JOURNAL OF THE ROYAL LAUREATES ACADEMY

www.rlaindia.org

REVIEW ARTICLE

NOVEL APPROACHES ON INTERNET OF THINGS: A COMPREHENSIVE REVIEW

Nirmalya Bose*

Department of Computer Application, Narula Institute of Technology, 81, Nilgunj Road, Agarpara, Kolkata - 700 109, West Bengal, India.

* Corresponding Author.

ABSTRACT:

The Internet of Things (IoT) has emerged as a novel paradigm that has transformed conventional lifestyles into a technologically advanced way of life. IoT has brought about significant developments in various sectors, such as smart cities, smart homes, pollution management, energy conservation, smart transportation, and smart industries. Researchers have conducted extensive studies and investigations to improve technology through the Internet of Things (IoT). Nevertheless, numerous obstacles and issues persist that necessitate attention in order to fully realize the potential of the Internet of Things (IoT). It is imperative to take into account a range of challenges and issues pertaining to the Internet of Things (IoT), encompassing applications, obstacles, enabling technology, as well as social and environmental ramifications.

KEYWORDS: Novel, Internet, Things.

INTRODUCTION:

The Internet of Things (IoT) is a conceptual framework that facilitates the exchange of information between electronic devices and sensors via the internet, with the aim of enhancing various aspects of human existence. On a global scale, the Internet of Things (IoT) leverages intelligent gadgets and the internet to offer inventive solutions to diverse challenges and concerns pertaining to a wide range of business, governmental, and public/private sectors. The Internet of Things (IoT) is becoming a significant aspect of our daily lives, permeating various aspects of our surroundings. The Internet of Things (IoT) is a comprehensive invention that integrates a wide range of intelligent systems, frameworks, devices, and sensors. Furthermore, it leverages the capabilities of quantum and nanotechnology to achieve unprecedented levels of storage, sensing, and computing speed that were previously inconceivable. Scholarly articles and news reports, both online and in printed formats, provide extensive research on the potential efficacy and practicality of Internet of Things (IoT) advancements. We can employ this approach as a first step before developing fresh and innovative business strategies, considering factors like security, assurance, and interoperability.

NOVEL APPROACHES:

The integration of Internet of Things (IoT) devices and technology has brought about a significant revolution in our daily routines. One notable advancement in the field of Internet of Things (IoT) is the emergence of smart home systems (SHS) and appliances, which encompass internet-connected gadgets, home automation systems, and dependable energy management systems. In addition, another significant accomplishment of the Internet of Things (IoT) is the Smart Health Sensing System (SHSS). To promote human well-being, SHSS integrates compact intelligent apparatuses and devices. Both indoor and outdoor settings can utilize these devices to assess and track various health conditions, fitness levels, and calorie expenditure within a fitness facility, among other applications. Additionally, it is employed for the purpose of monitoring crucial health situations in hospitals and trauma centers. Therefore, the integration of advanced technology and intelligent gadgets has significantly transformed the medical field. Furthermore, IoT developers and researchers are actively working to enhance the quality of life for individuals with disabilities and those in the senior age group. The Internet of Things (IoT) has demonstrated significant advancements in this domain, offering a novel trajectory for individuals' everyday existence in this context. Due to their cost-effectiveness in terms of development expenses and widespread availability within a reasonable price range, a significant number of individuals are utilizing these gadgets and equipment. The Internet of Things (IoT) has introduced several novel innovations aimed at enhancing efficiency, convenience, and reliability. Intelligent sensors and drone devices are facilitating traffic management at various signalized junctions in contemporary urban areas. Furthermore, there is a growing trend of introducing automobiles equipped with built-in sensing devices that can detect impending significant traffic congestion on the map. These gadgets can then recommend alternative routes with minimal traffic congestion. Thus, the Internet of Things (IoT) offers a multitude of applications in diverse domains of life and technology. We can infer that the Internet of Things (IoT) holds significant potential for technological advancement and human convenience.

The Internet of Things (IoT) has demonstrated its significance and potential in fostering economic and industrial advancement within a growing region. Furthermore, within the trade and stock exchange sectors, it is regarded as a groundbreaking advancement. The security of data and information is a significant concern and a highly sought-after objective, posing a substantial challenge. The internet, as a significant contributor to security concerns and cyber-attacks, has created several opportunities for hackers, resulting in compromised data and information security. Nevertheless, IoT is committed to providing optimal solutions to address data and information security concerns. Therefore, security is the primary concern of the IoT in trade and business. Hence, it is imperative for IoT developers to establish a secure pathway for integrating social networks while addressing privacy concerns.

The presence of security concerns in the context of edge data analytics has the potential to expose edge infrastructure to attacks or facilitate the occurrence of breaches that may be exploited at a later stage. Edge data analytics security solutions typically concentrate on centralized servers and network infrastructure, in contrast to traditional data processing settings like data centers or cloud platforms. However, in the realm of edge data analytics, where data processing takes place in close proximity to the data source on distributed devices, distinct security challenges emerge. These challenges encompass physical security risks, such as the potential for theft or tampering of edge devices, as well as network security threats, such as man-in-The-Middle attacks targeting data transmitted between edge devices and central servers. Additionally, there are risks associated with device compromise due to the limited resources and security features available on edge devices. Furthermore, the use of edge data analytics raises distinct questions about data privacy and integrity. This is because the edge processes sensitive data in close proximity, highlighting the importance of protecting data at its source.

The potential ramifications of security breaches in edge data analytics are significant, as they could compromise data privacy and system integrity, possibly contravening regulatory frameworks such as GDPR or HIPAA. The occurrence of unauthorized access to or exposure to sensitive data can lead to legal ramifications, erosion of trust, and harm to one's reputation. Integrity breaches have the potential to result in erroneous insights, posing a risk to the safety of vital systems. Data manipulation has the potential to mislead users or automated systems, influencing the process of decision-making. Service disruptions have the potential to affect business operations continuity and customer satisfaction. Additionally, financial losses may arise from remediation expenses, regulatory penalties, and a decline in revenue. The act of stealing intellectual property has the potential to erode both competitiveness and creativity.

Two often employed networks in edge-based traffic management applications are VANET (vehicular ad hoc network) and VSDN (vehicular software-defined networking). The significance of these networks lies in their ability to enhance driving efficiency, navigation, and information exchange in a decentralized network structure. A decentralized network structure is facilitated by a vehicular fog computing (VFC) network, which allows for the implementation of traffic schemes to enhance traffic management and road safety. Events such as traffic congestion, vehicular collisions, and road conditions are transmitted to edge nodes, which are in closer proximity to the units located along the roadside. Certain data collected at this particular level can be utilized for decision-making at the vehicle level, whereas other data undergoes processing by the servers located in the edge layer and is thereafter transmitted to the cloud. The cloud-based traffic control server transmits feedback messages to automobiles through edge nodes at roadside units. Insufficient authentication during data transmission to various nodes can result in malicious behaviors, such as unauthorized access to users' personal information or disruption of data integrity. A 5G-based intelligent transport system was developed to monitor traffic infraction reports by utilizing speed sensors on cars. A security mechanism incorporating a digital signature conducted the verification of location-based information. The edge nodes collect and consolidate numerous complaints of speed violations, authenticate them, and disseminate anonymous notifications to nearby entities. Based on these findings, the transportation authority is responsible for making decisions about traffic infractions involving automobiles. The implementation of a digital signature serves to reduce the potential for jamming, privacy infringement, and fake injection attacks. Therefore, the system achieves privacy in terms of information and location, mutual authentication, traceability, data confidentiality, and integrity. However, we do not consider hardware attacks that cause physical harm to sensor nodes or obstruct communication routes. These attacks have the potential to induce endless waiting times for the data at the edge nodes.

The implementation of smart city applications has significantly improved consumers' quality of life. Internet of Things (IoT) devices are crucial in these applications as they gather and detect real-time data. The data collected by users pertains to city supervision and utilities, including gas and lights. Within a system for video summarization, the edge nodes are responsible for gathering the acquired movies and generating an embedded vision. Additionally, the data is transmitted to the centralized servers located on the edge layer, which are interconnected by internet gateways. The servers function as master nodes, which in turn exercise control over the edge nodes. The servers transfer the embedded vision to the cloud using the MQTT communication protocol. Embedded vision significantly reduces the cloud's bandwidth usage. The MQTT protocol is susceptible to several security risks, including denial of service (DoS) attacks, floods, spoofing, tampering, and access control denial. These threats lead to the intentional loss or delay of information, the interception of sent data, the dissemination of numerous incorrect details, the impairment of decision-making effectiveness, and the obstruction of processing node resources.

The widespread adoption of artificial intelligence (AI) in edge computing, particularly in healthcare applications, is evident. The enhancement of the scope and computational efficiency of edge nodes is notably significant. Nevertheless, AI models present several challenges, including limited battery life, high power consumption, and the inability to handle delays, susceptibility to security risks, and a decline in reliability. BAN or WPAN connects the sensors in edge-based healthcare applications, enhancing IEEE communication standards.

Integrating energy harvesting techniques into edge computing for smart city applications provides a strong solution for protecting against data threats and ensuring the integrity, confidentiality, and authenticity of critical information. This helps preserve the longevity and processing capabilities of edge nodes in smart city applications.

We are developing trust management models in the context of edge computing. Decentralized edge computing faces a significant challenge in gathering and overseeing data from several edge nodes for the purpose of doing data analytics. The aforementioned criteria may exhibit variations across different apps and services. In addition, edge nodes may regularly transition between different areas.

Identifying and segregating the compromised edge nodes within the edge computing layer. Malicious nodes are the prevailing danger in the existing edge threat models, exerting a significant impact on the decision-making process. Malevolent nodes have the ability to consistently infiltrate other nodes and initiate additional attacks in the edge layer, such as denial of service (DoS), recurrent storage and processing requests, spoofing, or the exposure of sensitive information.

Strengthening security through the utilization of cutting-edge technology, such as artificial intelligence and block chain. Artificial intelligence algorithms have the ability to significantly contribute to the real-time identification of risks and anomalies at the edge layer. By continuously monitoring device behavior and network traffic, these algorithms can effectively identify possible security issues. Furthermore, AI-based methodologies can harness historical data to improve the precision and efficacy of security protocols within edge data analytics systems.

COMPREHENSIVE REVIEW:

Mahadevappa, Poornima et al. (2024). Edge data analytics pertains to the processing of data in close proximity to its sources at the periphery of the network, with the aim of minimizing delays in data transmission and facilitating instantaneous interactions. Nevertheless, the use of data analytics at the edge exposes a multitude of security vulnerabilities that can have an adverse effect on the processed data. As a result, it is critical to protect sensitive data from unauthorized access in order to avoid uncertainty and maintain the overall quality of the service provided. The majority of current edge security models have neglected to account for attacks that occur during data analysis. This paper presents a comprehensive examination of edge data analytics in the domains of healthcare, traffic management, and smart city applications. It includes an analysis of potential attacks and their consequences for the field of edge data analytics. Moreover, we conduct an investigation of existing models to gain insights into handling these attacks and identify areas requiring further study. In conclusion, this paper presents research directions aimed at improving data analytics at the edge. [1]

Asif, Rameez and Syed Raheel Hassan (2023). Both the Internet of Things (IoT) and the metaverse are dynamic technologies that possess the capacity to significantly influence the trajectory of our digital realm. The "Internet of Things" (IoT) refers to a network that connects physical devices, vehicles, buildings, and various items through the internet, enabling them to gather and exchange data. In contrast, the metaverse refers to a virtual environment wherein individuals have the ability to engage in real-time interactions with both fellow users and digital entities. This research study seeks to investigate the confluence of the Internet of Things (IoT) and the metaverse, with a focus on the potential and difficulties that emerge from this crossing. This study aims to explore the integration of Internet of Things (IoT) devices into the metaverse, with the objective of generating novel and engaging user experiences. Additionally, an examination will be conducted of the prospective use scenarios and implementations of this technology across diverse sectors, including healthcare, education, and entertainment. We will also scrutinize the privacy, security, and ethical issues that arise from the use of Internet of Things (IoT) devices in the metaverse. The survey methodology involves the integration of comprehensive literature research and a meticulous analysis of a case study. This paper aims to offer an analysis of the potential societal implications of the Internet of Things (IoT) and the metaverse, with the intention of informing the advancement of future technologies within this domain. [2]

Hassebo, Ahmed, and Mohamed Tealab. (2023). The world's growing urbanization necessitates the development of smart cities and the implementation of Internet of Things (IoT) applications. These initiatives are crucial in tackling urban difficulties and promoting the creation of sustainable and resilient urban settings. However, we must overcome obstacles like concerns about privacy and security, along with interoperability challenges. The resolution of these difficulties necessitates the establishment of collaborative efforts among governmental bodies, industry participants, and individuals to guarantee the conscientious and fair integration of Internet of Things (IoT) technology into smart urban environments. The Internet of Things (IoT) presents a wide range of opportunities for the implementation of smart city applications. It facilitates the seamless integration of diverse devices, sensors, and networks, allowing for the real-time collection and analysis of data. These applications, in addition to transportation, energy management, waste management, public safety, healthcare, and other industries, have a wide range of applications. Urban areas have the potential to optimize their infrastructure, optimize resource allocation, and improve their residents' overall quality of life through the use of Internet of Things (IoT) technology. This article presents eight worldwide models for smart cities, which aim to provide guidance for the development and implementation of Internet of Things (IoT) applications in such urban areas. These models offer structured frameworks and established criteria for urban planners and relevant parties to proficiently develop and implement Internet of Things (IoT) solutions. We conduct a comprehensive assessment of these models, utilizing nine evaluation indicators specific to smart cities. We have identified the aforementioned obstacles associated with the implementation of smart cities and put out corresponding proposals to address these challenges.[3]

Sgora, Aggeliki, and Periklis Chatzimisios (2022). The increasing prevalence of multimedia services has led to a significant focus on quality of experience (QoE). Quality of Experience (QoE) encompasses the integration of users' requirements and anticipations with multimedia applications and network performance. However, in various Internet of Things (IoT) applications such as healthcare, surveillance systems, and traffic monitoring, the availability of human feedback may be limited or unfeasible. Furthermore, when assessing the quality of immersive augmented and virtual reality, as well as other multimedia applications, it is imperative to include factors outside the visual and auditory senses. Hence, the conventional definition and methods of quality of experience (QoE) for assessing multimedia services may not be appropriate for the Internet of

Things (IoT) paradigm. Consequently, additional quality metrics are necessary to evaluate the quality of IoT. This study provides a comprehensive analysis of current quality definitions, quality influencing factors (IFs), and assessment methodologies for the Internet of Things (IoT). This research additionally presents problems pertaining to quality assessment within the Internet of Things (IoT) paradigm. [4]

Mouha, R.A. (2021). Presently, there is a significant global trend towards modern technology, with specialized companies undergoing a rapid advancement in information technology towards the Internet of Things (IoT) or Internet of Objects. The Internet of Things (IoT) refers to the integration of objects with the Internet, utilizing hardware and/or software to enable intelligent communication and effective participation in various aspects of daily life. This facilitates new forms of communication between individuals and objects, as well as between objects themselves. This transformation will elevate traditional lifestyles to a more sophisticated standard. However, the task at hand will not be without challenges, as we must confront numerous obstacles and concerns from multiple perspectives to fully harness their capabilities. The primary aim of this review article is to offer the reader an in-depth analysis from both a technological and sociological standpoint. The conversation revolved around the diverse challenges and issues, as well as the definition and design of IoT. Moreover, an elucidation of several sensors and actuators, together with their intelligent communication, Furthermore, the key domains of the IoT were showcased. This study aims to enhance readers' and researchers' comprehension of the Internet of Things (IoT) and its prospective implementation in practical contexts. [5]

Antima Bhimrao Shendge (2021). This article specifically examines the prospective uses of the Internet of Things. A network of physical objects, sometimes referred to as "things," equipped with sensors, software, and various technologies is known as the Internet of Things (IoT). The design of these objects enables them to establish connections and streamline data exchange with other devices and systems via the Internet. Recognizing the various applications of the Internet of Things (IoT) and the associated research challenges is crucial as the technology progresses. The Internet of Things (IoT) is anticipated to permeate many domains of everyday life, including smart cities, healthcare, smart agriculture, logistics, retail, smart living, and smart environments. Despite the significant advancements in IoT-enabling technologies in recent years, there remain unresolved issues that necessitate attention. Since the Internet of Things (IoT) stems from a blend of various technologies, it's inevitable that a multitude of research challenges will surface. The extensive reach and pervasive impact of the Internet of Things (IoT) render it a noteworthy subject of investigation within several domains, including information technology and computer science. Therefore, the Internet of Things (IoT) is facilitating the exploration of novel avenues for study. This paper provides an overview of the latest advancements in Internet of Things (IoT) technologies and explores potential future uses and research obstacles. [6]

Nižetić, Sandro et al. (2020). The expeditious progress and integration of intelligent and Internet of Things (IoT) technologies have facilitated diverse prospects for technological breakthroughs across many domains of human existence. . The primary objective of Internet of Things (IoT) technology is to streamline operations across several domains, thereby enhancing the efficacy of systems, technologies, or specialized processes and ultimately enhancing the overall quality of life. . Sustainability has emerged as a crucial concern for the population due to the rapid advancement of IoT technologies, which offer various advantageous outcomes. . However, it is imperative to closely monitor and assess this rapid development from an environmental perspective in order to mitigate any detrimental effects and ensure the efficient utilization of limited global resources. . Considerable study endeavors are required in the aforementioned context to thoroughly examine the advantages and disadvantages of Internet of Things (IoT) technology. . This review editorial focuses on the scientific contributions presented at the 4th International Conference on Smart and Sustainable Technologies, which took place in Split and Bol, Croatia, in 2019. . Additionally, it also incorporates recent results from the literature. . The SpliTech 2019 conference proved to be a highly important event that effectively facilitated the connection between various engineering professionals, industry specialists, and academic researchers. . The conference's primary emphasis was on prominent conference tracks, including Smart City, Energy/Environment, e-Health, and Engineering Modeling. . The research presented and deliberated upon during the SpliTech 2019 conference contributed to the comprehension of the intricate and interconnected impacts of Internet of Things (IoT) technologies on societies, as well as its potential implications for sustainability at large. . The paper examined diverse domains of Internet of Things (IoT) technology and the advancements achieved in these areas. . The editorial covered four primary subject areas, including the most recent developments in these domains. Internet of Things (IoT) technologies in sustainable energy and environment, IoT-enabled smart cities, e-health (ambient-Ambient supported living systems), and IoT technologies in transportation and low-carbon products . The primary findings of the initial article review have enhanced comprehension of the present advancements in IoT application domains as well as the environmental consequences associated with the growing utilization of IoT items. [7]

Kumar, S., Tiwari, P. & Zymbler, M. (2019). The year 2019. A smart city is a popular use of the Internet of Things (IoT) that includes smart homes. A smart home is comprised of Internet of Things (IoT)-equipped household appliances, air-conditioning and heating systems, televisions, audio and video streaming devices, and security systems that communicate with each other to ensure optimal comfort, security, and energy efficiency. The communication occurs only through an Internet of Things (IoT)-based central control unit. The notion of a smart city has garnered significant attention in the past decade and has sparked extensive research endeavors. By 2022, projections indicate that the smart home industry will surpass a market value of 100 billion dollars. Smart home technology not only improves indoor comfort, but also offers homeowners cost-saving benefits. For instance, by reducing energy consumption, homeowners can expect to incur cheaper electricity bills. Smart cities encompass not only smart homes but also smart vehicles. Sophisticated electronics and sensors outfit contemporary vehicles, regulating everything from the headlights to the engine. Smart automotive systems, which integrate wireless communication between vehicles and between vehicles and drivers, are the focus of the Internet of Things (IoT). This integration aims to facilitate predictive maintenance and enhance the driving experience by providing a comfortable and safe environment. [8]

Alavi AH et al. (2018). The phenomenon of urbanization in urban areas. The phenomenon of individuals migrating from rural to urban environments has led to a significant increase in the population of cities. Hence, it is imperative to offer intelligent solutions for transportation, energy, healthcare, and infrastructure. IoT developers consider smart cities to be a significant domain for applications. It examines various topics like traffic control, air pollution control, public safety measures, intelligent parking, intelligent lighting, and intelligent waste disposal. The authors indicated that the Internet of Things (IoT) is actively addressing these complex challenges. The increasing urbanization has created opportunities for entrepreneurs in the smart city technology sector, as there is a growing demand for enhanced smart city infrastructure. The researchers reached the conclusion that the integration of IoT-enabled technology plays a crucial role in the advancement of sustainable smart cities. [9]

Khajenasiri I et al. (2017). An examination of IoT options for intelligent energy management to enhance the functionality of smart city applications. They asserted that IoT currently serves both technology and individuals in a limited number of application domains. The Internet of Things (IoT) possesses a broad scope, and in the foreseeable future, it is poised to encompass nearly all domains of application. They stated that energy conservation is a crucial aspect of civilization, and the Internet of Things (IoT) can aid in the creation of an intelligent energy management system that can effectively conserve both energy and financial resources. They outlined an Internet of Things (IoT) framework in relation to the concept of a smart city. The authors also addressed the issue of IoT hardware and software immaturity as a significant challenge in achieving this goal. The resolution of these difficulties is crucial for establishing a dependable, effective, and user-centric Internet of Things (IoT) system. [10]

CONCLUSION:

An Internet of Things (IoT) system consists of a vast array of devices and sensors that engage in communication with one another. The proliferation and expansion of the Internet of Things (IoT) network have led to a significant rise in the quantity of sensors and devices within this domain. These gadgets engage in intercommunication and facilitate the transmission of a substantial volume of data via the internet. This data has a substantial volume and is continuously flowing, making it suitable for classification as big data. The ongoing growth of IoT networks presents intricate challenges, including data management, data collection, storage, processing, and analytics. The Internet of Things (IoT) big data framework is highly advantageous in addressing several challenges associated with smart buildings, including the management of oxygen levels, measurement of smoke and dangerous gases, and assessment of brightness. The latest developments in the Internet of Things (IoT) have captured the interest of researchers and developers globally. Collaboration between IoT developers and researchers aims to expand the technology on a large scale and maximize its societal benefits. However, we can only achieve enhancements by considering the diverse concerns and deficiencies in the current technical methodologies. The Internet of Things (IoT) not only offers services but also produces a substantial volume of data.

REFERENCES:

1. Mahadevappa, Poornima, Redhwan Al-amri, Gamal Alkawsi, Ammar Ahmed Alkahtani, Mohammed Fahad Alghenaim, and Mohammed Alsamman. (2024). Analyzing Threats and Attacks in Edge Data Analytics within IoT Environments. IoT 5, no. 1: 123-154. https://doi.org/10.3390/iot5010007

2. Asif, Rameez, and Syed Raheel Hassan. (2023). Exploring the Confluence of IoT and Metaverse: Future Opportunities and Challenges. IoT 4, no. 3: 412-429. https://doi.org/10.3390/iot4030018

3. Hassebo, Ahmed, and Mohamed Tealab. (2023). Global Models of Smart Cities and Potential IoT Applications: A Review. IoT 4, no. 3: 366-411. https://doi.org/10.3390/iot4030017

4. Sgora, Aggeliki, and Periklis Chatzimisios (2022). Defining and Assessing Quality in IoT Environments: A Survey. IoT 3, no. 4: 493-506. https://doi.org/10.3390/iot3040026

5. Mouha, R.A. (2021). Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9, 77-101. https://doi.org/10.4236/jdaip.2021.92006

6. Antima Bhimrao Shendge (2021). Internet of Things (IoT): An Overview on Research Challenges and Future Applications, International Journal of Engineering Applied Sciences and Technology, 6(8): 66-71.

7. Nižetić, Sandro et al. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. Journal of cleaner production vol. 274 (2020): 122877. doi:10.1016/j.jclepro.2020.122877.

8. Kumar, S., Tiwari, P. & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111. https://doi.org/10.1186/s40537-019-0268-2

9. Alavi AH, Jiao P, Buttlar WG, Lajnef N. (2018). Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement, 129: 589–606.

10. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. (2017). A review on internet of things for intelligent energy control in buildings for smart city applications. Energy Procedia; 111:770–9.