Definition, Challenges and Future Research for Internet of Things

[1]Li Hua Fang and [2]Dong Yonggui
[1,2]Institute of Opto-Electronic Engineering, Tsinghua University, Haidian District, Beijing, China, 100190.
[1]lihua@tsinghua.edu.cn, [2]dongyon332@hotmail.com

Correspondence should be addressed to Dong Yonggui : dongyon332@hotmail.com.

Article Info
Journal of Computing and Natural Science (http://anapub.co.ke/journals/jcns/jcns.html)
Doi: https://doi.org/10.53759/181X/JCNS202303020
Received 10 December 2022; Revised from 02 March 2023; Accepted 06 June 2023.
Available online 05 October 2023.

Abstract – This article aims to provide a review of Internet of Things (IoT), analyzing its significant challenges within the framework of existing research on the topic. The IoT is a contemporary technology that encompasses wireless telecommunication networks. It can be conceptualized as a smart and interoperable node integrated within a vibrant global architectural system, with the objective of achieving ubiquitous and uninterrupted connectivity. The IoT landscape encompasses various challenges that significantly impact its operational efficacy. The challenges can be categorized into two main groups: i) General challenges integrating heterogeneity, security, virtualization, and communication; and ii) Unique challenges including Quality of Service (QoS), wireless sensor network (WSN), and Radio Frequency Identification (RFID), which is considered a shared factor between both groups. The report additionally outlines the primary applications of the IoT.

Keywords – Internet of Things, Ubiquitous Computing, Wireless Sensor Networks, Radio Frequency Identification, Quality of Service.

I. INTRODUCTION

Currently, we find ourselves in the era of "ubiquitous computing" or "web 0.3," wherein there is a notable prevalence of advanced technological systems. The Internet of Things (IoT) has been recognized as a vital platform for showcasing state-of-the-art innovation. Cloud computing is not only not the inaugural technology of its kind, but it has also been employed as a representation of the ubiquitous presence of computers in contemporary society. The phrase "internet of things" was initially established in 1999, by Kevin Ashton in the RFID magazine. Subsequently, it gained official recognition in 2005, following its introduction in 1997 as "Challenges to the Network" in the seventh installment of the ITU Internet Reports. Kevin's proposed concept for the IoT entails enabling interconnected devices to exchange information pertaining to tangible objects in the physical world through the utilization of internet connectivity. Many contemporary IoT architectures employ web semantics to distribute data through social media platforms. An example of this is the Nike+iPod service on the iPhone, which collects data and shares it with users' acquaintances on Twitter and Facebook.

The definition of the IoT lacks consensus among scholars and experts. However, in a formal context, it can be characterized as a network that is globally distributed, dynamic, and capable of self-configuration, enabling interoperable communication. In essence, the IoT refers to the capacity to establish connectivity between various entities in our surroundings, encompassing machinery, devices, mobile phones, automobiles, urban areas, and thoroughfares. This connectivity enables these entities to operate independently and maintain privacy while being linked to the Internet. In the realm of the IoT, there exists a wide array of objects, primarily classified into two distinct categories. The first category encompasses objects equipped with rechargeable batteries, such as mobile devices like notebooks, tablets, and smartphones. The second category comprises objects that lack rechargeable batteries and remain stationary.

In order for the IoT to operate at its highest level of efficiency, it is imperative to fulfill three fundamental prerequisites. The initial requirement entails establishing a consensus regarding the condition of the users involved and the inherent characteristics of the applications utilized within the IoT framework. In order to attain its objective of autonomous and intelligent behavior, the IoT must initially depend on a resilient software architecture and extensive communication networks. The fundamental principle underlying the IoT is to enable seamless communication between various entities, employing context-aware software, without any temporal constraints.

Consequently, the integration of RFID and sensor network technologies has been incorporated into the IoT. As an example, IBM implemented IoT technology on oil platforms located in the Norwegian Sea. This was achieved through the installation of sensors on the seafloor, which facilitated the collection of data. The purpose of this data acquisition was to inform decision-making processes in the context of offshore oil drilling. Nevertheless, the IoT ecosystem presents distinct challenges that can significantly affect the performance of networks. The present study categorizes these challenges into

two distinct groups: i) Broad challenges encompassing both the IoT and traditional networks, encompassing aspects such as quality of service, virtualization, security, data mining, scalability, heterogeneity, and communication; and ii) Specific challenges exclusive to technologies like WSN and RFID.

This article aims to provide readers with an introduction to the IoT, encompassing its conceptual framework, architectural structure, and the differentiating factors between the IoT and the traditional Internet. Subsequently, the article will delve into the challenges associated with the IoT and highlight the latest research endeavors aimed at addressing these obstacles. The remaining contents of this paper have been organized as follows. Section II presents a detailed review of previous literature texts. On the history and definition of IoT, including its architecture and design. Section III discusses challenges and contemporary future research IoT. In Section IV, a discussion of potential applications of IoT is provided. Lastly, Section V presents a conclusion to the article as well as directions for future research.

II. LITERATURE REVIEW

The objective of this section is to present a comprehensive overview of the IoT, encompassing its definition, historical background, and origins. Additionally, it aims to emphasize the architectural design of the IoT (see **Fig 1**), which is structured around three dimensions referred to as the "IoT infrastructure." Finally, this section concludes by drawing a comparison and contrast between the IoT and the traditional Internet.

History and Definitions

Mark Weiser introduced the concept of "ubiquitous computing" in 1991 to describe his envisioned trajectory for the future of the Internet. The focus of his dream revolved around the activation of an intelligent and dynamic living environment, facilitated by the widespread presence of mobile phone technology. This, in turn, facilitates the development of a resilient multimedia system. Kevin Ashton is widely recognized as a prominent figure in the discourse surrounding the IoT. In their study, Eris, Drury, and Ercolini [1] classified the IoT into three distinct categories: internet-centric, things-centric, and semantic-centric. The internet-centric category focuses on middleware, while the things-centric category emphasizes sensors. Lastly, the semantic-centric category centers around knowledge in the context of IoT. Neil Gershenfeld, affiliated with the MIT (Massachusetts Institute of Technology) Media laboratory, authored the publication "When Things Start to Think" in the year 1999, wherein he expounded upon comparable concepts.

In 1999, a collaboration between MIT and Auto-ID laboratories resulted in the advancement of RFID (radio frequency identification) and EPC (electronic product code) technologies for the purpose of facilitating networked object identification [2]. The term "internet of things" started to emerge in scholarly literature around 2003-2004, as evidenced by its appearance in publications like Cooltown, Internet0, and the Disappearing Computer initiative. A comprehensive announcement has been issued by the United States Department of Defense regarding the application of RFID. The year 2005 marked the commencement of a new era with the publication of the inaugural report on the IoT by the International Telecommunication Union (ITU). The IPSO Alliance was established in 2008 by prominent firms such as SAP, Cisco, and Intel, and more than 50 other companies with the objective of promoting awareness and understanding of Internet Protocol (IP) and initiating the development of the IoT concept.

The inception of the IoT can be attributed to Cisco's Internet Business Solutions Group (IBSG) during the years 2008-2009. Based on the aforementioned information, the IoT could be well-defined as a system comprising of distinctively identifiable devices that are connected to the Internet. These devices encompass a wide range of consumer electronics, such as smartphones and laptops.

Architecture and Design

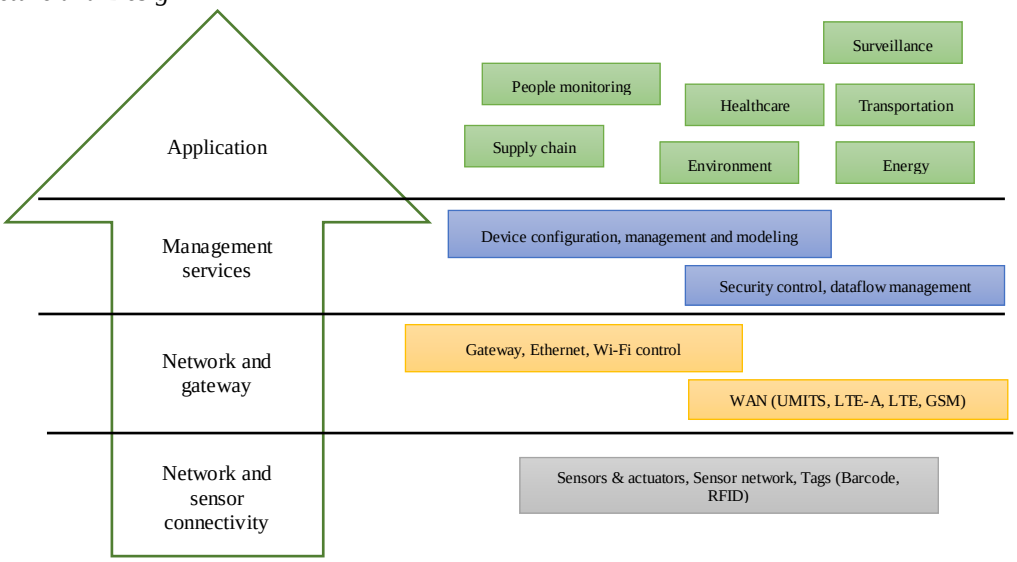

Fig 1. Reference Architecture of IOT

Sensor, Connectivity and Network Layer

RFID tags and sensors, which are integral components of IoT systems, constitute this level, which assumes the responsibility of collecting primary data. All of these elements are essential components of an IoT infrastructure. Wireless Sensor Networks (WSN) consist of wireless devices, namely sensors and RFID tags. The real-time collection and processing of data are imperative due to the inherent dynamism of sensors. The unprocessed data is transmitted from this particular layer via its network link, which may include PANs (personal area networks), WSNs, and other similar networks, to the Gateway and Network Layer situated beneath it. WSN consist of devices that possess constrained resources, such as limited processing capabilities, narrow communication bandwidth, and minimal storage capacity. The selection of sensors is contingent upon the specific task being performed. For instance, a temperature sensor is employed to collect temperature measurements, a water quality sensor is utilized to assess the quality of water, a moisture sensor is employed to ascertain the moisture content in the air or soil, and so forth.

Gateway and Network Layer

The Gateway receives data from the Network, Connectivity, and Sensor layers and subsequently transfers it to the Management Service Layer. In order for this layer to effectively operate, it is imperative that it possesses the capability to store the substantial volumes of data that are produced by the sensors, RFID tags, and other related components. The aforementioned layer should demonstrate consistent and dependable performance across various network environments, encompassing public, private, and hybrid networks. The assortment of network protocols supported by different IoT devices exhibits variability. The integration of all these protocols into a unified framework is imperative. Various networking protocols are incorporated at this layer.

Management Service Layer

The management of IoT services takes place at this particular level. The management Service layer encompasses the evaluation of security in IoT equipment, the evaluation of data through data analytics and stream analytics, as well as the management of these devices. The considerable quantities of unprocessed data generated by the sensor devices necessitate meticulous data management to extract pertinent information and yield a valuable outcome. This process occurs at this particular level. In addition, there are instances wherein prompt action is required. In order to enhance the process, this layer functions by abstracting information, extracting pertinent data, and controlling the flow of data. Data mining, text mining, and service analytics are all encompassed within the scope of this layer.

Application Layer

The application layer of the IoT assumes the responsibility of effectively utilizing the collected data. The applications of the IoT encompass a wide spectrum, spanning from the automation of household tasks to the management of electronic health records and the facilitation of electronic government services.

Differences between Traditional Network and IoT

The advent of IoT technology has significantly disrupted various established network paradigms, thereby initiating a paradigm shift in the realm of communications innovation. The IoT is reliant on the Internet as its underlying infrastructure, but it is important to note that it differs from traditional networks and other related technologies such as the Internet of People and WSN. These technologies are frequently utilized as foundational components for IoT applications. The prevailing notion posits that the IoT ecosystem can be best described as the amalgamation of WSN and the Internet. To effectively evaluate the precision of this statement, it is necessary to examine and assess the similarities and distinctions among the IoT, the Internet, and WSN.

The aforementioned approach, predicated on the notion that the evaluation of the IoT ecosystem can be conducted by considering preexisting knowledge, is flawed due to a minimum of two reasons. The TCP/IP protocol may not be well-suited for addressing objects in the context of the IoT, especially when dealing with small, smart devices. As a result, alternative addressing methods may be utilized in certain IoT scenarios. Secondly, in distinction to traditional systems, the ecosystem of the IoT is majorly oriented on the interconnectedness of intelligent devices. Given the aforementioned rationales, it may be necessary to reconsider the previous assertion: The IoT transcends being a mere expansion of the Internet; its functionality is also contingent upon the advancement of interoperable systems.

III. CHALLENGES AND CONTEMPORARY FUTURE RESEARCH

This part of the article outlines the ongoing research efforts pertaining to the most critical challenges faced by the IoT.

Networking

The issue of Networking holds significant relevance in the context of the Internet, as it encompasses various essential facets pertaining to network administration. Initially, Zhao, Pop, and Steinhorst [3] discuss the influence of traffic and protocols on network performance. In an effort to address networking challenges, the utilization of a mobile Ad-Hoc network is being explored. The implementation of fixed-mobile gateway interconnection has been carried out by the authors through the utilization of mobile ad hoc networks (MANET). In the context of the IoT, the determination of an item's destination is inherently uncertain, thereby necessitating the potential transfer of said item across different networks. The most challenging

elements encompass the frequent and unforeseen alterations to gate assignments, as well as the complexity in ascertaining spatial orientations. A Mobile Ad hoc Network (MANET) is comprised of numerous autonomous mobile nodes or objects, and is commonly regarded as a mechanism for maintaining connectivity. The IoT incorporates multi-homed ad hoc networks as a supplementary component to the existing infrastructure.

Routing

In order to effectively complete a communication process, the "routing process" is responsible for determining the most efficient route between the destination and the source. The determination of the optimal route can be achieved through various methods, with some of them contingent upon the specific communication protocol employed. There are two main categories of routing protocols: In contrast to proactive protocols that establish the course of action in advance, reactive protocols generate it upon receiving a transmission request. The fault-tolerant routing protocol for the IoT was proposed by Misra, Gupta, Krishna, Agarwal, and Obaidat [4]. This protocol was developed by employing cross-layer theory and incorporating a learning automaton (LA).

The issue of achieving energy savings across multiple layers in IoT devices, specifically in the context of FRID technology, poses a significant challenge that necessitates the attention of the academic community in Los Angeles. Addressing this challenge is crucial in order to identify and implement effective solutions for optimization problems. Variability refers to the extent to which data points in a dataset differ from each other The heterogeneity problem is frequently exemplified by the diverse array of devices within the IoT ecosystem. The primary objective of the IoT is to establish a standardized method for abstracting the variations among these devices, thus optimizing their capabilities. In pursuit of this objective, scholars persist in seeking improved approaches to manage various types of devices.

In their study, Neha, Gupta, and Alam [5] sought to address various challenges in the field of IoT by creating a specialized language, graphical editor, and platform known as Midgar. Their objective was to provide solutions for issues such as heterogeneity, interconnection, and the development of an application, which facilitates the interconnectivity of services via the Internet. To exemplify a potential resolution to this matter, one may examine the increasing prevalence of applications such as WhatsApp, Skype, and similar platforms that facilitate communication between individuals utilizing diverse devices via the Internet. The Midgar software, designed for the purpose of managing diverse smart devices within an IoT ecosystem, has undergone a comprehensive evaluation.

The primary focus of this software lies in the generation of a domain that enables seamless communication between these entities. The researchers conducted an analysis of Midgar, a software tool designed for the management of diverse smart devices within an IoT environment. Additionally, they investigated DSL, a software tool that enables the creation of a domain specifically tailored to facilitate interactions between objects of varying types. Midgar Software circumvented the complexities associated with traditional methods of resolving this problem. The city of Midgar can be regarded as an initial stage in the development of interconnectedness, as it is anticipated that future connectivity will extend beyond mere technological devices to encompass human interactions, thereby facilitating the resolution of pertinent issues.

Furthermore, the IoT utilizes a service-oriented architecture (SOA) approach, similar to other networks, in order to enhance the efficiency of diverse resources, including sensors and actuators. This strategy enables the system to achieve a high level of adaptability and scalability in terms of both internal exchange and external integration process in the middleware.

Middleware Layer

Middleware represents the software layer or a collection of sub-layers between the application and technology layers. Its primary function is to provide a standardized approach for representation and communication. The concept of transparency is a prominent characteristic of distributed systems and is frequently facilitated by the middleware layer to shield the end user from intricate details. One type of middleware technology utilized for the management of the IoT is Service-Oriented Architecture (SOA). This technology facilitates the dynamic reutilization and utilization of pre-existing real-world services. Service Level Agreements (SLAs) are a type of service that is facilitated by Service-Oriented Architectures (SOAs). They serve the purpose of formalizing the commitments made between service providers and consumers. The key feature that sets SLAs apart is their ability to ensure the QoS, specifically through the guarantee of timely delivery of the service. The middleware layer integrates 3 fundamental pillars, which are as follows: The Service Compilation Layer, typically constructed upon SOA Middleware, enables the aggregation of individual services into more comprehensive applications. This particular layer is specifically designated for the purpose of delivering services or providing service provision.

The architecture of a service composition, as outlined in the SLA, is derived from the distinct architectures of the services involved. The Service Management layer, situated as the second layer, serves the purpose of enabling the management of IoT operations. There are two overarching categories that can be employed for service management: Services that are dependent on the progression of time in order to operate effectively fall into the classification of "i) runtime." The design process encompasses both maintenance services and the creation of new services. In addition to quality of service (QoS) management and lock management, certain middleware systems incorporate supplementary functionalities pertaining to the service management layer. These include status monitoring, object dynamic discovery, service policy enforcement, service configuration, and service Meta model updates. It is important to acknowledge that the service management layer has the

potential to facilitate the development of supplementary services during runtime. The organization of layers facilitates the integration of various devices by providing a uniform language and approach.

Consequently, an object abstraction layer becomes essential for managing the extensive and diverse range of items present within the IoT. The object abstraction layer integrates 2 different sub-layers. The first sub-layer, known as the interface sub-layer, is responsible for managing and delivering messages. The second sub-layer, referred to as the wrapper layer, provides an interface to the object's methods through a web service. The communication sub-layer, as described by Panja, Chattopadhyay, and Nag [6], serves the purpose of facilitating bidirectional communication between virtual and physical entities by translating web service protocols for device compatibility.

Interoperability

The fundamental concept of interoperability revolves around the ability to conceive and develop systems and devices that possess the capability to communicate and collaborate seamlessly. In their study, Emruli, Sandin, and Delsing [7] propose the utilization of a semantic level interoperability architecture, referred to as "smart-M3," for the purpose of facilitating semantic information sharing in the domains of ubiquitous computing and the IoT. The proposed design is based on the assumption that implementing a compartmentalized approach to the IoT environment would facilitate its management. Furthermore, the Semantic Information Broker (SIB) not only enables the real-time monitoring and updates of the physical environment but also facilitates the exchange of semantic information among agents. Furthermore, the design's primary observation is that the agent interaction procedures exhibit favorable scalability, while also facilitating real-time connectivity with the physical environment. In forthcoming IoT system architectures, there will be a need for tools that enable the seamless development and dissemination of interconnected devices and software.

Quality of Service (QoS)

In an ideal scenario, Quality of Service (QoS) can be described as the duration it takes for a message to be transmitted from the sender to the receiver. QoS is considered to be achieved when this duration meets or falls below a predetermined time threshold. The International Telecommunication Union (ITU) has provided a new QoS definition as the agreement level between the user and the service provider regarding the expected quality of the service to be provided [8]. To ensure a consistent level of quality for all Internet services, it is imperative to address service models. Furthermore, Internet service models can be employed for the purpose of classifying Internet services, thereby facilitating two primary objectives: prioritizing Internet applications and establishing the necessary Quality of Service criteria to guarantee user contentment. The service model comprises three primary elements: the delay factor, the critical factor, and the interactivity factor.

The delay factor pertains to time and can be further categorized into Soft Real Time (SRT), Non-Real Time (NRT), and Hard Real Time (HRT). The critical factor alludes to an application or process type and its sensitivity. Lastly, the interactivity factor considers whether the user can engage with the service. In their study, Masoudi-Sobhanzadeh, Motieghader, Omidi, and Masoudi-Nejad [9] conducted a comparative analysis of three widely used algorithms, namely Genetic Algorithm (GA), Backtracking Algorithm (BA), and Integrated Linear Programming (ILP). The objective of their investigation was to identify the most suitable algorithm for efficiently addressing the given context at a large scale and in real-time scenarios within the IoT domain. In contrast to other algorithms, the BA algorithm yielded superior real-time outcomes. Consequently, the authors opted to utilize it for the implementation of their concept.

Scalability

Scalability, which refers to the ability to effectively manage the continuous expansion of the Internet, poses a significant challenge for the implementation of IoT. In other terms, scalability refers to the capacity of a network or a system to effectively manage the increasing magnitude of a given environment, while maintaining optimal performance. This encapsulates the essence of the concept of scalability. The anticipated addition of approximately 24 billion devices to the Internet in the upcoming era, referred to as Web 0.3 or ubiquitous computing, will result in significant implications for the network's capacity and speed due to its exponential growth. In their study, Bittencourt et al. [10] sought to integrate the IoT with cloud computing technologies, specifically focusing on the utilization of the Aneka software. Cloud computing frequently delivers a range of advantages, like scalability and abundant storage capacity, a visualization infrastructure, and client delivery, alongside a flexible payment model based on usage for each service. The Aneka cloud computing platform facilitates the utilization of data storage and computational capabilities offered by both public and private cloud infrastructures.

Virtualization

The term "virtualization" refers to the phenomenon wherein multiple operating systems are able to utilize a shared hardware infrastructure. Virtualization technology enables the consolidation of multiple servers into a single physical server, thereby facilitating the hosting of diverse operating systems, applications, and services on a unified platform. The objective of this concept is to enhance network performance through various means, such as increased utilization, improved scalability, and reduced expenses. The three primary conceptual frameworks for virtualization technology are storage virtualization, server virtualization, and network virtualization. Alarbi and H. Lutfiyya [11] developed a framework for IoT virtualization, which is founded on the concept of Sensor as a Service (SaaS).

The aforementioned structure incorporates a database for the storage of relevant data, alongside the levels of "real world," "semantic," and "virtualization." The objective of the proposed framework is to address this challenge by employing a semantic approach to handle the heterogeneity. This is achieved by introducing a standardized language known as Sensor Model Language (SensorML). The aforementioned issues can be categorized into three distinct areas: firstly, the absence of a centralized registry mechanism; secondly, the challenges posed by heterogeneity and discovery; and finally, concerns regarding security and privacy. The future prospects of this model can be categorized into two distinct areas: firstly, boosting its real-time performances, and secondly, refining its micro-format specifically for promotion purposes on social media networks.

Big Data

The term "Big Data" refers to datasets of significant size, which can be either structured or unstructured. These datasets pose challenges to traditional database management strategies and software tools in terms of their efficient processing. The term "Big Data" alludes to an extensive volume of data. The phrase "Big Data" alludes to datasets that possess significant value, substantial volume, rapid velocity, and diverse data types. Social media platforms such as Twitter, Facebook, and Instagram exemplify the types of enterprises that are attracted to Big Data due to the substantial amount of data produced by their user populations. According to [12], Twitter was responsible for generating a substantial amount of data, specifically up to 120 terabytes per day. The application of the term "Big Data" to the IoT has been successful due to the vast and diverse nature of the data collected through the extensive utilization of sensors in IoT environments. The IoT and Big Data are closely interconnected. Fararni, Nafis, Aghoutane, Yahyaouy, Riffi, and Sabri [13] sought to integrate the concept of Big Data within the IoT framework. Their objective was to develop a software architecture capable of addressing practical situations by utilizing data derived from the SMARTCAMPUS project. This design effectively tackled challenges related to data storage, processing bottleneck mitigation, and achieving high throughput.

Cloud Computing

Cloud Computing and the IoT are frequently employed as exemplars of the distributed computing paradigm. However, it is worth noting that the latter, in comparison to the former, lacks the same level of widespread recognition. In addition to facilitating the distribution of affordable software to a substantial user base through a reliable and decentralized approach, cloud computing also enables convenient utilization of extensive computational resources. The three major cloud computing tiers, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), offer distinct sets of valuable functionalities from a remote data center. Both the IoT and cloud computing possess inherent advantages and disadvantages; nevertheless, they are widely acknowledged as a prevailing paradigm for delineating the Internet. The storage and processing capacity of cloud computing is nearly boundless, whereas the IoT is constrained by its representation of the physical world and the limited number of objects within it.

The incorporation of IoT and cloud computing has emerged as a prominent subject of investigation in contemporary research. The primary objective is to leverage the scalability, storage capabilities, and virtualization offered by cloud computing to effectively address the computational requirements of sensors and other IoT devices. In a previous study conducted in [14], Mousavi, Mood, Souri, and Javidi examined the present incorporation between cloud computing and IoT within the paradigm of CloudIoT. Their objective was to highlight the advantages derived from this integration. This study is representative of a broader body of recent research that has explored the incorporation of IoT concept and cloud computing. Virtualization technology offers transparency to the end user by concealing the intricacies of sensors. Cloud computing facilitates the provision of storage resources. The big data movement presents a novel approach to organizing vast quantities of data in the context of the IoT. Computational resources are a crucial component of the IoT. The scalability of the IoT is significantly improved through the utilization of cloud computing, eliminating associated concerns.

Power Consumption

The issue of power consumption holds significant importance in the context of wireless networks. The efficacy of sensors in carrying out their tasks is frequently contingent upon the duration of their battery life. Sensors have become a ubiquitous feature in contemporary electronic devices, such as smartphones, tablets, and computers, thereby endowing them with the capacity to effectively operate advanced software applications. An example of this is a weather forecasting software that heavily depends on data from the global positioning system (GPS). If the GPS function is continuously enabled throughout the entire sensing process, it can lead to a significant depletion of the device's battery. The issue of power consumption through the utilization of sniffer agents is examined by Gomez-gualdron and Velez-Reyes [15].

A study was conducted by [16] to assess the present power demand by examining the consumption of mobile energy of integrated consumer devices. The study provided a description of the framework for the recommended SOPCA approach (self-organized power consumption approximation). In this methodology, devices establish connections with other devices in order to facilitate the transmission of energy through the utilization of a wireless communication protocol known as the energy sniffer agent (ESA). These connections are established between peer devices as well as servers. To estimate energy consumption, the European Space Agency (ESA) locates and monitors electronic devices. After the source node has utilized GPS to ascertain the precise location of the target node, it will proceed to revise its internal metrics according to observed consumption of local energy. The implementation of flags on individual devices is a key feature of the SOPCA algorithm,

which effectively mitigates the possibility of data being redirected. The suggested algorithm was tested on a random network using an agent-based model (ABM) by the authors.

Security and privacy

The primary objective of the security policy is to mitigate potential risks to the system, originating from both external threats, such as hacker attacks, as well as internal vulnerabilities, such as data loss or improper usage. The three foundational principles that underpin security are the integrity, privacy, and veracity of an individual's data. The system employs two key components to enforce data security: an access control mechanism and an object authentication procedure. These components collectively ensure that only individuals with proper authorization are granted the ability to access and modify data. Digital certificates are widely recognized as a prominent illustration of a veracity assurance mechanism employed to enforce security prerequisites within a given system. Privacy is a concept encompassing secrecy, anonymity, and solitude. It entails the regulated control over personal information, enabling the preservation of specific data and information in a confidential manner. Regarding the safeguarding of one's online identity, recent research places emphasis on the augmentation and enhancement of privacy within applications through the utilization of Privacy Enhancing Technologies (PET). These technologies have the capacity to be customized to suit the needs of individual users, specific items, transactions, or entire systems. In order to establish a reliable connection between the physical realm and the digital realm, ensuring security and privacy is of utmost importance within the context of the IoT.

In their study, Ray, Abawajy, and Chowdhury [17] proposed a hybrid approach that utilizes a group-based and collaborative framework incorporating SCH (security check handoff) with radio frequency identification (RFID) technology. The security checks and re-clearance flags, denoted by binary values of 0 and 1 to indicate their activation or deactivation, respectively, serve the purpose of monitoring the security status of a tag and facilitating an expedited process for the tag to successfully undergo the security check. The majority of existing protocols pertaining to RFID exhibit various limitations, including but not limited to issues related to security, inefficient identification methods, low throughput rates, and a lack of adaptability. The proposed protocol facilitates the implementation of necessary modifications to effectively accommodate the updated and enhanced methodologies. Advancements in RFID security protocols contribute to the establishment of a heightened level of security within the distributed architecture of the IoT.

IV. APPLICATIONS

The IoT is increasingly becoming an essential component of our everyday existence, finding utility in a wide range of domains such as surveillance, smart water management, healthcare, transportation, and numerous others. Moreover, a multitude of applications have been developed to bolster this concept. The applications of the IoT can be categorized as follows, utilizing the classification scheme outlined in [18]: The healthcare industry is frequently referenced as an illustrative case for the utilization of WiFi as a primary infrastructure for data transfer, enabling enhanced bandwidth and sampling rates.

This industry can be classified into three categories: i) Personal and Home, where WiFi is employed to facilitate high-speed data transfer and increased sampling rates; ii) Enterprise, encompassing the collection of information from network sources and environmental surveillance, like video surveillance, which serves as a prominent example in this group. Additionally, the domain of smart home and smart environment falls under this classification; and iii) Mobile, which pertains to the integration of WiFi technology within mobile healthcare applications. The primary incentive for businesses to utilize such software typically revolves around the objective of augmenting revenue generation while concurrently reducing operational costs. The most notable instances of this nature include smart metering, smart grid, smart water, and the assessment of the quality of drinking water.

Healthcare

The healthcare sector has widely adopted the IoTCloud paradigm for the purpose of remotely diagnosing, treating, and monitoring patients' conditions. The paradigm must be designed to uphold four fundamental pillars. There are four main functions associated with the use of RFID technology in healthcare settings. The first function is tracking, which involves the identification of patients while they are in motion. The second function is identification and authentication, which aims to minimize diagnostic errors. The third function is data collection, which involves integrating RFID technology with other health information systems to reduce processing time. Lastly, the fourth function is sensing, which provides valuable information about the patient's condition to ensure their well-being. The issues present in this context can be characterized by terms such as control, heterogeneity, security, interoperability, and streaming quality of service.

Ambient Assisted Living

Ambient Assisted Living (AAL) technologies have the potential to address individual healthcare challenges and foster increased citizen engagement in healthcare. In the context of healthcare monitoring, which can be facilitated by the IoT, AAL systems offer a comprehensive framework comprising computers, medical sensors, software applications, and wireless networks. Put simply, it is necessary to have a specialized IoT service.

m-Health Things (m-IoT)
The concept of Mobile IoT (m-IoT) is characterized as a novel framework that combines the functionalities of m-health and IoT to enable the development of innovative applications for the future, specifically in the realm of 4G health. M-health, also known as mobile health, encompasses the application of mobile computing, medical sensors, and communication technologies with the aim of enhancing healthcare accessibility. In theory, the concept of "m-IoT" introduces a new healthcare connectivity model that establishes a connection between the 6LoWPAN protocol and emerging 4G networks. This model aims to facilitate the delivery of m-health services over the internet in future scenarios. While the term "m-IoT" commonly refers to the application of IoT in medical services, it is crucial to acknowledge that there are distinct attributes associated with the worldwide mobility of the individuals engaged in this domain.

Adverse Drug Reaction
An adverse drug reaction, as defined by medical literature, refers to the harm caused by a medication, whether resulting from a single dose, prolonged use, repeated dosing, or drug interaction. The sources mentioned above provide solutions to this issue.

Community Healthcare
One instance of an IoT-enabled service can be observed in the form of a cooperative network structure that encompasses various regions such as an urban vicinity, a hospital catering to the inhabitants of said city, a residential neighborhood, or even a rural area. Wang, Shibamura, Ng, and Inoue [19] have proposed a cooperative IoT platform that is designed to monitor healthcare in rural areas with a focus on energy efficiency.

Wearable Device Access
Numerous non-intrusive sensors have been established for a wide-range of clinical application, with key interest in WSN-oriented medical services. In subsequent periods, these sensors have the potential to leverage the IoT in order to offer equivalent functionalities. Conversely, the IoT facilitates the incorporation of numerous desirable features into wearable devices.

Semantic Medical Access
The utilization of ontologies and semantics has been extensively examined as a strategy for enhancing the distribution of extensive collections of medical knowledge and data. The designers of IoT healthcare applications have demonstrated a keen focus on the extensive possibilities offered by medical semantics and ontologies.

Indirect Emergency Healthcare
Indirect healthcare emergencies encompass a range of events, such as natural disasters, transportation accidents (including those occurring in air, sea, and land settings), and the failure of earthen structures. Consequently, the provision of indirect emergency healthcare (IEH) service offers a range of solutions like facilitating access to pertinent information.

Embedded Gateway Configuration
The Embedded Gateway Configuration (EGC) services establish a connection between patient network nodes and the Internet, facilitating communication with all interconnected medical devices. These services exhibit a common set of integration characteristics that are essential irrespective of the intended usage of the installed gateway.

Embedded Context Prediction
Third-party developers may be required to develop frameworks that incorporate appropriate mechanisms, which are referred to as suitable mechanisms for ECP service. A comparable framework is established for ubiquitous healthcare in [20].

Early intervention/prevention
The monitoring of human activity and health, including the reporting of anomalies in daily routines to medical institutions or individuals of personal significance. The monitoring of embedded devices can be facilitated through the utilization of the IoT.

The convergence of IoT and cloud computing has garnered significant interest in recent times as a fundamental approach to establishing an intelligent ecosystem, like a smart city or a smart city, while ensuring the preservation of service excellence. The IoT encounters several challenging issues, with the primary concern being the heterogeneity of interconnected devices. Numerous middleware solutions have been developed to tackle this issue, including RFID middleware and WSN middleware. In contrast, cloud computing presents the advantage of scalability and leverages virtualization technologies to obfuscate the intricacies of sensors from end users. The application encounters significant challenges primarily in the areas of security and real-time use cases.

A. Smart environment

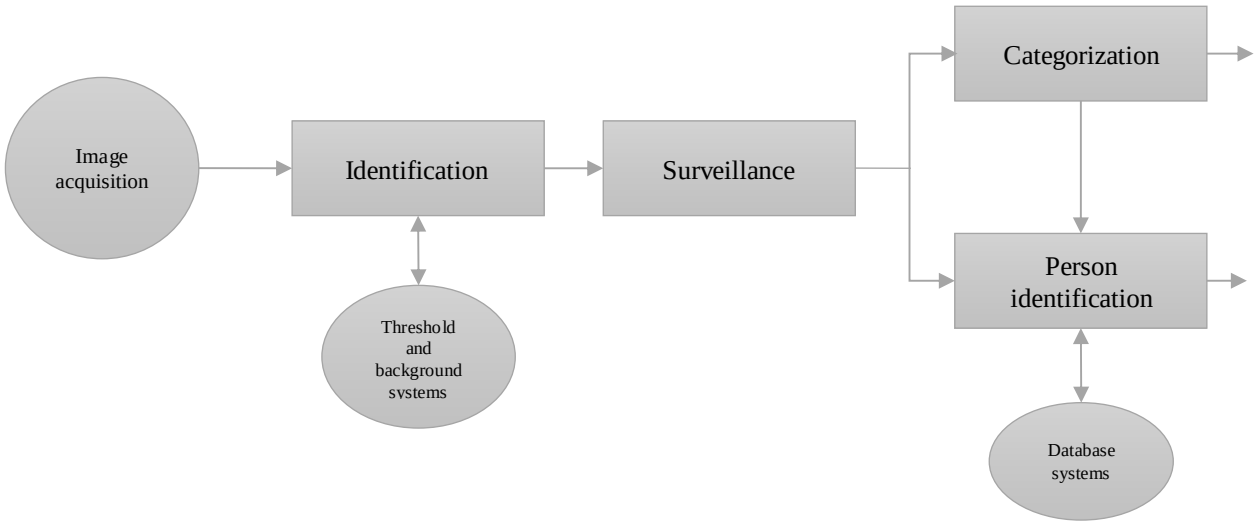

Fig 2. The System Block Diagram of A Video System Designed Specifically for Urban Surveillance Purposes

Video Surveillance

Video surveillance is a sophisticated method of monitoring the actions and conduct of various entities (see **Fig. 2**). It has gained significant significance in the realm of security-related applications and can be considered as a viable substitute for independent management systems. The intricate nature of video analytics requires the implementation of Cloud-based solutions. Additionally, video surveillance can effectively address the requirement for expanding the storage capacity of media. The primary objective of this position is to optimize transportation and mobility within the automotive industry through the improvement of road safety measures, reduction of traffic congestion, and effective management of traffic flow. The convergence of Cloud Computing and IoT presents an unprecedented opportunity to explore a cost-efficient solution that demonstrates exceptional performance and security capabilities. The challenges associated with this particular category encompass aspects such as object recognition, sensor diversity, scalability, and object behavior alteration.

The system encompasses various functionalities such as object detection, tracking, recognition, and categorization. Several methodologies have been employed to address the object detection problem. One approach involves utilizing statistical models of the background image. Alternatively, some researchers have employed frame differences techniques. Additionally, a hybrid approach combining both methodologies has also been explored. Multiple approaches have been employed to address the challenge of tracking multiple interacting targets in video sequences. The tasks of object recognition and classification are achieved through the utilization of Statistical Pattern Recognition and a neural network. Various characteristics can be employed to examine the present state of the problem. The utilization of geometric characteristics such as motion patterns, color histogram, and bounding box aspect ratio can be observed in these analyses.

System Description

The surveillance system that has been implemented can be divided into four separate yet interconnected modules: detection, tracking, classification, and recognition. In order to accomplish the detection process, we made modifications to a rapid real-time technique put forth by Li, Jia, and Mao [21]. The employed methodology incorporates two distinct backdrop images, diverse pixel thresholds, and a region grouping mechanism known as quasi-connected components (QCC). In the absence of any uncertainty, the tracking algorithm computes the degree of overlap between identified regions in consecutive frames in order to establish their connection. The displacement of the center of mass is depicted as a trajectory, formed by linking a region of interest across consecutive frames. The classification of a stroke is achieved by determining the category that is most frequently selected from the various active areas identified across all frames. The system incorporates a supplementary color identification module to assist in mitigating issues related to tracking ambiguity.

Detection

The main difficulties associated with this methodology arise from the dynamic nature of the background, which undergoes continuous changes even in controlled settings. These changes primarily result from variations in lighting conditions and the presence of distractors, such as passing clouds or swaying branches of trees. By employing adaptive background models and per-pixel thresholds, it is possible to enhance the system's resilience to variations in the lighting conditions of the scene. The utilization of the QCC grouping technique, in conjunction with the incorporation of multiple backgrounds, contributes to the algorithm's robustness against noise. The system employs two background models that have been trained using grayscale data. The underlying principle involves the examination of pixel variations in the scene that do not correspond to the intended target. This is achieved by incorporating both lower and higher pixel values. The initial value assigned to the per-pixel limit is established to be higher than the dissimilarity observed between the two different backgrounds. The ability to perceive

occurrences, as well as determine the position and track mobile entities, is imperative for the functionality of any surveillance system.

The primary challenge faced by human intelligence analysts in video-oriented monitoring is the interpretation of digital analysis information and data to identify vital events and discern patterns. There exist numerous challenges in this domain, including the augmentation of video analysis through the incorporation of temporal and deployment condition knowledge, the interpretation of events by leveraging geometric models of the environment as well as object and activity models, and the improvement of system performance and identification of anomalous events through the utilization of learning techniques. Object detection serves as the initial stage in the majority of tracking systems, facilitating the process of narrowing down the scope of analysis. Object detection can be achieved through the utilization of two distinct methods: salient motion detection and background removal. Background subtraction considered a static background and handles any modifications in the scenario as a possible object of interest. Salient motion detection, on the other hand, expects that a scene will contain various forms of motion, but only a subset of these motions are relevant for surveillance purposes.

Tracking

The objective of tracking is to gather and analyze data pertaining to the location and movement of all targets within a given scene. The construction of strokes does not require any position prediction, as the visual motion of targets is consistently insignificant when compared to their spatial dimensions. A binary association matrix is generated by testing overlaps between segments in successive frames. This matrix is subsequently utilized to establish the linkage between regions and their corresponding classification. The stroke undergoes revision upon the identification of each match. The act of monitoring also influences the identification process. When a target remains in a fixed position for an extended period, the tracker will integrate it with the surrounding background elements.

Classification

In order to successfully complete the classification assignment, it is imperative to address three key concerns. Firstly, it is necessary to determine the classes that should be taken into consideration. Secondly, it is important to identify the characteristics that most effectively differentiate these groups. Lastly, it is crucial to determine the classifiers that are most suitable for adapting to the aforementioned selections. The primary objective of classifiers is to achieve low probabilities of miss-classification, while considering a wide range of classes. Nevertheless, the classifier was designed to exclusively consider geometric characteristics, making it impractical to incorporate the element of time. The classifier obtained exhibits portability across different computer systems due to its independence from specific frame rates. The classes comprising numerous merged targets are not adequately characterized by a Gaussian distribution across the feature space. Parameterizing these entities can be a complex task due to their potential to exhibit diverse forms.

Resultantly, it is plausible to consider employing a non-parametric classifier, such as the K-Nearest Neighbors approach. Within each frame, the tracker and the classification task engage in communication to ascertain the appropriate category for each observed target. The aforementioned approach is employed to ascertain the ultimate classification for each stroke, taking into consideration the quantity of votes garnered. The classification of an object holds significant importance in various applications of surveillance. Video tracking-based systems utilized statistical analysis to efficiently distinguish between various types of movements, such as those made by humans, vehicles, doors, and trees, by considering factors such as size, shape, and speed of the moving objects. Face, pedestrian, and vehicle detection systems employ image analysis techniques to identify objects of specific categories, without requiring precise knowledge of their precise spatial coordinates or dimensions. Video tracking methods that utilize real-time tracking data are generally more efficient in locating and segmenting the target item compared to these methods, which often require more time for the same task.

Recognition

Just like the classification subsystem, the recognition function does not require the incorporation of temporal data. The purpose of this identification method is to quickly detect targets that undergo temporary disappearance due to obstructions or blending before reappearing and separating again. The models are described using PDF estimations of the chosen feature space, specifically color.

V. CONCLUSIONS AND FUTURE DIRECTIONS

Although cloud computing technology has experienced extensive adoption, the IoT has not kept pace. The first section of this paper presented a comprehensive examination of the concept of the IoT by delving into its historical roots and highlighting its initial advocate, Kevin Ashton, in the year 1999. Ashton has emerged as a prominent figure in the discourse surrounding the IoT, and his concepts have been embraced by Cisco. The paper subsequently provides a summary of the fundamental concept underlying the design of the IoT architecture. This concept revolves around the interaction and interdependence of three key dimensions, namely data points, decentralized networks, and smart programs. Consequently, the trajectory of the IoT architecture will be contingent upon the dynamic interaction among the physical and virtual realms, as well as the social dimension. In conclusion, an analysis is conducted to delineate the disparities between the traditional Internet framework and IoT. Section II of the paper examined the main overarching obstacles that had a significant effect on IoT performance. These challenges encompassed networking, communication, quality of service (QoS), virtualization, scalability, big data, security, and heterogeneity. The objective of this section was to demonstrate and present the most recent

strategies for every challenges. In the concluding segment, an examination was conducted on the diverse practical applications of the IoTcloud and IoT framework, encompassing domains such as smart cities, healthcare, smart grids, smart transportation, and others. Given the aforementioned points, it can be argued that the ecosystem of the IoT presents a promising avenue for scholarly investigation, specifically in relation to the integration of cloud computing. This area of study provides novel contexts for the effective administration of intelligent services and applications.

Data Availability
No data was used to support this study.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
No funding was received to assist with the preparation of this manuscript.

Ethics Approval and Consent to Participate
The research has consent for Ethical Approval and Consent to participate.

Competing Interests
There are no competing interests.

References

[1]. O. Eris, J. L. Drury, and D. Ercolini, "A collaboration-centric taxonomy of the internet of things: Implications for awareness support," Internet of Things, vol. 15, no. 100403, p. 100403, 2021.
[2]. K. Ashok, M. Ashraf, J. Thimmia Raja, M. Z. Hussain, D. K. Singh, and A. Haldorai, "Collaborative analysis of audio-visual speech synthesis with sensor measurements for regulating human–robot interaction," International Journal of System Assurance Engineering and Management, Aug. 2022, doi: 10.1007/s13198-022-01709-y.
[3]. L. Zhao, P. Pop, and S. Steinhorst, "Quantitative performance comparison of various traffic shapers in time-sensitive networking," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 3, pp. 2899–2928, 2022.
[4]. S. Misra, A. Gupta, P. V. Krishna, H. Agarwal, and M. S. Obaidat, "An adaptive learning approach for fault-tolerant routing in Internet of Things," in 2012 IEEE Wireless Communications and Networking Conference (WCNC), 2012.
[5]. Neha, P. Gupta, and M. A. Alam, "Challenges in the adaptation of IoT technology," in A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems, Cham: Springer International Publishing, 2022, pp. 347–369.
[6]. S. Panja, A. K. Chattopadhyay, and A. Nag, "A review of risks and threats on IoT layers," in Lecture Notes on Data Engineering and Communications Technologies, Singapore: Springer Singapore, 2021, pp. 735–747.
[7]. B. Emruli, F. Sandin, and J. Delsing, "Vector space architecture for emergent interoperability of systems by learning from demonstration," Biol. Inspired Cogn. Arch., vol. 11, pp. 53–64, 2015.
[8]. H and A. R, "Artificial Intelligence and Machine Learning for Enterprise Management," 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), Nov. 2019, doi: 10.1109/icssit46314.2019.8987964.
[9]. Y. Masoudi-Sobhanzadeh, H. Motieghader, Y. Omidi, and A. Masoudi-Nejad, "A machine learning method based on the genetic and world competitive contests algorithms for selecting genes or features in biological applications," Sci. Rep., vol. 11, no. 1, p. 3349, 2021.
[10]. L. Bittencourt et al., "The Internet of Things, Fog and Cloud continuum: Integration and challenges," Internet of Things, vol. 3–4, pp. 134–155, 2018.
[11]. M. Alarbi and H. Lutfiyya, "Sensing as a Service Middleware Architecture," in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 2018.
[12]. V. Joevivek et al., "Spatial and temporal correlation between beach and wave processes: implications for bar–berm sediment transition," Frontiers of Earth Science, vol. 12, no. 2, pp. 349–360, Jun. 2017, doi: 10.1007/s11707-017-0655-y.
[13]. K. A. Fararni, F. Nafis, B. Aghoutane, A. Yahyaouy, J. Riffi, and A. Sabri, "Hybrid recommender system for tourism based on big data and AI: A conceptual framework," Big Data Min. Anal., vol. 4, no. 1, pp. 47–55, 2021.
[14]. Haldorai, A. Ramu, and S. Murugan, "Computing and Communication Systems in Urban Development," Urban Computing, 2019, doi: 10.1007/978-3-030-26013-2.
[15]. J. Gomez-gualdron and M. Velez-Reyes, "Simulating a multi-agent based self-reconfigurable electric power distribution system," in 2006 IEEE Workshops on Computers in Power Electronics, 2006.
[16]. Haldorai and U. Kandaswamy, "Energy Efficient Network Selection for Cognitive Spectrum Handovers," EAI/Springer Innovations in Communication and Computing, pp. 41–64, 2019, doi: 10.1007/978-3-030-15416-5_3.
[17]. B. R. Ray, J. Abawajy, and M. Chowdhury, "Scalable RFID security framework and protocol supporting Internet of Things," Comput. Netw., vol. 67, pp. 89–103, 2014.
[18]. J. Bzai et al., "Machine learning-enabled Internet of Things (IoT): Data, applications, and industry perspective," Electronics (Basel), vol. 11, no. 17, p. 2676, 2022.
[19]. Y. Wang, H. Shibamura, K. Ng, and K. Inoue, "Implementation of edge-cloud cooperative CNN inference on an IoT platform," in 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), 2022.
[20]. S. Pasricha and A. Veidenbaum, "Improving branch prediction accuracy in embedded processors in the presence of context switches," in Proceedings 21st International Conference on Computer Design, 2004.
[21]. H. Li, M. Jia, and Z. Mao, "Dynamic reconstruction principal component analysis for process monitoring and fault detection in the cold rolling industry," J. Process Control, vol. 128, no. 103010, p. 103010, 2023.