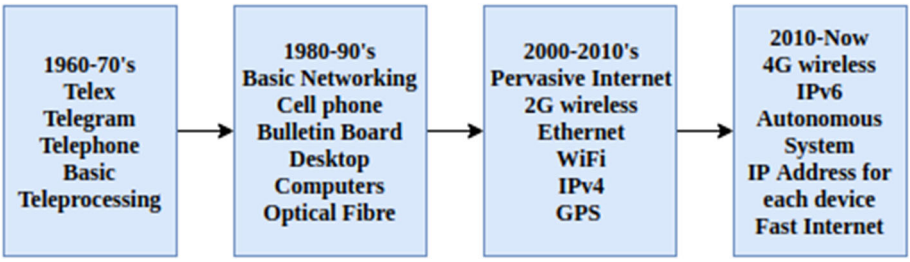

Fig. 1 Network technology evolution

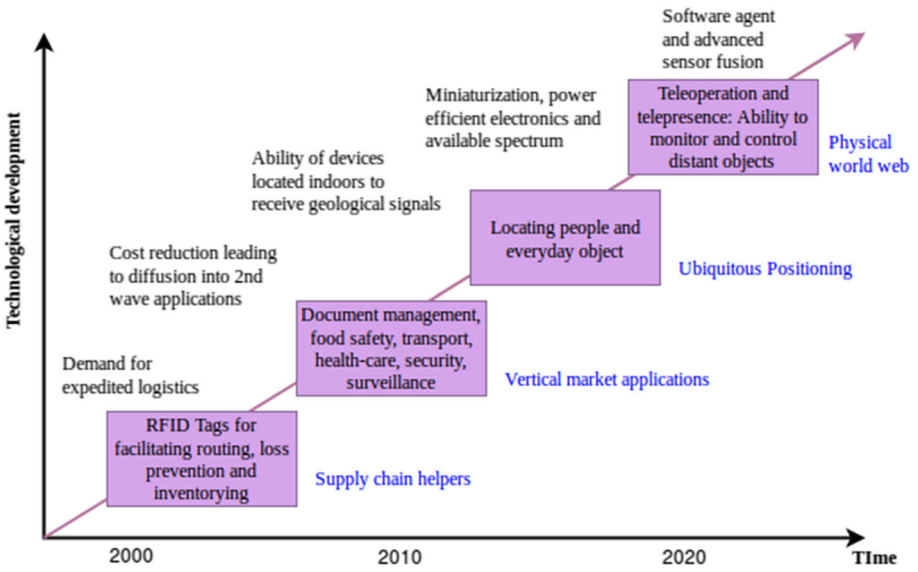

Fig. 2 Technological development of IoT

in different visions, as shown in Fig 3. Therefore. In this paper, the word IoT is mainly used to connect sensors and actuators via the Internet. The definitions of IoT are not unique; various authors have given their definitions. The Oxford Dictionary used the term "Internet of Things" for the first time in August 2013. It describes IoT as "The interconnection via

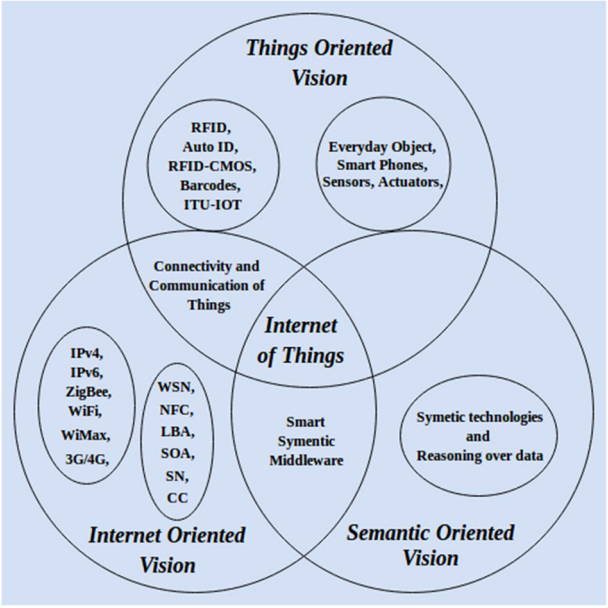

Fig. 3 Different vision of IoT

the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.". ITU defines the IoT as "from any time, anyplace connectivity for anyone, being transformed to connectivity for anything" [4].

A similar definition was given by the European Commission- "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts.".

If one thing can prevent the Internet of Things from transforming the way we live and work, We need more efficient and secure systems that are error-free, resilient, secure [5], and intelligent. It can be done by following the suitable guidelines, according to real-world situations, when deploying the IoT elements as shown in Fig. 4.

A thing in the IoT world can be a human being with a health monitor implant in his body, an animal farm with a chip transponder in each animal, an automobile with sensors that can send an alert about any malfunction in real time, or anything in the world that has been assigned an IP address, and have the ability to transfer some data through the network. However, this paper will focus mainly on non-living things, including computers, intelligent objects, smartphones, actuators, sensors, RFID tags, etc., as shown in Fig. 5.

2.1 Applications of IoT

By the recent survey of McKinsey Global Institute, it is estimated that IoT will have a potential economic impact of 3.9tn-11.1tn USD per year [6, 7] as shown in Fig. 6.

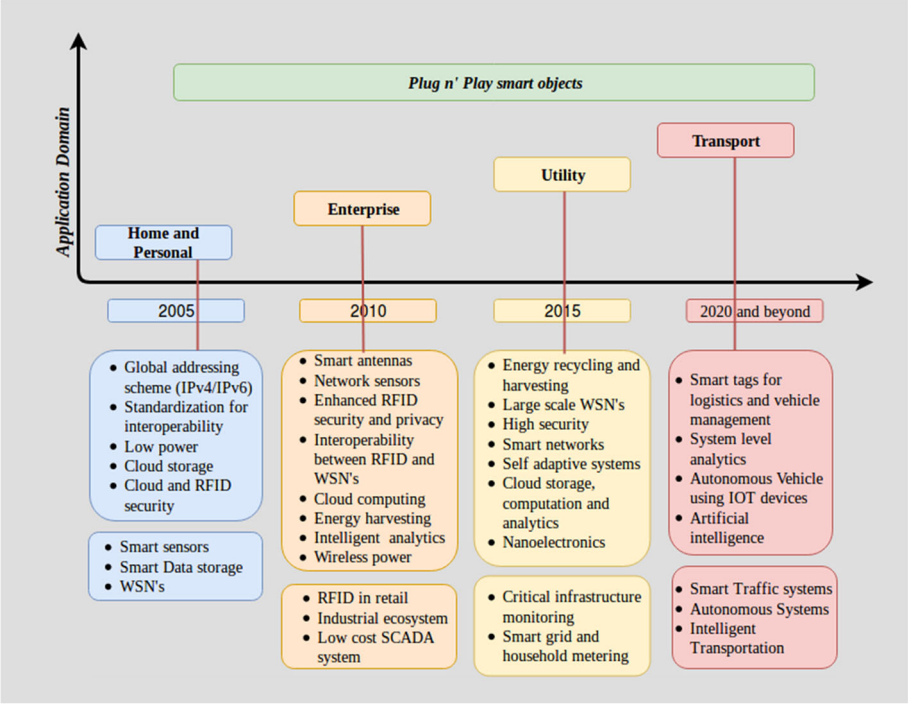

Fig. 4 Technological development of IoT applications

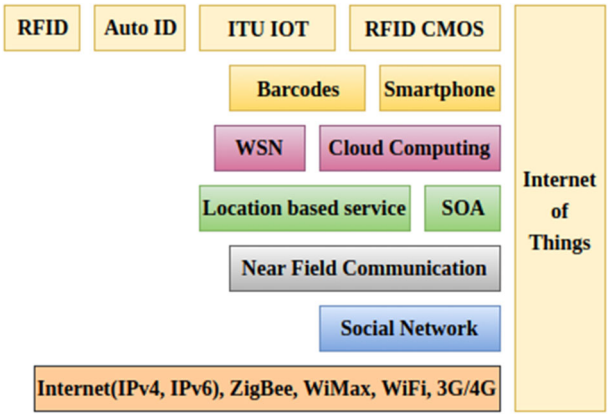

Fig. 5 Key element of IoT

In today's worlds, IoT is playing a crucial role in developing smart applications as shown in Fig. 7. These include the following:

Smart Cities: Smart parking, structural health (to monitor the condition of roads, bridges, buildings), smart roads, urban noise maps, power generation and it's smart distribution, population monitoring and control, smartphone detection, traffic congestion, smart lighting, waste management.

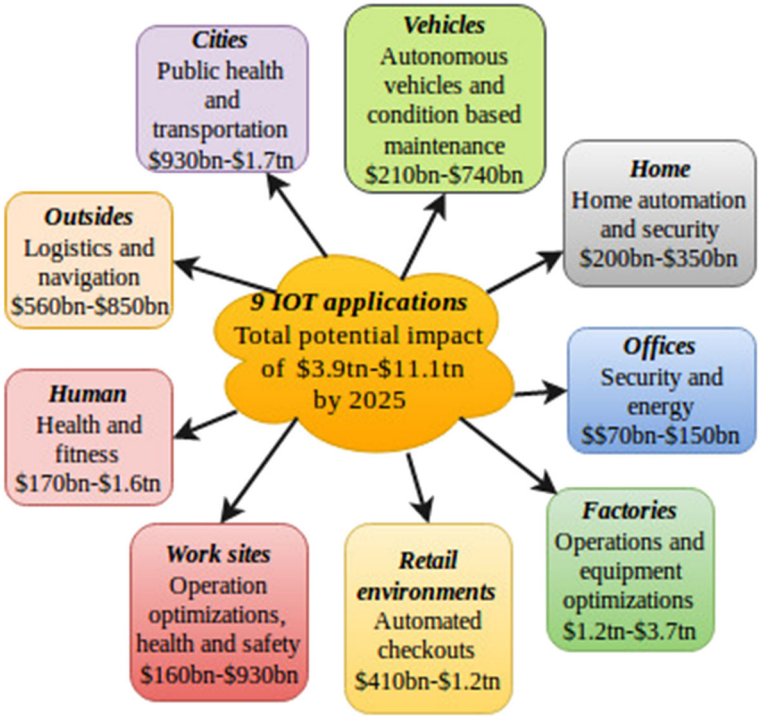

Fig. 6 9 IoT application by McKinsey Global Institute and their global impact

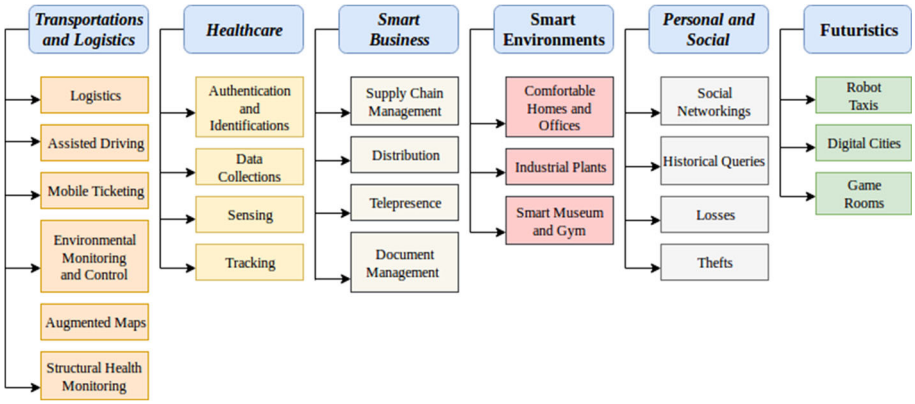

Fig. 7 Applications of IoT

Smart Environment: forest fire detection, air pollution control, snow level monitoring and control, landslide prevention, avalanche prevention, earthquake detection.

Smart water: potable water monitoring, centrally controlled swimming pool, water leakage detection, river flood monitoring, chemical detection in river, pollution level monitoring in sea.

Connected Vehicles: IoT enables connectivity among vehicles (V2V) and between vehicles and infrastructure (V2X), allowing for real-time data exchange.

Infrastructure Monitoring: IoT sensors deployed on bridges, tunnels, and roads monitor structural health, temperature, vibration, and environmental conditions in real-time. Predictive analytics powered by IoT data enable proactive maintenance and minimize disruptions to transportation networks.

Road Safety and Emergency Management: IoT sensors installed along roadways monitor environmental conditions, detect hazards such as potholes or icy patches, and provide real-time alerts to drivers and transportation authorities.

Remote Patient Monitoring: IoT devices such as wearables, biosensors, and medical implants enable continuous monitoring of patients' vital signs, activity levels, and health parameters outside of traditional clinical settings.

Telemedicine and Telehealth: IoT technologies facilitate telemedicine and telehealth services by enabling remote consultations, virtual visits, and digital health monitoring. Telemedicine platforms integrated with IoT devices enhance access to healthcare services, reduce travel burdens, and improve patient outcomes.

An IoT application works in five phases: create phase (collect input data from physical devices through which action will be performed), communicate phase (transfer of data from the devices to control entity), aggregate phase (aggregation of collected data), analyse phase (pattern classification, control and optimization), and act phase (action performed to acheive desired objectives).

2.2 Research question

Here's a list of research questions related to the Internet of Things (IoT) across various domains:

- How can IoT be leveraged to improve energy efficiency and sustainability?

- How can edge computing enhance the performance and efficiency of IoT systems?
- How can machine learning algorithms be optimized for resource-constrained IoT devices?
- What are the most effective strategies for managing security risks in IoT deployments?
- What are the privacy implications of IoT data collection, and how can they be addressed?

2.3 Contribution

The contribution of the paper is as follows based on the research question:

- By using a systematic literature review, IoT has revolutionized how Internet-based systems can be built.
- IoT enables continuous learning for efficient classifications and better decision-making to minimize energy consumption and maximize the network's lifetime.
- We can now use IoT elements to sense and give AI and machine learning engines inputs.

The paper is further organized as follows as shown in Fig. 8. Section I describes the history of IoT, and Section 2 discusses the introduction. Section 3 presents a preliminary section focus on IoT protocols and standards, characteristics of IoT, Technology and platform of IoT, IoT solutions, IOT challenges, and application of IoT; Section 4 describes the Literature survey; Section 5 highlights research possibilities in IoT; finally, Section 6 gives the conclusions.

3 Preliminary

To understand the research presented in this paper, the outlines are preliminary topics relevant to the entire work. A detailed and relevant discussion includes Technology and platform, Protocols and standards, Characteristics of IoT, and IOT challenges. The purpose of this introduction is to provide a concise summary of the significant principles and concepts relating to such topics, with a focus on the ideas that are relevant to the work in the survey and make it easier to comprehend how it contributes to the field and the objectives of this research work.

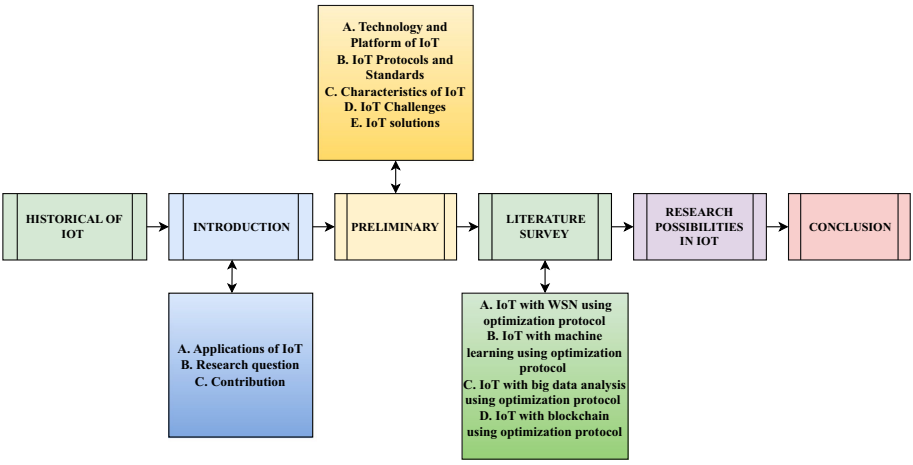

Fig. 8 Organization of research paper

3.1 Technology and platform of IoT

IoT devices can be operated through various platforms, including hardware and software platforms like AWS IoT, ARTIK, Ubidots, Cypress, Marvell, Raspberry Pi, etc.

3.1.1 Artik cloud:

This smart thing cloud is the collaborative effort of Samsung Connect Cloud and ARTIK Cloud [8] as shown in Fig. 9. It is an open data exchange platform for IoT applications that enables new sight and accelerates device interoperability.

It develops its module, cloud onboarding, and network stack to develop any application. It uses Python, Ruby, Objc for IOS and Mac, and Java for Android to develop any application software. MQTT, CoAP, WebSocket, and REST/HELP protocols transfer the data from the device to the ARTIK cloud service.

3.1.2 Autodesk fusion connect:

This cloud-based IoT platform communicates bidirectionally with devices that encapsulate IP-based communication protocol, as shown in Fig. 10.

Fusion Connect provides vendor-specific machine-to-machine IoT solutions using existing protocols CoAP, MQTT, DDS, XMPP, Modbus, HTTP, and UDP. This integrated IoT device technology connects devices and the cloud through data adapters. It can manage 100,000 device messages and 500,000 assets per second.

3.1.3 AWS IoT:

It is an Amazon-based IoT platform as shown in Fig. 11 that provides secure and bidirectional communication between connected devices such as Samart appliances, embedded microcontrollers, adapters, sensors, and the AWS cloud.

It collects and analyzes data on the cloud by using the device gateway, rules engine, message broker, device provisioning services, device shadow service, group registry, security

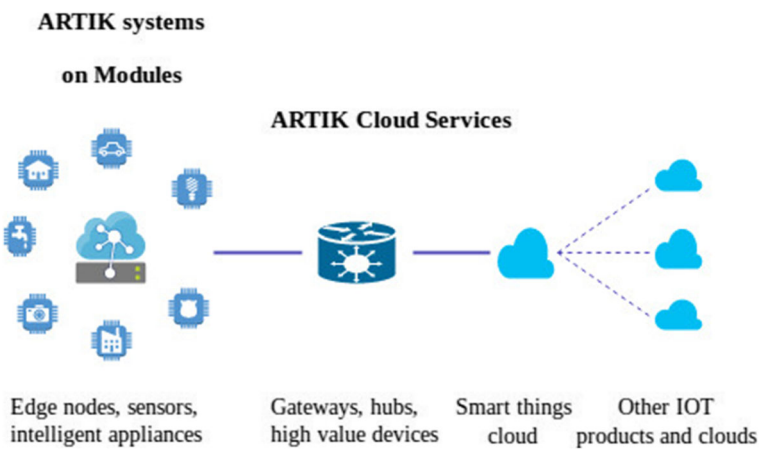

Fig. 9 ARTIK and SmartThings Cloud functionality. [8]

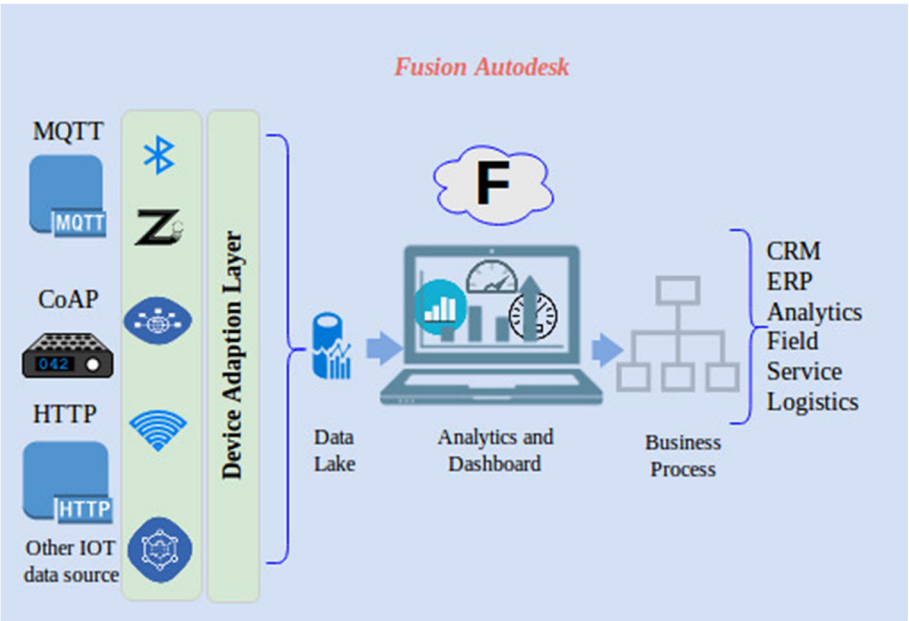

Fig. 10 Fusion connect architecture.[9]

and identity services, etc. AWS IoT will consolidate with AMAZON DynamoDB, Amazon machine learning, Amazon S3, Amazon Kinesis, and Lambda to build IoT applications, analyze data, and manage infrastructure [11]. It supports MQTT, Websockets, and HTTP for managing and analyzing the data.

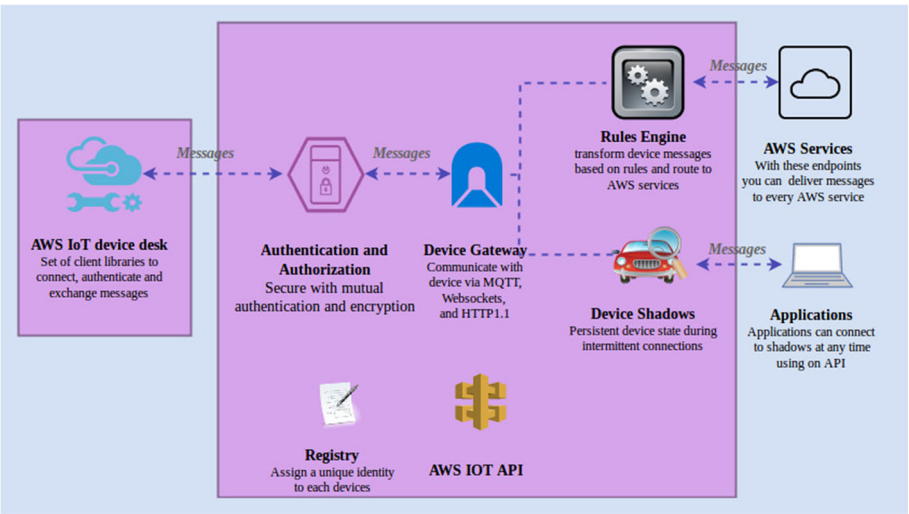

Fig. 11 AWS IoT structure. [10]

3.1.4 GE predix

GE prefix is cloud-based PaaS for industrial IoT, as shown in Fig. 12. It has a unique feature such as M2M communication, asset data management, big data analytics, and distributive computing to connect machines, people data, and other IoT devices [12].

The benefit of the Predix platform includes industrial internet support, central control of devices, quick response to live applications, ease of implementation, flexibility, and rapid development. To reduce development costs, it uses cloud foundry, which supports continuous delivery with the following advantages: easy maintenance, distributed environment, centralized management, and application lifetime management.

3.1.5 Google cloud IoT:

Google cloud services take advantage of Google's legacy of web-scale processing, machine intelligence and analytics, global fiber network, and ultra-low latency [14].

Google Cloud Platform consists of physical hardware devices like virtual machines, virtual resources, and hard disk drives in Google's data center. Services of GC machine learning (ML APIs, cloud ML engines), big data (data analysis, batch and streaming data processing, asynchronous messaging), networking (networks, firewall, and routes), cloud storage, computing, and hosting as shown in Fig. 13.

3.1.6 Microsoft azure IoT suite:

Azure is a comprehensive solution for IoT devices that accelerates time to value and leverage worldwide ecosystems, as shown in Fig. 14. It consolidates cloud services for any IoT application to be deployed, tested, developed, and managed efficiently.

Azure provides preconfigured solutions, dashboard and visualization, workflow and automation, stream processing, predictive analytics, data ingestion command and control, device connectivity, and management [16].

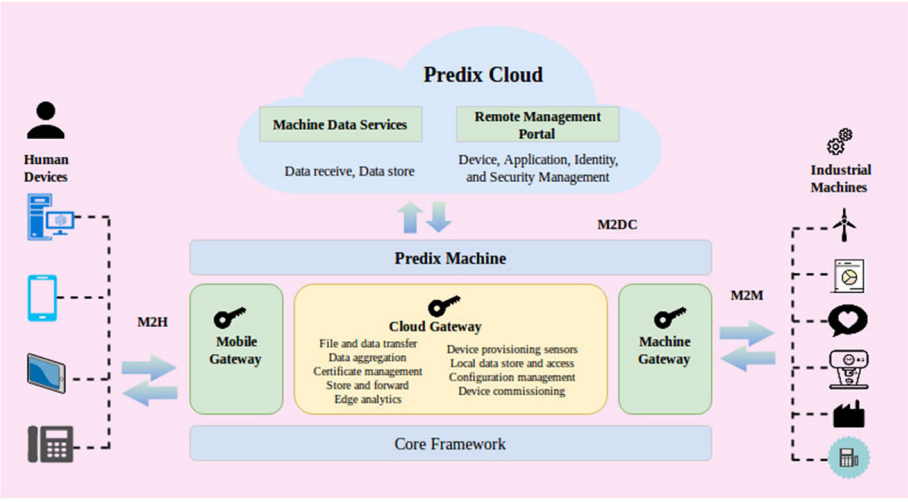

Fig. 12 Predix platform architecture. [13]

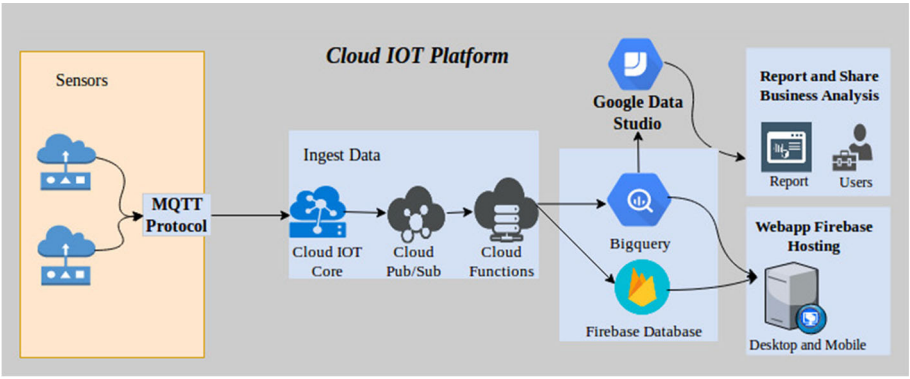

Fig. 13 Google cloud platform architecture. [15]

3.1.7 IBM watson IoT:

This platform for Bluemix gives a functional toolkit that includes powerful application access, device management, and gateway devices, as shown in Fig. 15.

It uses REST and IBM real-time APIs to communicate with the cloud and devices through lightweight MQTT protocol [18]. This protocol gives more impactful devices, meaningful data, and advanced analytics for aggregated data.

The features of this platform include data analytics, information management, better connectivity, and risk management. Watson IoT uses machine learning to automate data and rank it based on priorities assembled by APIs, cognitive capabilities, and Raspberry Pi.

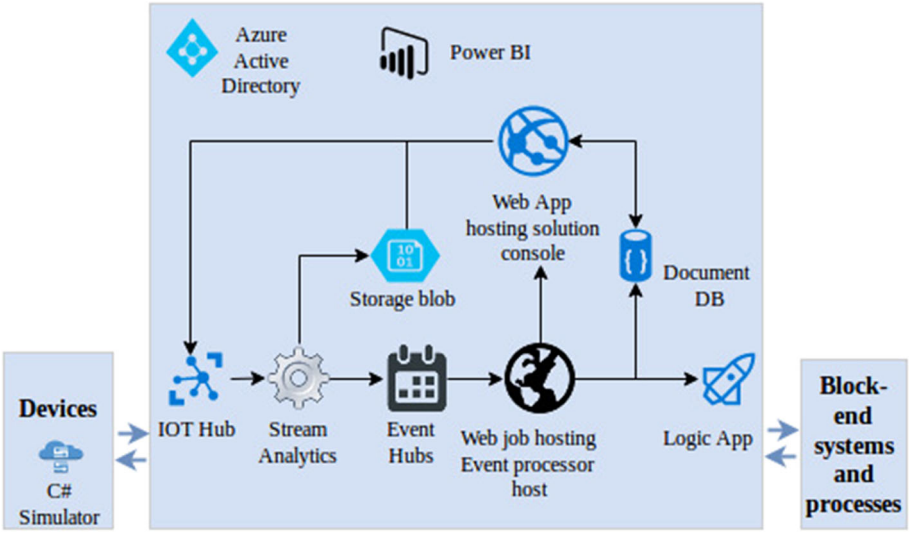

Fig. 14 Azure IoT plateform architecture. [17]

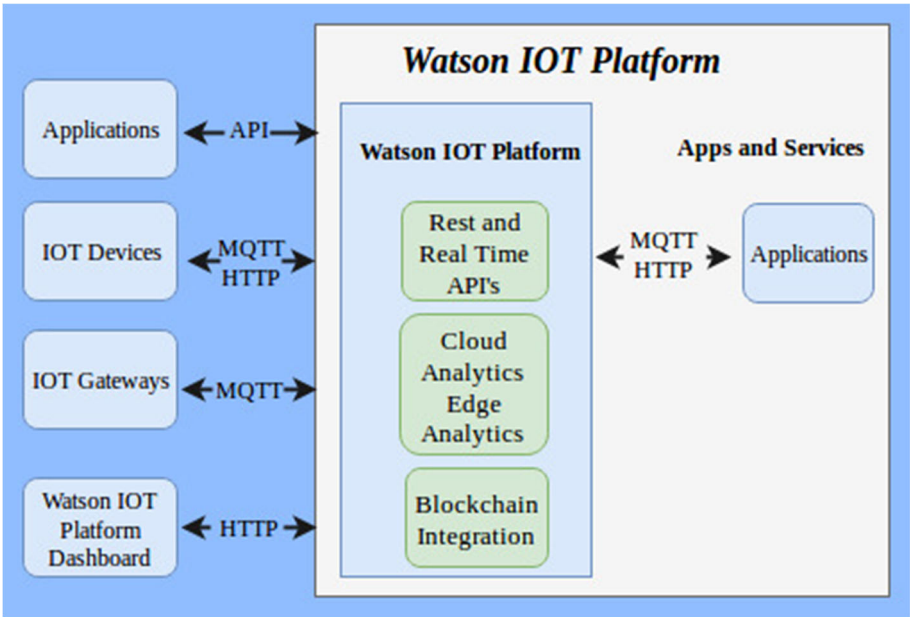

Fig. 15 IBM plateform architecture. [19]

3.2 IoT protocols and standards

The Internet of Things is the interconnection of electronic devices that communicate with each other and pass information by following specific standards and protocols.

3.2.1 IPv6

IPv6 is the latest internet protocol and the successor to traditional IPv4. IETF developed IPv6 to resolve the problem of shortage of addresses. IPv6 has 128-bit address which allows 2^{128} theoretically and $3.4 * 10^{38}$ practical addresses [20]. IPv6 uniquely identifies and locates any computer [21]. IPv6 has several advantages over other network layer protocols, such as expanded addressing capabilities, multicasting, header format simplification, stateless address autoconfiguration, flow labeling capability, network layer security, simplified router processing, mobility, option extensibility, authentication, and privacy capabilities.

3.2.2 6LoWPAN

IPv6 over Low-Power Wireless Personal Area Networks is based on the simple fact that "every electronic device should have its unique IP address resulting in more independent hardware. This protocol provides the capability of sensing communication in wireless technology. The main advantages of 6LoWPAN are QoS guarantees and end-to-end interoperability. The 6LoWPAN group has defined encapsulation and header compression mechanisms between the MAC and Network layers, allowing IPv6 packets to be sent and received over IEEE 802.15.4-based networks. This is done in 6LoWPAN through: 1. Fragmentation; 2. Header compression; 3. IPv6 address auto-configuration; and 4. IPv6 acquaintance exploration [22].

The route-over and the mess-under are the two routing decision algorithms used for 6LoWPAN. The application of IPsec for small devices, service discovery, and secure neighbor discovery are some of the issues worth investigating for 6LoWPAN [23].

3.2.3 UDP

User Datagram Protocol is a connectionless transport protocol, which means after every output, one UDP datagram will be produced by any application, which causes one IP packet to be sent. This protocol uses an IP datagram to send a message between two devices, but there is no provision to guarantee a packet's delivery [24]. UDP protocol is beneficial for real-time applications such as IoT, where the loss of a few packets is tolerable. [25].

3.2.4 QUIC

Quick UDP Internet Connection is an experimental transport layer protocol similar to TCP+TLS+HTTP/2 implemented on UDP. It can be seen as the successor of HTTP/2.0, which provides multiplexed in-order reliable stream transport. QUIC provides security equivalent to SSL/TSL, reducing connection latency and complexity while avoiding network congestion. The main advantages of this protocol are reliable stream support, better congestion avoidance, security and privacy, improved quality, and mobile interface migration. The protocol uses a collision avoidance algorithm to reduce congestion, which is processed at both ends of UDP. QUIC was accepted by IETF in 2016 and became more famous for low latency protocol.

3.2.5 Aeron

Aeron relies efficiently upon IPC messages, UDP multicast, and UDP unicast transport. Aeron protocol allows the exchange of any message via IPC, which helps in IoT connections in which most devices use different protocols. It is a high-performance protocol for IoT applications because it uses a simple binary encoding mechanism to send and receive the data.

3.2.6 CCN

content-centric networking is a next-generation network architecture developed to solve the challenges raised in content distribution, security, mobility, and scalability. The biggest advantage of this protocol is that it can route and deliver any packet to the network by enabling application-neutral caching. CCN protocol is very effective and efficient in content delivery. It has automatic caching, which helps in dynamic memory.

3.2.7 MQTT

Message queuing telemetry transport is a messaging protocol developed by Arlen Nipper of Arcom and Andy Stanford Clark of IBM in 1999, standardized at OASIS in 2013 [27]. It is mainly used for lightweight machine-to-machine communication. This protocol uses a packet-switching mechanism, which sends the data from the client to the server without any queuing. MQTT protocol has a very smart code footprint, low network bandwidth, and is lightweight. This protocol is very suitable for real-time applications because it does not store

any message before transfer; hence, it has better battery utilization. MQTT assures reliability by three QoS levels: 1. Fire and forgot; 2. Delivered at least once; 3. Delivered exactly once [26]. MQTT also supports security; it uses username and password, which can be handled by SSL or independently by MQTT itself. This protocol is straightforward, easy to implement, open, and lightweight.

3.2.8 CoAP

The Constrained Application Protocol is mainly developed for web transfer protocols with constrained networks and nodes. CoAP uses an 8-bit microcontroller with memory elements, constrained network IPv6 rather than 6LoWPAN [28, 29]. The protocol has a throughput of 10 Kbps and a high packet error rate. CoAP used 2 bits of messages as header, which are: 1. Confirmable; 2. Non-Confirmable; 3. Acknowledgment; 4. Reset. CoAP is specially designed for machine-to-machine communication, such as building automation and intelligent energy. In real-time applications, CoAP interfaces with HTTP for the specialized requirement of low overhead, multicast support, and simplicity for the constrained environment[26].

3.2.9 XMPP-IoT

Extensible messaging and presence protocol is an open XML-based protocol developed to provide information about presence and instant messaging. XMPP is extended with new features like file transfer, signaling, and voice-over IP. XMPP used a decentralized network like an email, and this server can be run by anyone and anywhere with an internet connection and domain name [31]. XMPP protocol is an open-source and extensible implementation, so any new functionality can be added to make a more specific application by writing a protocol extension. It has a TTL/SSL security mechanism and does not provide any QoS options, making it unuseful for M2M communication [26].

3.2.10 HTTP2

Hypertext Transfer Protocol Version 2 is a new version of HTTP, released by IETF standard in 2015. It is an application-level protocol for collaborative distributive and hypermedia information systems. While retaining the features of basic HTTP, it adds some new critical features such as prioritization, SSL encryption, binary encoding and header compression, multiplexing, and single persistent connection [32]. HTTP2 protocol is faster, more efficient, and the most secure data transfer in lots of real-time applications, having the feature of connectionless media independent and stateless. This protocol is based on a deprecated open specification networking protocol SPDY, which manipulates web traffic, reduces load latency, and improves web security.

3.2.11 IEEE 802.15.4

The communication protocol specifies media access control and a physical layer for a low-rate wireless personal area network. This protocol uses the feature of 6LoWPAN, which delivers the internet protocol over WPAN. The protocol has a higher communication range, such as wifi. Still, these high-range devices need high power and high cost to connect devices as the IEEE802.15.4 protocol emphasizes low cost and low power consumption [33]. CSMA/CD method makes it suitable for the real-time application and provides secure communication.

This protocol can identify every connected radio and the connection format but is limited to peer-to-peer communication links. This protocol is designed for low-duty cycle communication with a high data rate and low power consumption [38].

3.2.12 Bluetooth

Bluetooth is a short-range, low-cost radio link that enables protected ad-hoc connection. It is available as integrated microchip technology used for personal area networks. Bluetooth networks are token-based, contention-free, multi-access networks based on master-slave technology [30]. It is an ad-hoc network operating in the 2.4GHz band, which allows connection between devices when they are in range. Bluetooth uses the FH-CDMA technique, which helps inherent interference rejection. The Bluetooth technology offers interoperability among different applications by implementing connection-oriented, service discovery, and connectionless links. It is easy to use, widely available, convenient, inexpensive, small, reliable, and consumes low power.

3.2.13 ZigBee

Zigbee is a complete interoperable IoT solution. This protocol uses packet packet-switching techniques for data transfer, providing an easy-to-use architecture for a robust, reliable, and secure wireless network. Zigbee and IEEE802.15.4 both have low data rate wireless networking standards. Still, Zigbee has some unique features such as stochastic addressing, link management, frequency agility, multicasting, many-to-one routing, asymmetric link, fragmentation and reassembly, power management, and security [33]. It is the most popular mesh networking standard for instrumentation, connecting sensors, and control systems. Zigbee is more suitable for low-duty cycle, power, and data rate requirement devices.

3.2.14 WiFi

Wireless fidelity is a physical link layer interface communication protocol that operates at 2.4 GHz for the ISM band and 5 GHz for the U-NII band. WiFi (IEEE 802.11) is a set of physical layers and media access controls for implementing WLAN. WiFi is a half-modulation technology whose frequency band operates and is controlled by IEEE in association with its rules and regulations. It is an open-source wireless network technology that uses radio waves to transfer data. It can suffer interference from Bluetooth devices, cordless telephones, and other devices that produce short-range radio frequencies. WiFi controls susceptibility and interference by using Orthogonal Frequency Division Multiplexing (OFDM) and Direct Sequence Spread Spectrum (DSS) signaling methods. This is an open-access protocol, so most of the standards in the 802.11 series have the issue of threat and security. The key benefit of WiFi application is fast connection establishment, improved transport performance, end-to-end performance, wireless ethernet, extended access, low cost, mobility, and flexibility [34].

3.2.15 WiMAX

Worldwide interoperability for microwave access is wireless radio data transmission technology comes under ETSI hyperMAN and IEEE 802.16 standard designed for broadband

wireless access [37]. WiMAX utilized frequency band of 10GHz - 66GHz and it also fulfills the requirement of Line of Sight (LOS). due to the attenuation of propagated energy, data transmission gets a break, and signal decay occurs. these attenuation problems can be solved by using higher radio waves in frequency bands less than 11GHz [36]. WiMAX has many features such as a service range of 50KM, no LOS operation, quality of service, very high spectrum utilization of 3.8 bit/Hz, true broadband, and high speed (280 Mbps) per base station [44]. The main advantages of this protocol are:

- Advanced IP-based architecture
- Flexible channel bandwidth
- QOS robust control
- Superior performance
- Flexibility
- High throughput
- Cost-effective
- Customer premise availability

3.2.16 NB-IoT

Narrowband IoT is a low-power comprehensive area network radio technology developed for a wide range of devices and services to connect using cellular telecommunication bands. NB-IoT is based on the dominant global cellular system for devices that rely on batteries and need to send a small amount of data. According to Machina Research, 1.5 million devices will be connected to the LPWA network by 2020. Most IoT applications require short-range communication with less data transfer, many connecting devices, indoor coverage, long battery life, and low cost. NB-IoT technology is best suited for such type of application because of data integrity, improved indoor coverage, reduced complexity, improved power efficiency, latency, entity authentication, user identity confidentiality, and mobile equipment identification [35].

3.3 Characteristics of IoT

IoT devices possess some key characteristics as shown in Fig. 16, which are as follows:

3.3.1 Intelligence:

IoT devices are intelligent. Machine learning, pattern recognition, image classification, etc., with the help of a specific set of protocols and hardware like sensors, actuators, RFID, and LED, make IoT devices intelligent. These technologies help IoT devices to make their own decision based on requirements.

3.3.2 Connectivity:

The IoT devices require fast internet to communicate among themselves. As the internet technology changing rapidly, 4G and 5G help devices connectivity

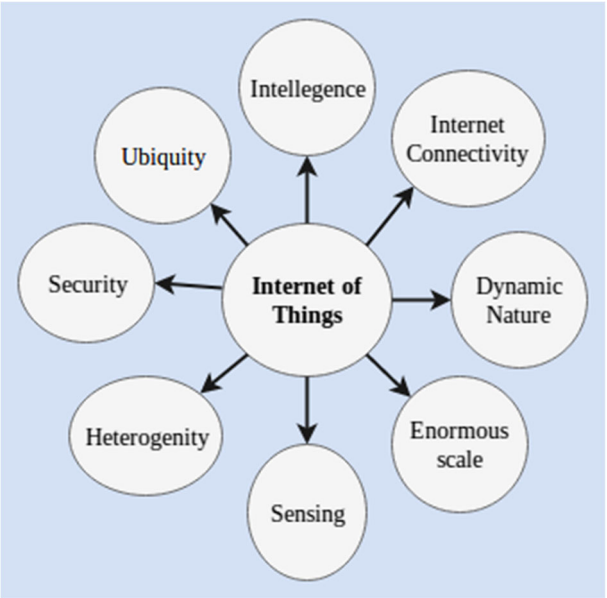

Fig. 16 Characteristics of IoT

3.3.3 Dynamic Nature:

IoT devices should be able to process fast sampled sensory data and should be able to communicate it appropriate entity for the desired purpose.

3.3.4 Enormous scale:

Gartner predicted that the number of internet-connected devices will reach up to 20 billion by 2020. IoT design should scale to such massively large numbers to be useful.

3.3.5 Sensing:

Sensors are the key element in any IoT application; They sense the environment and produce data for future interpretation and necessary action. All IoT elements are supposed to have one one or other kind of sensors. IoT elements should have the capability to connect single or multiple sensors, and sensing the environment simultaneously should be there.

3.3.6 Heterogeneity:

IoT applications require different types of hardware, software, protocols, and standards for building the sensor network. To make a meaningful application, all connected devices should be allowed to have diversity (heterogeneity). Additionally, interoperability, extensibility, modularity, and scalability should be heterogeneously framed.

3.3.7 Security:

As IoT devices gain popularity, the chances of exploiting their vulnerability also increase. The data transfer and network connectivity will not be secure because of IoT standards and protocol transparency.

3.4 IoT Challenges

IoT Challenges as shown in Fig. 17 , which are as follows:

3.4.1 Memory constraint

IoT devices use a General Purpose Operating System (GPOS) or Real Time Operating System (RTOS) with limited flash memory and RAM. With limited program memory, developers must optimize their code to minimize its size while retaining functionality. Techniques such as code optimization, code compression, and stripping unnecessary features are used to reduce the memory footprint of IoT firmware. This optimization process often requires trade-offs between functionality, performance, and memory usage.

3.4.2 Context awareness for privacy

Context awareness is crucial for addressing privacy concerns in IoT deployments. By understanding the context in which data is collected, processed, and shared, IoT systems can implement privacy-preserving measures to protect sensitive information.

Fig. 17 IoT Challenges

3.4.3 Digital Device in physical ambient

Communication between the physical environment and processor has grown significantly to measure different types of information. A sensor in the car, human body, or atmosphere has lots of data to send the processor through a wire or wirelessly. Any hacker can attack the system and cause significant damage; protecting these data is the major challenge in IoT applications.

3.4.4 Identification in IoT environment

IoT applications have different types of architectures, patterns, and unpredictable characters, so they need identification for all layers of IoT to communicate with each other. This is the biggest problem, even for the closed and bounded environment and the distributed environment.

3.4.5 Data combination

Combining all data for an application will lead to a complex system, but to make any system effective, it needs centralized management of data. The security of all nodes is not possible at one time, so data needs to be combined. However, it will reduce the security cost but increase the data handling cost at that node.

3.4.6 Human IoT trust relationship

IoT plays a vital role in daily life and is connected with medical equipment, wearable sensors, and human body interface with machines. Trust is the essential component of digital interaction in information and communication technology. As everyone knows, human expectations of technology are infinite. Due to this nature of human beings, they don't trust any devices easily, and it is also one of the biggest problems.

3.4.7 Secret data management

Management of secret data is the conflict between protocols and cryptographic mechanisms. Some small applications may be able to manage these mechanisms, but one data management policy cannot cover the whole application. A policy enforcement mechanism is needed to manage various types of data. Interpretation and translation are required to reconcile the rules series optimally.

3.4.8 Quality of service

The heterogeneous network provides multiple applications simultaneously, which apply enormous traffic of different protocols. There are two classes of applications: elastic (actual parameter with low sampling rate) and inelastic (real-time like traffic or noise monitoring). It needs different QoS for different applications for high and low-resolution videos. Therefore, an optimal QoS is required for each application. It is tough to provide QoS in wireless networks due to bandwidth, sampling rate, and power constraints.

3.4.9 Optimizing routing

Meta-heuristic algorithms can be used to optimize the routing of data in WSNs.

3.4.10 Load balancing

Load balancing techniques can distribute the data traffic evenly across the network.

3.4.11 Fault-tolerance

Failure of SNs is due to physical harm and intervention in the WSN environment. WSNs should keep functioning without being affected by these SN flaws. The capacity to maintain network functionality without interruptions is known as fault tolerance. Hot-spot problem: In meta-heuristic routing, the hot spot problem refers to a situation where a small subset of nodes in the network experiences high traffic load, causing congestion and potentially leading to performance degradation or even network failure.

3.4.12 Data aggregation

Data aggregation techniques can reduce the amount of data transmitted in the network.

Table 1 represents the challenges of IoT.

4 Literature survey

In 2010 Luigi et. al. [39] had predicted the exponential increase in IoT application such that by 2025, it will become "Disruptive Civil Technology." He further argued that IoT would be useful in healthcare, smart city implementation, home automation, industrial automation, logistics, transportation, etc. The issues that need to be addressed include auto-configuration, unique identification, and more efficient sensing and communication. Additionally, database management and lightweight middleware must be addressed without compromising security. It was also emphasized that with more universal and widespread usage, standardization of IoT systems would be needed.

In 2011 Luca et. al. [40] proposed using wireless sensor networks in the Internet of Things. He proposed a non-proprietary solution based on IPv6 called 6LoWPAN, which will allow the connection between the internet and WSN. Both non-IP and IP-based solutions have been proposed for wireless sensor technology, such as ZigBee, Z-wave, Insteon, Wavenis, CoAP, and 6LoWPAN. The author proposed a structure for integrating heterogeneous WSNs and the internet, which was tested for building automation.

In 2012 Daniele et. al. [41] defined the IoT as - i) Interconnection of the internet and smart objects; They also discussed supporting technologies such as M2M communication devices, RFID, sensors, and actuators, and ii) Applications that will be integral to future of businesses and markets. The key features of IoT technology were identified: device heterogeneity, self-decision, tracking and localization capabilities, energy optimization, scalability, data management and semantic interoperability, privacy, and security.

Li da Xu et. al. [42] made a statement based on the status of industries in 2014 - “IoT will revolutionize the society again by providing an opportunity to frame the dynamic industrial application by using the various IoT components and devices like wireless technology,

Table 1 Challenges of IOT

Challenges	Description
Memory Constraint:	Memory constraints in IoT requires a combination of hardware optimization, software optimization, and architectural design considerations. Developers must carefully manage memory resources, prioritize critical tasks, and implement efficient memory management techniques to ensure optimal performance and reliability in memory-constrained IoT deployments.
Context awareness for privacy	Context-aware privacy mechanisms enable IoT systems to adapt to changing circumstances and user preferences while ensuring compliance with privacy regulations and standards.
Digital Device in physical ambient:	In the context of the Internet of Things (IoT), a digital device in a physical ambient refers to a smart device or sensor that is embedded within a physical environment to collect, monitor, and transmit data about that environment. These devices play a crucial role in enabling the connectivity and intelligence of IoT systems by gathering real-world data and providing insights into various aspects of the physical environment.
Identification in IoT environment:	Identification in an IoT environment refers to the process of uniquely identifying and authenticating devices, users, or entities within an IoT ecosystem . Identification is crucial for ensuring IoT deployments' security, integrity, and trustworthiness.
Data combination:	Data combination in IoT involves merging and integrating data from various IoT devices, sensors, and sources to create a unified and comprehensive dataset for analysis, decision-making, and automation.
Secure setup and configuration	Securing the setup and configuration of IoT devices is crucial to prevent unauthorized access, data breaches, and other security threats.
Human IoT trust relationship:	In the context of IoT, where devices collect, process, and exchange data autonomously, establishing trust between humans and IoT systems is essential for ensuring user acceptance, adoption, and confidence in IoT technologies.
Quality of Service:	Quality of Service (QoS) in IoT refers to the ability of IoT systems and networks to meet specific performance requirements, such as reliability, availability, latency, throughput, and scalability, to satisfy the needs of applications and users. QoS is essential for ensuring IoT deployments deliver the desired service and performance, particularly in applications where real-time data processing, responsiveness, and reliability are critical. Monitoring, measuring, and optimizing QoS metrics are essential for continuously improving the performance and efficiency of IoT systems and driving innovation in IoT applications and services.
Optimizing routing	Optimizing routing in IoT involves designing and managing efficient communication paths for data transmission between IoT devices, gateways, and backend systems. Optimized routing helps minimize latency, conserve bandwidth, reduce energy consumption, and improve overall network performance in IoT deployments.
Load balancing	Load balancing in IoT involves distributing data processing and communication tasks across multiple computing resources, such as IoT devices, gateways, and cloud servers, to optimize resource utilization, improve performance, and ensure scalability in IoT deployments. Load balancing helps prevent resource bottlenecks, minimize latency, and enhance reliability by efficiently managing workload distribution across the IoT ecosystem.

Table 1 continued

Challenges	Description
Fault-tolerance	Fault tolerance in IoT refers to the ability of IoT systems and devices to continue operating reliably and effectively in the presence of faults, failures, or disruptions. Ensuring fault tolerance is essential for maintaining IoT deployments' availability, reliability, and performance, particularly in mission-critical applications where downtime or data loss can have significant consequences.
Data aggregation	Data aggregation in IoT involves collecting, combining, and summarizing raw data from multiple IoT devices, sensors, or sources to generate meaningful insights, reduce data volume, and optimize data transmission and storage. Aggregating data at various levels of the IoT architecture helps streamline data processing, analysis, and decision-making while reducing bandwidth usage and resource consumption.

RFID, sensor devices and mobile devices". So far, IoT has been extensively used in manufacturing, logistics, pharmaceuticals, and retail. According to the author, the main application of IoT will be in the healthcare industry (remote monitoring, drug tracking, hospital asset tracking, diagnosis, recovery, smart device connectivity, and data management). Other industries that will use IoT are the Food Supply Chain (Public food safety, operational efficiency, quality management, etc.), mining industries (safety of workers, disaster forecasting, early disease detection), transportation and logistics (automotive pilot, security, theft protection, reducing unauthorized access), firefighting (detection of fire, early warning, environmental monitoring). The main research challenges in the industries are technical competence, standardization, privacy protection, and information security.

Allesio Botta et. al. [43] proposed the integration of IoT and cloud computing and called it the CloudIoT paradigm. According to the National Institute of Standard and Technologies (NIST): "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) which can be rapidly provisioned and released with minimal management effort or service provider intervention". They said integrating IoT and the Cloud will lead to new applications and interesting research issues. The main advantages of this integration are low-cost Communication, Computation, and Storage. However, the problems of standardization, power and energy efficiency, extensive data handling, privacy, security, etc., need to be addressed.

4.1 IoT with WSN using optimization protocol

An energy-efficient fuzzy-based unequal clustering with a sleep scheduling (EFUCSS) [45] protocol for IoT that uses WSN for clustering, scheduling, and data transmission. It increases the network lifetime and minimizes network energy consumption by using Fuzzy C-mean in unequal clusters to balance the energy uses. The CH selection is based on the gateway's (GW) distance, remaining energy, and fuzzy variables (FV). The FV output varies as input by using the Mamdani technique. The connected nodes employ the sleep scheduling approach to minimize the number of sent nodes.

ACRA protocol's [46] main objective is to maximize the adaptivity of priority messages traveling in a network using dynamic CH selection. The dynamic CH selection is based on a Dragonfly algorithm with opportunistic routing that uses a fitness function. Distance, node

density, and residual energy are parameters for fitness functions. Global Search Optimisation (GSO) and Local Search Optimisation (LSO) form the foundation of DA. The primary goal of LSO is to provide a solution for situations where a node is rapidly dying, its energy is being wasted, and it becomes caught in a loop. Consequently, a deadlock happens to resolve the deadlock issue by LSO. Non-Adaptive Routing (NAR) is the cause of livelock issues in IoT assist WSN. Data is delivered over the fixed path in NAR. ARCA utilizes an adaptive routing method to address this issue. GSO is the foundation of the adaptive routing method. It conveys priority data to BS via the best path and fine-tunes the path selection. The optimally selected or optimal CH sends priority data to BS by adaptive routing. MBASE [47] Base station (BS) placement is essential in enabling flawless coverage of present and emerging IoT (Internet of things) to assist WSN. The position of a BS in a sensor network significantly impacts its network's lifetime. This challenge is tough for a multi-hop communication network since it is coupled with data routing.

An optimized Orphan-LEACH (O-LEACH) [48] based on cluster formation can reduce energy consumption and increase network lifetime. The orphan node has enough energy and will try to cover the entire network. With very high connectivity rates and the fewest number of orphaned nodes, the O-LEACH protocol covers the whole network. A hybrid optimization that combines particle swarm optimization with Lightning Search Algorithm (PSA-LSA) and simulated annealing with LSA (SA-LSA). These methods efficiently control the CH election, resulting in optimal path routing and energy consumption minimization, which prolongs the WSN's lifespan.

An effective IWSN model can be achieved with the help of the Adaptive Coverage and Connectivity (ACC) mechanism [49]. It uses two fundamental methodologies: the first assures the coverage rate and offers the best coverage to all target items based on a mathematical model. The network's energy usage and connection are addressed by the second technique.

An oppositional artificial bee colony (OABC)–based routing algorithm is used in the CBR-ICWSN technique [50] to identify the best possible paths. To efficiently choose the ideal group of cluster heads (CHs), use a clustering technique based on black widow optimization (BWO). Information-centric networking, or ICN, is one innovative model that can overcome the difficulties of acquiring large amounts of data. The data access method, reliability issues in a mobility event, and maximum delay under multi-hop communication may all be improved by utilizing the ICN design for resource-constrained WSN-enabled IoT networks. A cluster-based routing (CBR) protocol called CBR-ICWSN for information-centric wireless sensor networks (ICWSN) enabled by the Internet of Things.

Table 2 represents IoT with WSN using optimization protocol. and finds research gaps such as hot spot problems, data aggregation, routing, and uneven energy consumption.

4.2 IoT with machine learning using optimization protocol

SHANN [51], a multilayer machine learning method for CRN applications that may be reconfigured. The distributed control system monitors the whole environment and generates CRN reports to make the best decisions when choosing the cluster head, cluster members, and routing path. This perfect pick considers the entirety of CRNs, including their properties, enabling the actual transfer of data. With cluster, threshold, and CRN reconfiguration depending on network constraints, employing three phases with machine learning (ML) further improves this choice. Furthermore, the SHO technique was abused when adjusting the ANN model's hyperparameters. One benefit is that a controller CRN network can be used to its fullest potential, enabling optimal data transmission at a higher network level. With periodic reconfiguration, this cross-cutting technique enables coordination between layers during

Table 2 IoT with WSN using optimization protocol

Protocol	Targeted attributes	Decision-making approach for optimization	Finding
EFUCSS [45]	Reducing the number of transmitting nodes, thus saving energy	Fuzzy C-Means for clustering and sleep scheduling approach for routing	network stability, network lifetime, and energy efficiency,
ACRA [46]	Remove Hotspot (Deadlock) and fault tolerance (Livelock) issues	Dragonfly algorithm clubbed with opportunistic routing	Cover large region, network lifetime, and energy efficiency,
MBASE [47]	Remove network overhead issue and fault tolerance issues	Forwarder Node (FN) selection and using meta-heuristic-based opportunistic routing	PDR, MSR, Throughput, and AEC
Hybrid PSO-LSA algorithm [48]	Resolving multimodal optimization problems, poor accuracy of the solution, premature convergence, and easy fall into local optimum	Hybrid optimization that combines particle swarm optimization with Lightning Search Algorithm (PSA-LSA) and simulated annealing with LSA (SA-LSA)	Delay, Average packet loss rate, Average packet loss rate, and network lifetime
Adaptive Coverage and Connectivity (ACC) scheme [49]	Reduce the coverage, connectivity and energy consumption problem,	The improved development of IWSN is facilitated by these multi-objective optimization strategies used appropriately.	AEC, and network lifetime
IoT-enabled cluster-based routing (CBR) protocol for info motion-centric wireless sensor networks (ICWSN), named CBR-ICWSN [50]	Resolve big data gathering	Black widow optimization (BWO) based clustering technique and Oppositional artificial bee colony (OABC) based routing process for optimal selection of paths	AEC, and network lifetime

the routing process. By working together, the dispersed controllers optimize the processes during the settlement phase, which leads to the usage of the routing paths.

The fuzzily grouping nodes [52] simulate the separations between the sensor and CH and the energy left in each sensor node. Integrating time series and machine learning methods to forecast energy usage, then using the output to optimize the choice of CH according to the HTOA algorithm. The ACO algorithm sends Packets from CH to sink via multi-hop routing. Lowering computational burden, load balancing, energy usage, network longevity, and data packet transmission latency.

Inspired by deep reinforcement learning's diverse applications, the Intelligent Congestion Control Algorithm (iCoCoA) [53] is designed for constraint devices. To determine the optimal Retransmission Timeout to reduce congestion in dynamic situations, the iCoCoA learns from the different network properties. In addition, it optimizes energy consumption, throughput, and avoidable, frequent retransmissions compared to the current models.

Table 3 represents IoT with ML using optimization protocol. and finds research gaps such as resource utilization, data quality, and energy optimization.

4.3 IoT with Big data analysis using optimization protocol

To solve a PdM problem with an actual industrial use case that involves sophisticated processing and monitoring equipment, a Decision Support System (DSS) [54]. The fundamentals of DSS include cloud storage, data analysis, feature extraction, data collecting, and predictive modeling. A feature extraction method and machine learning prediction model driven by particular subjects gathered from the production system's upper and lower tiers. By directly assisting the maintainer/operator, the cloud-based architecture's integration of the ML technique allows for optimizing the machining quality procedures. These benefits could help manufacturers cut service costs by increasing uptime and productivity while optimizing maintenance plans and providing real-time alerts regarding operational concerns.

An edge-cloud computing optimized significant data analytics architecture for the Internet of Things utilizing machine learning [55]. A framework that enables data analytics at the edge, comprising effective preprocessing to prepare the data for speedy processing and precise prediction, effective concurrent edge storage methods, and parameter selection for modules impacting the distributed files for edge data availability. Using cloud technology, an edge intelligence module effectively processes and stores large amounts of data at the network's edges. MapReduce is an optimized parallel technique for data injection and storage. The cluster is efficiently managed using an optimized yet another resource negotiator (YARN), and model parallelism is achieved through an upgraded weighted backpropagation (BP) technique.

Using wireless relay cooperative transmission technology [56], the Big data analysis of the Internet of Things (IoT) system, data energy collecting, and information transmission system model are built. This enhances the model's performance, including energy efficiency, optimization, and accuracy. In energy efficiency analysis, information transmission capacity grows as the power split factor does. A multi-hop path can lower the bit error rate (BER) and outage probability (OP).

Particle Swarm Optimisation (PSO) is used in the Internet of Things (IoT) clustering routing technique to determine the optimal amount of clusters [57]. The fitness function is determined by the distance between clusters, node spacing, and remaining energy of sensor nodes. By preventing particles from entering local optima, the two-way chaotic search establishes both a chaotic search strategy and a reverse learning method. From the querying and

Table 3 IoT with Machine learning using optimization protocol

Protocol	Targeted attributes	Decision-making approach for optimization	Finding
SHANN [51]	Issues concerning road discovery, diversity of resources and mobility	CRN-based cross-layer routing protocol uses Spotted hyena optimizer (SHO) of machine-learning models	Residual energy, the strength of the resistant scalability, and resource
A machine learning-metaheuristic-enhanced energy-sensitive routing framework for the internet of things [52]	Solve NP-hard energy optimization	For data routing in IoT based on Machine Learning (ML) and metaheuristic HTOA (Heat Transfer Optimizer). For selection of optimal cluster heads (CH) fuzzy clustering, predicting energy consumption based on Support Vector Regression (SVR) and time series techniques, and from CH to the sink using Ant Colony Optimization (ACO) algorithm	Energy consumption, end-to-end delay (EtED), load balancing, overhead, and network lifetime
Intelligent congestion control algorithm (iCoCoA) [53]	support for congestion control mechanism	CoAP using deep reinforcement learning	Throughput, PDR, Energy efficiency, and reduced number of retransmissions

data writing standpoint, the Hbase particle swarm optimization technique enhances Hbase's performance.

Table 4 represents IoT with Big data analysis using optimization protocol. It also finds research gaps in data processing and storage, data analysis, convergence, and security.

4.4 IoT with blockchain using optimization protocol

A layered hierarchical design that enables the deployment of a dispersed yet practical Blockchain-enabled SDN-IoT framework [58], ensuring safe network communication through the discovery and isolation of rouge switches and effective cluster-head selection. In addition, the controller cluster's consistency is preserved, the Blockchain-enabled rules are monitored, and the regulations implemented in the switches are recorded.

Three processes are involved in creating a poEM model [59]: cold startup, data collection, and model training. The cold startup of new joining nodes and the cold startup of the BaaS-based IoT system are both included in the cold startup challenge. Secondly, the phase of data collecting consists of the subsequent five steps: acquiring training datasets, generating features, processin2g features, analyzing features, and gathering system logs. In its final form, model training comprises progressive training and a model based on initial training. Efficiency and applicability are increased by using this paradigm.

High-performance IoT protocol with secured management [60] model cope with efficient transmissions of sensitive data on insecure communication systems. It provides high performance for IoT networks and lowers the overheads on network devices. The intelligence of the SDN controller and the addition of data validation increased the security.

As shown in Table 5, represent IoT with blockchain using optimization protocol. It also finds research gaps such as resource consumption, scalability, optimal route, and security.

4.5 Limitations of IoT

Figure 18 shows research repositories cited of WSN is 37%, Blockchain is 18%, Big data analysis is 25%, ML is 25%, and other is 2%. Limitations of IoT in various domains, such as Wireless Sensor Networks (WSN), Blockchain, Machine Learning (ML), and Big Data Analysis, can arise due to technical challenges, scalability issues, security concerns, and regulatory constraints. Here are some limitations specific to each domain:

4.5.1 Wireless Sensor Networks (WSN)

- Limited Energy: WSN nodes are often constrained by limited energy and bandwidth resources, which can restrict data transmission and processing capabilities.
- Communication Constraints: WSN nodes may operate in environments with intermittent connectivity or harsh conditions, leading to communication failures or packet loss.
- Scalability Challenges: Scaling WSN deployments to large networks may pose challenges in managing network congestion, synchronization, and node coordination.

4.5.2 Blockchain

- Scalability Issues: Blockchain networks may face scalability limitations regarding transaction throughput and processing speed, especially as the network grows and transaction volume increases.

Table 4 IoT with big data analysis using optimization protocol

Protocol	Targeted attributes	Decision-making approach for optimization	Finding
Knowledge-based to big data analytic model [54]	Issues concerning data collection, feature extraction, predictive model, cloud storage, and data analysis	Decision Support System (DSS) for solving a PdM task	Optimization of maintenance schedules and cost
IoT-Enabled Big Data Analytics for Edge-Cloud [55]	Issue related to high volume of data storage and processing, data heterogeneity, and processing time	data injection and storage with an optimized MapReduce parallel algorithm and optimized yet another resource negotiator (YARN) is used for efficiently managing the cluster	Communication overhead
Wireless IoT Relay Cooperative Transmission Technology [56]	Enhance power-split factor and information transmission ability	Uses wireless relay cooperative transmission technology to integrate Big data analysis	Energy efficiency, outage probability (OP), and accuracy
IoT cluster routing protocol based on PSO [57]	Convergence Issue resolve	PSO based optimal cluster head routing algorithm	improve the functioning of Hbase from the perspective of data writing and query

Table 5 IoT with blockchain using optimization protocol

Protocol	Targeted attributes	Decision-making approach for optimization	Finding
SmartBlock-SDN [58]	Focused on security, privacy, flexibility, scala ability, and confidentiality	cluster head selection procedure that combines both sorting and swapping techniques,	energy-utilization, end-to-end delay, and throughput
Proof of Evolutionary Model (PoEM) [58]	Issue Low Efficiency, Weak Applicability, Poor Scalability, Unsafety	dynamically joining and exiting the BaaS-based IoT system using Consensus Model Evolution	efficiency and applicability
High-performance IoT protocol with secured management [60]	Issue identification of optimal routes	Optimized Routes Generation for Big Data Management and Secured System Using Blockchaining of IoT Data	network throughput, computing overhead, data delay, response time, and dropped packets

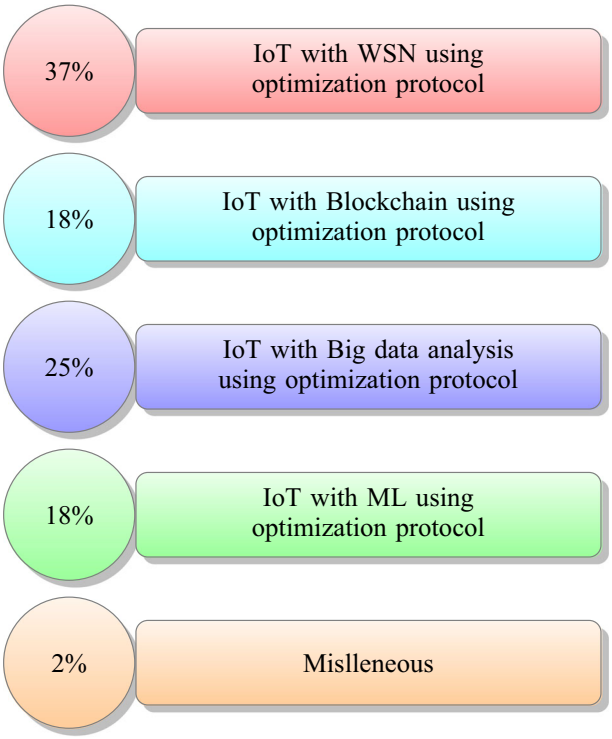

Fig. 18 IoT research repositories

- High Resource Consumption: Blockchain consensus mechanisms, such as proof-of-work (PoW) or proof-of-stake (PoS), can require significant computational resources and energy consumption, leading to scalability and sustainability concerns.
- Latency and Confirmation Times: Blockchain transactions may experience delays in confirmation times and high latency due to network congestion and block propagation times.

4.5.3 Machine Learning (ML)

- Data Quality and Quantity: ML algorithms require large volumes of high-quality data for training, which may be challenging to obtain in IoT environments due to data sparsity, noise, or inaccuracies.
- Model Complexity: ML models with high complexity may require significant computational resources and memory, which may not be feasible for resource-constrained IoT devices.
- Interpretability and Explainability: ML models may lack interpretability and explainability, making it difficult to understand the rationale behind their predictions or decisions, especially in safety-critical applications.

4.5.4 Big data analysis

- Data Privacy and Security: Big data analysis in IoT may raise concerns about data privacy, security, and compliance with regulations such as GDPR. Collecting, storing, and processing large volumes of sensitive data may pose risks of unauthorized access, data breaches, or misuse.
- Data Integration and Interoperability: Integrating heterogeneous data sources from diverse IoT devices and platforms may pose challenges in data interoperability, standardization, and compatibility.
- Processing Complexity: Analyzing large-scale IoT data sets may require distributed computing frameworks, such as Hadoop or Spark, which may introduce complexities in data processing, management, and fault tolerance.

Addressing these limitations requires innovative solutions, interdisciplinary collaborations, technological advancements, standards, and regulatory frameworks. Researchers and practitioners continue to explore novel approaches, such as edge computing, federated learning, differential privacy, and blockchain scalability solutions, to overcome these challenges and unlock the full potential of IoT in diverse applications and domains.

5 Research possibilities in IoT

5.1 SDN-IoT integration-based blockchain model

SDN-based IoT security is a new research topic; very few works have been done in this field. Despite having alluring properties such as agility, flexibility, and dynamism, it opens vulnerabilities after integrating IoT and SDN for real-time applications. Limited switches and central management are SDN's security issues. IoT networks comprise millions of connecting devices, and security threat issues have increased since SDN-IoT integration. SDN has a central management system that causes single-point failure, affecting the whole network. Literature on security issue [61] which is based on an efficient backup mechanism, but the proposed mechanism fails when SDN integrates with IoT. The communication between the controller and gateway generates enormous amounts of data, and security and management of these are other significant challenges. Information Centric Network (ICN) provides users with content rather than a communication channel between devices. Integration of ICN with SDN may be valuable for IoT applications because of SDN-ICN's properties, such as heterogeneity, scalability, and identity management. A role-based security controller architecture that will provide security to SDN-IoT integration [62].

5.2 WSN-IoT based optimized routing and clustering protocol

The existing WSN-IoT technology cannot connect nodes, protocols, standards, security, etc. The evolution of WSN-IoT technology will give massive connectivity, high throughput, ultra-reliable network, ultra-low latency, high coverage for wireless communication, and a secure and trustworthy network [63]. The WSN-IoT network can connect billions of smart devices that can mutually interact and share the data without any human intervention [64].

Narrowband IoT, Network function virtualization, software-defined network, mobile edge computing, millimeter wave, machine type communication, direct device to device, advanced spectrum sharing and interface management, heterogeneous network, wireless network func-

tion virtualization, and WSN-IoT architecture are the key enabling technology for the future WSN-IoT application. Privacy concern and security assurance, heterogeneity, and interoperability [65], scalability and network management [66], energy and spectral efficiency for the device-to-device communication, full-duplex transmission, multiple access techniques for WSN, dense heterogeneous networks are the prime research challenge topics for WSN-IoT applications.

5.3 Big data analytics -IoT based optimization protocol

The generated data in IoT applications are in massive amounts, uncertain provenance, real-time data, and variable structure. The analytic solution to store this variety, velocity, and volume of data is very complex. We need big data solutions for storing and analyzing this data because traditional solutions such as SQL-queried relational database management systems (RDBMS) are unsuitable. Alamri et al. and Botta et al. given the solution to complex analysis and long-term storage in terms of IoT cloud [43, 67], but handling this vast amount of data is still a big challenge. Some solutions to this problem include the Hadoop distributed data processing system given by Apache, business intelligence platforms, and various NoSQL databases. However, the data integrity is still a big problem. Some vendors like Software AG, SAP, Oracle, and Microsoft IBM provide open source and proprietary solutions in the field of the analytic pipeline (data presentation, core analytics, data storage, and data integration), graph database, comprehensive column store, document store, key-value, and time series. Security and privacy of outsourced data [68] in the cloud-based management system is the worst problem in this case. However, there is no simple solution to handling big data in the cloud.

5.4 Machine learning-IoT based optimization protocol

Machine learning (ML) and IoT are highly complementary technologies that, when combined, offer significant opportunities for improving efficiency, automation, and decision-making in various domains [69]. ML algorithms can analyze historical sensor data from IoT devices to identify patterns indicative of equipment failures or malfunctions. ML algorithms can analyze data from IoT sensors, cameras, and GPS devices in autonomous vehicles to enable advanced driver assistance systems (ADAS), autonomous navigation, and predictive maintenance. ML models can process sensor data, interpret road conditions, and anticipate traffic patterns to assist decision-making and enhance vehicle safety, efficiency, and autonomy [70]. ML algorithms can detect anomalies in IoT data streams, such as sudden spikes, deviations, or outliers, that may indicate unusual behavior or security threats. ML models can help organizations optimize resource allocation, minimize waste, and improve operational efficiency by predicting demand patterns, consumption trends, and supply chain dynamics. ML models can identify energy-saving opportunities, such as optimizing HVAC systems, lighting controls, or equipment scheduling, based on real-time data and user preferences. ML models can help organizations monitor and manage environmental resources, such as water quality, air pollution, or waste management, to mitigate environmental impacts and ensure sustainability. ML algorithms and IoT technologies, organizations can gain actionable insights from IoT data, automate decision-making processes, and deliver personalized experiences to users, ultimately driving business growth and competitive advantage.

6 Conclusion

The term "Internet of Things" (IoT) refers to a network of networked physical items, including machinery, buildings, and cars, that are network-connected and equipped with sensors. These devices gather and exchange data, allowing them to communicate with one another and with centralized or cloud-based services. IoT has evolved as a revolutionary technology with numerous applications in various fields of daily life. As a result of the enormous diversity of devices and applications that make up the Internet of Things (IoT), many communication protocols are used to connect, communicate, and share data across these devices. Various elements, including the application, device capabilities, network constraints, and other particular requirements, influence IoT protocol selection.

Here are some of the commonly used Optimized IoT models, such as IoT with WSN, IoT with blockchain, IoT with machine learning, and IoT with big data analysis. Conducting research on the Internet of Things (IoT) involves exploring various aspects of IoT technology, applications, and its impact on different domains. IoT research spans various topics, from technical aspects such as IoT security and connectivity protocols to application-specific research in healthcare, agriculture, smart cities, and more.

Author Contributions Equally contributed.

Funding No funding was received to carry out this work.

Data Availability Available on request.

Declarations

Conflicts of interest No conflict of interest.

Consent to Publish As per journal policy.

References

1. Ghorbani HR, Ahmadzadegan MH (2017) Security challenges in internet of things: survey. In: 2017 IEEE conference on wireless sensors (ICWiSe)
2. Brock DL (2013) The electronic product code (EPC) a naming scheme for physical objects. http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf
3. IoT Analytics (2014) Why the internet of things is called internet of things: definition, history, disambiguation. https://iot-analytics.com/internet-of-things-definition/
4. Internet of Things (2005) International telecommunication union (ITU), Geneva. https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf
5. Internet of Things (2010) https://en.oxforddictionaries.com/definition/us/internetofthings
6. Manyika Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) Unlocking the potential of the internet of things. https://www.mckinsey.com/~/media/McKinsey
7. Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A, Jubert IS, Mazura M, Harrison M, others (2011) Internet of things strategic research roadmap
8. Artik cloud (2017) https://developer.artik.cloud/documentation/getting-started/index.html
9. Fusion Connect (2014) https://autodeskfusionconnect.com/iot-devices
10. (2016) https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html
11. Guth J, Breitenbücher U, Falkenthal M, Leymann F, Reinfurt L (2016) Comparison of IoT platform architectures: A field study based on a reference architecture. In: 2016 Cloudification of the internet of things (CIoT)

12. Balani, Naveen and Hathi, Rajeev, Enterprise IoT: A Definitive Handbook. In: CreateSpace Independent Publishing Platform, 2015
13. GE Predix (2017) https://docs.predix.io/en-US/platform
14. Soliman M, Abiodun T, Hamouda T, Zhou J, Lung CH, (2013) Smart home: integrating internet of things with web services and cloud computing. In: 2013 IEEE 5th International conference on cloud computing technology and science
15. Google Cloud (2016) https://cloud.google.com/solutions/iot-overview
16. Familiar B (2015) IoT and microservices. In: Microservices, IoT, and Azure. Apress, Berkeley, CA. In: Internet of Things;Web services:Azure IOT
17. Microsoft IoT platform (2015) https://docs.microsoft.com/en-us/rest/api/iothub/?redirectedfrom=MSDN
18. High R (2012) The era of cognitive systems: an inside look at ibm watson and how it works. In: Internet of Things;Web services:Azure IOT
19. IBM Watson IoT (2017) https://www.ibm.com/internet-of-things
20. Deering S, Hinden R (2017) Internet Protocol, Version 6 (IPv6) Specification. https://tools.ietf.org/html/rfc8200
21. WInter Ed T, Thubert P, Brandt A, Hui J, Kelsey R, Levis P, Pister K, Struik R (2012) ipv6 routing protocol for low-power and lossy networks. https://tools.ietf.org/html/rfc6550
22. Saputro N, Akkaya K, Uludag S (2012) A survey of routing protocols for smart grid communications. http://www.sciencedirect.com/science/article/pii/S1389128612001429, vol 56
23. Yi P, Iwayemi A, Zhou C (2011) Building automation networks for smart grids. In: International journals of digital multimedia broadcasting
24. Fairhurst G Jones T (2018) Transport features of the user datagram protocol (UDP) and lightweight UDP (UDP-Lite). https://www.rfceditor.org/info/rfc8304
25. Palattella MR, Accettura N, Vilajosana X, Watteyne T, Grieco LA, Boggia G, Dohler M (2013) Standardized protocol stack for the internet of (Important) things. In: IEEE communications surveys tutorials, vol 15
26. Karagiannis V, Chatzimisios P, Vazquez-Gallego F, Alonso-Zarate J (2015) A survey on application layer protocols for the internet of things. Transaction on IoT and Cloud Computing
27. Banks A, Gupta R (2014) MQTT Version 3.1.1. Edited by Andrew Banks and Rahul Gupta. OASIS Committee Specification Draft 02 / Public Review Draft 02. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/csprd02/mqtt-v3.1.1-csprd02.html
28. Bormann C, Castellani AP, Shelby Z (2012) CoAP: An Application Protocol for Billions of Tiny Internet Nodes. IEEE Internet Computing
29. Shelby Z, Hartke K, Bormann C (2014) The constrained application protocol (CoAP). https://tools.ietf.org/html/rfc7252
30. Johansson P, Kazantzidis M, Kapoor R, Gerla M (2001) Bluetooth: an enabler for personal area networking. IEEE Network
31. Kirsche M, Klauck R (2012) Unify to bridge gaps: Bringing XMPP into the Internet of Things. In: 2012 IEEE international conference on pervasive computing and communications workshops
32. Naik N, Jenkins P (2016) Web protocols and challenges of Web latency in the Web of Things. In: 2016 Eighth international conference on ubiquitous and future networks (ICUFN)
33. Han Dm, Lim Jh (2010) Smart home energy management system using IEEE 802.15.4 and zigbee. IEEE Transactions on Consumer Electronics
34. Eriksson J, Balakrishnan H, Madden S (2008) Cabernet: vehicular content delivery using wifi. https://doi.org/10.1145/1409944.1409968
35. Ratasuk R, Vejlgaard B, Mangalvedhe N, Ghosh A (2016) NB-IoT system for M2M communication. In: 2016 IEEE Wireless communications and networking conference
36. ANDRIES MI, BOGDAN I, NICOLAESCU SV, SCRIPCARIU L (2007) WiMAX features and applications. http://www.agir.ro/buletine/687.pdf
37. Kucharzewski L, Kotulski Z (2014) WiMAX networks architecture and ata security. Annales UMCS Informatica AI X
38. Adams JT (2006) An introduction to IEEE STD 802.15.4. In: 2006 IEEE aerospace conference
39. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. journal = Computer Networks. http://www.sciencedirect.com/science/article/pii/S1389128610001568, vol.54
40. Mainetti L, Patrono L Vilei A (2011) Evolution of wireless sensor networks towards the Internet of Things: A survey. In: SoftCOM 2011, 19th international conference on software, telecommunications and computer networks

41. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. http://www.sciencedirect.com/science/article/pii/S1570870512000674, vol 10, pp 1497–1516
42. Xu LD, He W, Li S (2014) Internet of things in industries: a survey. In: IEEE Transactions on industrial informatics, vol 10
43. Botta A, De Donato W, Persico V, Pescapé A (2016) Integration of cloud computing and internet of things: a survey. http://www.sciencedirect.com/science/article/pii/S0167739X15003015, vol 56
44. Seyedzadegan M, Othman M (2013) IEEE 802.16: WiMAX Overview, WiMAX Architecture. http://www.ijcte.org/papers/796-Z1030.pdf
45. Abdulzahra AM, Al-Qurabat AK, Abdulzahra SA (2023) Optimizing energy consumption in WSN-based IoT using unequal clustering and sleep scheduling methods. Internet of Things 22:100765
46. Chaurasia S, Kumar K (2023) ACRA:Adaptive Meta-heuristic Based Clustering and Routing Algorithm for IoT-Assisted Wireless Sensor Network. Peer to Peer Networking and Application. Springer
47. Chaurasia S, Kumar K (2023) MBASE: Meta-heuristic Based optimized location allocation algorithm for baSE station in IoT assist wireless sensor networks. Multimedia Tools and Applications, pp 1–33
48. Senthil GA, Raaza A, Kumar N (2022) Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network. Wirel Pers Commun 122.3: 2603-2619
49. Prasanth A, Jayachitra S (2020) A novel multi-objective optimization strategy for enhancing quality of service in IoT-enabled WSN applications. Peer Peer Netw Appl 13:1905–1920
50. Vaiyapuri T, et al (2022) A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing. Wirel Pers Commun 127.1: 39-62
51. Dhiman G, Sharma R (2022) SHANN: an IoT and machine-learning-assisted edge cross-layered routing protocol using spotted hyena optimizer. Complex Intell Syst 8(5):3779–3787
52. Seyfollahi A, Taami T, Ghaffari A (2023) Towards developing a machine learning-metaheuristic-enhanced energy-sensitive routing framework for the internet of things. Microprocess Microsyst 96:104747
53. Donta PK et al (2023) iCoCoA: intelligent congestion control algorithm for CoAP using deep reinforcement learning. J Ambient Intell Humaniz Comput 14(3):2951–2966
54. Rosati R et al (2023) From knowledge-based to big data analytic model: a novel IoT and machine learning based decision support system for predictive maintenance in industry 4.0. J Intell Manuf 34.1:107–121
55. Babar M et al (2022) An optimized IoT-enabled big data analytics architecture for edge-cloud computing. IEEE Internet Things J 10(5):3995–4005
56. Lv Z, Singh AK (2021) Big data analysis of internet of things system. ACM Trans Internet Technol 21(2):1–15
57. Qiu Y, Zhu X, Jing L (2021) Fitness monitoring system based on internet of things and big data analysis. IEEE Access 9:8054–8068
58. Rahman A et al (2021) Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot. IEEE Access 9:28361–28376
59. Zhao Y et al (2023) A lightweight model-based evolutionary consensus protocol in blockchain as a service for IoT. IEEE Transactions on Services Computing
60. Saba T et al (2023) Blockchain-enabled intelligent iot protocol for high-performance and secured big financial data transaction. IEEE Transactions on Computational Social Systems
61. Abed S, Reem J, Bassam JM (2023) A review on blockchain and IoT integration from energy, security and hardware perspectives. Wirel Pers Commun 129(3):2079–2122
62. Javanmardi S et al (2023) An SDN perspective IoT-Fog security: A survey. Comput Netw 229:109732
63. Qayyum A et al (2023) Secure and trustworthy artificial intelligence-extended reality (AI-XR) for metaverses. ACM Computing Surveys
64. Rawat P, Chauhan S (2021) Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. Comput Sci Rev 40:100396
65. Albouq SS et al (2023) A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access 10:36416–36428
66. Rana B, Singh Y, Singh PK (2021) A systematic survey on internet of things: Energy efficiency and interoperability perspective. Trans Emerg Telecommun Technol 32(8):e4166
67. Sasaki Y (2021) A survey on IoT big data analytic systems: current and future. IEEE Internet of Things Journal 9(2):1024–1036
68. Alfandi O et al (2021) A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. Cluster Comput 24(1):37–55
69. Bian Jet al. Machine learning in real-time internet of things (iot) systems: A survey. IEEE Internet of Things J 9(11): 8364–8386
70. Donta PK et al (2022) Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. Digital Commun Netw 8(5):727–744