MATHEMATICAL MODELING AND COMPUTING, Vol. 10, No. 3, pp. 796–806 (2023)

Challenges and issues for Internet of Things (IoT): recent survey

Guéro A.-M. M., Chiba Z., Abghour N.

Department of Mathematics and Computer Science,
Faculty of Sciences Ain Chock, Hassan II University of Casablanca,
LIS Labs, Casablanca, Morocco

(Received 18 February 2023; Revised 19 July 2023; Accepted 20 July 2023)

The Internet of Things (IoT) is one of the most emerging and revolutionary technologies of this century. The IoT is a network of dedicated devices called things deployed and used to collect, handle and exchange real-world data over the Internet or other networks. Combined with automation systems, IoT devices can help manage, monitor, and alert users to the changes in their environment, assist them to make smarter decisions, facilitate daily life, and contribute to the development of the economy and industry. Nevertheless, the exponential growth of IoT equipment as well as the absence of common international standards leads to huge challenges, among which are security and performance. Indeed, with an increasing number of devices, the old methods of managing connected devices become inappropriate, which creates security breaches. Furthermore, the limited resources of IoT devices besides the nature of their network prevent the implementation of strong and sophisticated security measures on them. As a result, IoT appliances are vulnerable and prone to many security threats and intrusions. This paper presents an overview of IoT issues and challenges. Also, it exhibits a deep analysis of the solutions proposed in the literature for these issues. This assists to mark the concerns that still require to be handled, well outlines the mainstream of research direction, and clears the way for new avenues of research for forthcoming researchers. Finally, we deliver a guide or support for scientists interested in the Internet of Things.

Keywords: *Internet of Things; challenges; issues; IoT performance; IoT security.*
2010 MSC: 68M10, 68M11, 68M12, 68M20, 68P20 **DOI:** 10.23939/mmc2023.03.796

1. Introduction

The Internet of Things (IoT) refers to the next evolution of the Internet that will enable a networking infrastructure that connects a large number of devices to allow them to collect data and communicate with each other in order to make processed smart decisions [1]. It is important to note that devices, in this case, refer to any object embedded with the necessary hardware and software to support processing and networking capabilities. IoT provides businesses with applications that they can use to control their assets and come up with efficient and cost-effective business models. This technology is also an enabler of a hyper-connected society and can be used to optimize transportation and mobility [2]. However, this hyper-connected society accentuates the evolution of connected devices number.

Indeed, billions of things (i.e. smart devices) are being connected to communicate, collect and exchange data including smart phones, smart watch, smart bracelets, RFID tags, smart vehicles, sensors, and actuators. These devices are exponentially growing as they have the potential to provide unlimited benefits to our society. According to the latest available data, there are approximately 7.74 billion connected IoT devices. But thanks to 5G and other technologies, this figure is expected to increase more than 3 times to reach 25.44 billion total IoT devices by 2030 [3] (Figure 1). This growth does not come without its share of issues and challenges.

With its fast development, IoT technology faces a lot of security, performance, and privacy challenges that need to be addressed to enhance its acceptance and use [4]. Indeed, without a clear appreciation of the challenges posed by the security and privacy issues related to the IoT and the

possible solutions to the problems, the success of this technology and the privacy of potential users face significant peril. In addition to giving an overview of the problems and challenges of IoT, this paper exposes and analyzes the solutions proposed in the literature.

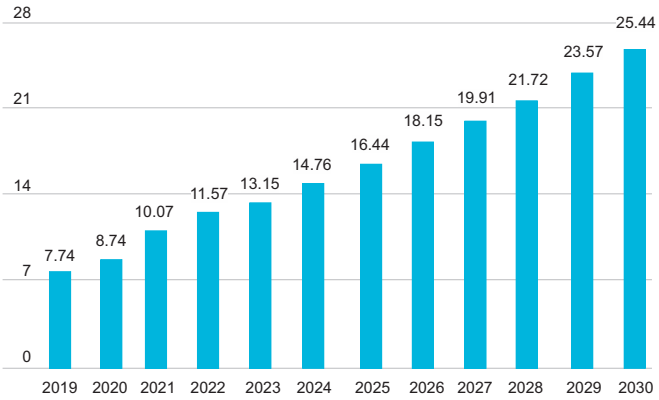

Fig. 1. Growth in the number of IoT devices.

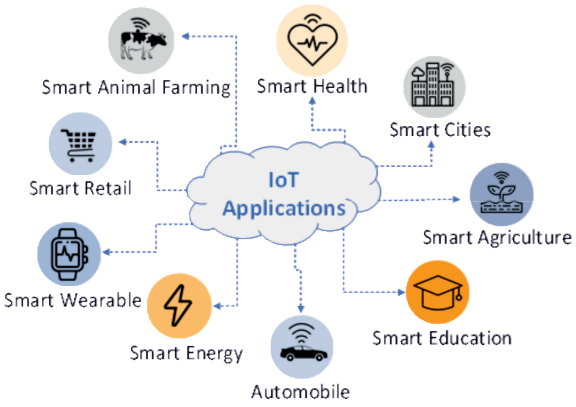

Fig. 2. IoT application.

Our main contribution compared to existing survey in IoT area are:

— In the current study, we analyze thoroughly numerous recent, and pertinent works for IoT developed between 2021 and 2023.
— Our paper meanwhile, in addition to giving a background on the Internet of Things, it gives the challenges, the issues.
— The survey papers [5–7] all point to certain limitations, including lack of in-depth and critical analysis, also surveys does not include any empirical research or experimental results, which could have added more weight to the conclusions.
— In our work, we focus essentially in identification of the strong points and limitations of these recent papers. This aids to spot the issues that still need to be tackled, well define the mainstream of research direction, and clear the way for new avenues of research for future researchers. Other particularity of our work, we afford in section Discussion relevant guidelines and recommendations for new scientists in domain of IoT. As it is done in the articles [8, 9].

The rest of this paper is organized as follows: Section 2 gives a brief overview of the IoT architecture and its application areas. While Section 3 exposes the issues and challenges of the Internet of things. The Section 4 is dedicated to the analysis of existing work. In the Section 5, a discussion on these recent articles is made. Also, some recommendations are giving to future researchers in this field. And finally, we end with conclusion.

2. Theoretical background

IoT is a need in today's life. There can be many IoT-enabled applications such as smart parking, smart animal farming, smart waste management system, smart grid, smart cities, etc. Some of the applications of this technology are shown in Figure 2.

On the other hand, regarding the IoT architecture, many of researches agree on three layers (Figure 3). They are: Perception layer, Network layer and Application layer [10].

Perception layer: It is first layer in IoT composition. The role of this layer is to collect and send data to the Network layer. It collects the data from sensors which are attached to the various IoT gadgets. There are various types of sensors which sense different physical properties. It also does some initial processing on collected data [10].

Network layer: It is the layer placed in between of three tiers in IoT composition. The role of this layer is to route and transmit the data received from Perception layer. Data may be passed by using Web as a media. Various protocols used at this layer are Bluetooth, Zigbee, Wi-Fi [10].

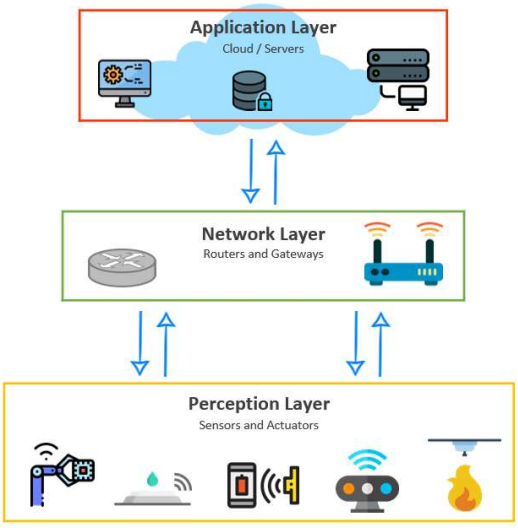

Fig. 3. Three layers of IoT architecture.

Application layer: It displays applications to end stakeholders for specialized ambition. For example, Smart Home application, Smart City application. The application layer process the data received from Network layer and produces end result according to purpose of specific IoT application [10].

3. The IoT issues and challenges

The Internet of Things, being a new technology, has countless issues and challenges. These are present on all layers of the architecture. In the following points, we will present the most critical challenges and issues.

3.1. Challenges

The Internet of Things presents countless challenges. Among these, we can cite:

Data management: The IoT can generate huge volumes of data, and organizations need to be able to efficiently manage, store, process, and analyze this data to get the most out of their IoT systems.

Power: In some circumstances, managing power supplies for IoT devices can be challenging, especially devices located in hard-to-reach places or those that rely on battery power.

Device management: Managing IoT devices can be an overwhelming undertaking for even the most experienced IT administrators, who often need to take extra steps to monitor and manage these devices.

Network connectivity: Maintaining network connectivity for multiple types of IoT devices can be a significant challenge, especially when these devices are highly distributed or in remote locations or if bandwidth is severely limited.

IoT standards: The lack of common IoT standards can make it difficult to deploy and manage a large number of IoT devices from different vendors and based on very different proprietary technologies.

System reliability: Ensuring the reliability of an IoT system can be difficult because IoT devices are highly distributed and often have to deal with several Internet traffic. Natural disasters, disruptions to cloud services, power outages, system failures, or other conditions can affect the components that make up an IoT system.

Government regulations: Complying with government regulations is another big challenge with IoT, especially if you operate in multiple regions or in regions where regulations conflict or change frequently.

3.2. Issues

The biggest issues of the IoT are security and performance. Indeed, the lack of resources for IoT devices prevents the implementation of strong and sophisticated security measures to preserve the confidentiality, authenticity, and integrity of the data transmitted by these objects. As a result, IoT appliances are vulnerable and prone to many security threats and intrusions.

Security: IoT systems face security threats from many fronts, botnets, ransomware, domain name server threats, shadow IT, physical vulnerabilities and other sources. Furthermore, organizations need to be able to protect their IoT devices, their network infrastructure, their on-premises computing and storage resources, and all data provided with the IoT.

Performance: Most IoT devices have limited resources due to their small size. This resource limit means that their performance is limited. Thus, it is difficult to implement energy and resource-intensive operations.

Scalability: Is another major research issue that has to be addressed because a large number of devices are going to be connected to IoT network. Data generated by these devices are very large, so the scalability issue must be considered while storing data, transmitting data and existing protocols for IoT must work even when size of the network keeps on increasing.

Energy efficiency: Since, devices have constraints in memory, processing power and battery life, etc. Therefore, IoT implementations must consider the constraints and use the battery power of devices efficiently. It can be done using smart processing of data, i.e., instead of sending data to every other device in the network, some processing must be done and then send to the required devices, we can also use the computing power of firewalls instead of totally using devices computing power.

4. Analysis of works on IoT

In this section, an analysis of recent works in the literature on the Internet of Things is done. It outlines the strengths and limitations of each of these works.

4.1. Proposed framework for IoT

Blockchain technology was suitable to solve security issues in IoT. Blockchain is a decentralized system that relies on user anonymity and further guarantees data integrity. However, adopting Blockchain in the IoT is not that easy. Indeed, IoT devices suffer from low computing power that will not be capable of running encryption algorithms rapidly. Marah R. et al. [11] propose an Enhanced Rich-Thin-Client architecture (ERTCA) to address the limitations of IoT devices. ERTCA is a proposed architecture that integrates IoT and Blockchain at any application, smart homes, smart city, smart manufacturing, or health care.

Zhang et al. [12] presents a framework for evaluating the energy performance of different retrofit packages for a reference building located in British Columbia, Canada. The framework uses artificial neural networks (ANNs) to predict natural gas and electricity consumption and a multi-objective optimization method to identify Pareto optimal retrofit solutions. The prediction performance of the ANN model was measured using the R2, RMSE, and MAE indicators, and was found to be good with an average coefficient of determination score of 0.995 and 0.991 for natural gas and electricity consumption, respectively. The study then used the carbon emissions and life cycle costs to identify Pareto optimal retrofit solutions, which can help decision-makers choose the best retrofit scenario based on their budgets and emission reduction targets.

S. Arumugam, et al. [13] proposes a secure and privacy-preserving Internet of Things (IoT) framework for healthcare applications. The proposed framework uses an encryption-based data protection mechanism and a user authentication mechanism to ensure the confidentiality and integrity of sensitive patient data. The framework is evaluated using a real-world medical dataset, and the results show that it can provide efficient and secure data transmission for healthcare applications.

4.2. Energy efficiency and IoT

Energy is a critical factor to be considered in electrical and electronic systems. With the advent of technology, numerous techniques have been developed in communication systems to make the systems reliable, durable, and economic.

In modern communication systems, the major requirements of an efficient radio model are to improve the delay and throughput, reduce the energy consumption, and extend the network lifetime. So, there is a need to design a radio model to improve the quality of service (QoS) parameters. From the limitations identified in the wireless communication networks, Premkumar C. et al. [14] proposed an Enhanced Energy-Efficient Fuzzy-based Cognitive Radio (EEFCR) scheme for Internet of things (IoT) networks. The proposed protocol is compared with the conventional method, Cognitive Radio-based Heterogeneous Wireless Sensor Area Network (CoRHAN).

A. Ahmed et al. [15] proposes an Energy-Efficient Data Aggregation Mechanism (EEDAM) for IoT that is secured by blockchain technology. The growing importance of IoT devices has resulted

Table 1. Summary of Recent Framework for IoT.

Ref.	Methods	Strengths	Limitations
[11]	Blockchain: Enhanced Rich-Thin-Client architecture (ERTCA).	This contribution solves some of the problems that other integration methods suffer, such as the limitation in resources at the IoT layer, and the difficulty in implementation at the blockchain layer. This framework provides a solution to distribute the load in a way that IoT devices can tolerate.	As a limitation of this method, we can point out that it has been tested and evaluated only on health care systems. In addition, the blockchain environment on which the solution was tested is unique, Ethereum. Although, the system can be scalable to thin clients; due to task simplicity and low latency. But at the rich client level, it may suffer at some point due to the necessary computing power and storage for recording Blockchain transactions.
[12]	ANNs for consumption prediction and multi-objective optimization for retrofit solutions.	The use of ANNs to predict energy consumption, which allows for accurate and efficient evaluation of retrofit scenarios. The use of a multi-objective optimization method to identify Pareto optimal retrofit solutions, which takes into account both carbon emissions and cost impacts. The consideration of both energy consumption and carbon emissions, which provides a more comprehensive evaluation of retrofit packages.	The study only considers a single reference building located in British Columbia, Canada, and it is uncertain if the results can be generalized to other building types and locations. The study assumes equal weights for the carbon emissions and cost objectives, but decision-makers may prioritize one objective over the other. The study only considers energy consumption and carbon emissions, and does not take into account other factors such as building materials and occupant comfort.
[13]	Framework uses encryption and authentication to protect patient data confidentiality and integrity.	The proposed framework provides a comprehensive approach for securing IoT-based healthcare applications, including data protection, user authentication, and secure data transmission. The evaluation of the framework is based on a real-world medical dataset, which enhances the validity and reliability of the results. The framework has the potential to improve the security and privacy of patient data in IoT-based healthcare applications, which is an important concern in the field.	The proposed framework assumes that the encryption-based data protection mechanism and user authentication mechanism are reliable and effective, which may not always be the case. The evaluation of the framework is based on a specific medical dataset, and the results may not be generalizable to other healthcare applications. The paper does not discuss the performance implications of the proposed framework, such as the processing time and energy consumption.

in an increased volume of data that needs to be processed and transmitted. The current Internet infrastructure is not efficient enough to handle this massive volume of data, which leads to issues such as transmission collision, security issues, and energy dissipation. To address these issues, the EEDAM uses data aggregation at the cluster level to reduce data redundancy and save energy. Blockchain technology is integrated with edge computing to provide secure services to IoT devices. The proposed mechanism was evaluated through simulations, and the results showed that it was able to reduce the amount of data transmitted, provide proper security to the IoT, and extend the life of the wireless sensor network (WSN). The authors concluded that there is a need for a decentralized architecture for IoT networks to overcome the limitations of centralized cloud servers and provide efficient, reliable, and secure services to end-users.

X. Zhang et al. [16] paper describes the development and analysis of a predictive energy consumption model for intelligent IoT-enabled cities. The model incorporates various prediction models such as neural networks and decision-making processes to reduce energy consumption and achieve social benefits. The Internet of Things assisted smart green energy (IoT-SGE) model resolves issues related to energy demand, unidirectional information flow, reliability, energy wastage, and security compared to conventional power grids. The proposed model is validated using an Omnet++ simulator scenario with 60 residences and 2 industries, and its performance is compared to existing methods such as JODRBRL, SEES, and REMS-SCMG. The metrics considered for analysis are operational logs, power wastage, power requirement, and average failure ratio.

C. Tipantuna and X. Hesselbach [17] presents a PHRASE (Power Management using PHAsed Energy Shifting) strategy for energy management in smart homes. The strategy aims to optimize energy consumption in a small-scale and home energy management system (HEMS) scenario by using a combination of time-shifting and quality degradation mechanisms.

Table 2. Summary of Energy Efficiency Means in IoT.

Ref.	Methods	Strengths	Limitations
[14]	Enhanced Energy-Efficient Fuzzy-based Cognitive Radio (EEFCR).	EEFCR protocol has higher goodput, lower bit error rate, faster computational time, and lower delay compared to other methods. The protocol also has an 80% reduction in sensing time and 53% increase in spectrum utilization. The average bit error is reduced up to 5%.	Despite the fact that the method actually works effectively, it is more appropriate for latency-tolerant devices than for real-time applications.
[15]	Energy-Efficient Data Aggregation Mechanism (EEDAM) for IoT that is secured by blockchain technology.	Energy-efficient: The proposed method reduces energy consumption compared to the other two protocols, making it a better choice for IoT devices with limited energy resources. Good performance with variable node densities: The proposed method shows stability in the number of cluster heads (CHs) selected, even when the node density is high. Improved data accuracy: The proposed method has a better data accuracy compared to the other two protocols. Reduced time delay: The proposed method reduces the time delay in data transmission, leading to improved network throughput.	High time delay with high node densities: The proposed method still shows a higher time delay compared to the other two protocols when the node density is high. Complex mechanism: The proposed method involves a more complex mechanism compared to the other two protocols.
[16]	Model uses prediction models and decision-making to reduce energy consumption and achieve social benefits.	Reduced energy consumption leading to social benefits. Improved energy demand and reliability. Seamless and continuous operation of the power grid. Minimization of power wastage.	The need for precise balancing of power requirement and power dissipation to improve efficiency. The need for a smart error management system for state transactions. The need for energy-related information to be accumulated through different devices in the cloud. The need for the cloud to have sufficient storage capacity.
[17]	Power Management using PHAsed Energy Shifting strategy for energy management in smart homes.	It leads to optimized energy consumption, reflected in an increase in energy available for use and energy allocation rate and a decrease in power reserve and power lacking rate. It produces adaptive consumption and high-quality results compared to those obtained with an optimal solution, while having a lower computational complexity. It runs much faster (90 times faster in the offline approach) than the optimal solution and can exceed the limits imposed on the optimal solution in terms of the number of services and the value of time-shifting. It is a feasible solution in a variety of application environments such as HEMS, and can be executed with a reasonable running time using a small amount of computational capacity, making it suitable for deployment in embedded devices with limited computational resources.	Its performance may be lower than that of the optimal solution in diverse scenarios. The algorithmic strategy may not achieve optimal solutions and future research could address the development and evaluation of adaptive solutions based on genetic algorithms or dynamic programming. The improvement in the energy allocation rate may appear to be insignificant as it is produced by the rejection of several small energy demands.

4.3. Security for IoT

The article of Tohid Shekari et al. [18] focuses on the countermeasures against the MaDIoT 2.0 attack. The authors suggest that the most effective way to prevent these attacks is to update the protection schemes of the power grid. The main protection schemes involved during MaDIoT 2.0 attacks are UFLS and UVLS, but these are not designed to deal with IoT botnet attacks. The authors suggest that by using the voltage falling rate of grid nodes as an indicator, it is possible to detect the region of the attack and drop the loads accordingly. They modified the UFLS and UVLS schemes to achieve this and the results showed that the F-1 score of the studied attack mechanisms significantly decreased. The modified UFLS algorithm was also tested against natural events and was able to recover the system stability. However, further in-depth analysis is required to verify its effectiveness and identify any weaknesses against natural events.

M. A. Alsmirat and M. Alenezi [19] proposes an efficient security mechanism for Internet of Things (IoT) networks using blockchain technology. The proposed mechanism uses a distributed ledger to store and manage IoT data, and a consensus mechanism to ensure the integrity and confidentiality of the data. The performance of the mechanism is evaluated using a real-world dataset, and the results show that it can provide efficient and secure data management for IoT networks.

Table 3. Summary of Security for IoT.

Ref.	Methods	Strengths	Limitations
[18]	MaDIoT 2.0 attack	Adaptive protection scheme that drops loads in the region where the voltage falling rate is higher than other nodes, which helps the grid to recover from the attack and prevent a system-wide blackout. The modified UFLS algorithm is able to recover system stability following both MaDIoT 2.0 attacks and natural events, as it drops similar amount of loads as the conventional UFLS algorithm.	Difficulty in detecting and identifying the location of the MaDIoT 2.0 attack in the grid, which is needed to determine where to drop loads. Further in-depth analysis is required to verify the effectiveness of the modified protection scheme against natural events and identify any possible weaknesses. Reliance on the voltage falling rate of grid nodes as the indicator to detect the region of the manipulation of demand attack, which may not always be a reliable indicator.
[19]	Efficient security mechanism for IoT networks using blockchain technology	The proposed security mechanism provides a comprehensive approach for securing IoT networks using blockchain technology. The mechanism uses a distributed ledger and consensus mechanism to ensure the integrity and confidentiality of IoT data, which is a significant concern in the field. The evaluation of the mechanism is based on a real-world dataset, which enhances the validity and reliability of the results.	The paper does not discuss the scalability of the proposed mechanism, which may be a significant challenge for large-scale IoT networks. The proposed mechanism assumes that all IoT devices are capable of participating in the consensus mechanism, which may not always be the case. The paper does not discuss the energy consumption and processing time implications of the proposed mechanism.

4.4. Intrusion detection for IoT

Using intrusion detection approaches are important for identifying attacks and taking appropriate countermeasures for each specific threat, especially for IoT. De Souza et al. [20] presents a two-step approach for intrusion detection and identification. The first step performs a traffic analysis with an Extra Tree binary classifier. Events detected as intrusive are analyzed in the second stage by an ensemble approach consisting of Extra Tree, Random Forest, and Deep Neural Network.

Due to the resource limitations of Internet of Things devices, the performance of most security measures is degraded. Thus, Amir Basati et al. [21] presents a new lightweight architecture based on Parallel Deep Auto-Encoder (PDAE) that uses both local and surrounding information around individual values in the feature vector. This type of feature separation helps increase model accuracy while dramatically reducing the number of parameters, memory footprint, and need for processing power.

Table 4. Summary of Intrusion Detection for IoT.

Ref.	Methods	Strengths	Limitations
[20]	Two-step approach for intrusion detection and identification using Extra Tree, Random Forest, and Deep Neural Network	Experimental outcomes obtained based on BotIoT, IoTID20, NSLKDD, and CICIDS2018 datasets show that the IDS developed achieves high rates (between 99% and 100%) of DR, Recall, Precision, and Balanced Accuracy.	Unfortunately, the prediction time is high compared to KNN, RF and NB techniques. It should be reduced. Additionally, the robustness of this IDS against network routing attacks such as sinkhole, wormhole, and selective forwarding has not been evaluated.
[21]	New lightweight architecture based on Parallel Deep Auto-Encoder (PDAE)	The advantages of this method are that it has a lightweight and efficient architecture of NN, it requires few numbers of parameters, and tests have yielded a high accuracy of 99.37%.	However, to evaluate the performance of the proposed IDS, the false alarm rate was not used. Moreover, to assess the low computational complexity of the proposed model, the detection time metric was not used.

4.5. Performance and IoT

Alkhateeb et al. [22] proposes a real-time performance optimization approach for IoT-based systems using machine learning techniques. The approach uses a decision tree algorithm to predict the response time and energy consumption of IoT devices based on the available network resources and application requirements. The proposed approach is evaluated on a real-world IoT testbed, and the results show that it can improve the performance of IoT-based systems by reducing the response time and energy consumption.

M. H. Khalid, et al. [23] presents a performance evaluation of LoRaWAN technology in IoT-based industrial automation. The evaluation is based on the analysis of network coverage, capacity, reliabil-

ity, and energy consumption of a LoRaWAN-based IoT network. The results show that LoRaWAN technology can provide efficient and reliable connectivity for IoT-based industrial automation systems, with low energy consumption and high scalability.

Table 5. Summary of Performance in IoT.

Ref.	Methods	Strengths	Limitations
[22]	A real-time performance optimization approach for IoT-based systems using machine learning techniques	The proposed approach is based on machine learning techniques, which can adapt to changing network conditions and application requirements in real-time. The approach can be applied to a wide range of IoT-based systems, including smart homes, industrial automation, and healthcare applications. The proposed approach is evaluated on a real-world IoT testbed, which enhances the validity and reliability of the results.	The proposed approach is evaluated on a specific IoT testbed, and the results may not be generalizable to other IoT systems. The approach assumes that the decision tree algorithm can accurately predict the response time and energy consumption of IoT devices, which may not always be the case. The approach does not consider the security and privacy implications of the machine learning-based performance optimization approach.
[23]	A performance evaluation of LoRaWAN technology in IoT-based industrial automation.	The paper provides a comprehensive evaluation of LoRaWAN technology for IoT-based industrial automation, including the analysis of multiple performance metrics. The evaluation is based on real-world experiments, which enhances the validity and reliability of the results. The paper highlights the advantages of LoRaWAN technology, such as low energy consumption, high scalability, and reliable connectivity.	The evaluation is based on a specific industrial automation scenario, and the results may not be generalizable to other IoT applications. The paper does not compare the performance of LoRaWAN technology with other IoT connectivity options, such as Wi-Fi or cellular networks. The paper does not discuss the security and privacy implications of using LoRaWAN technology in IoT-based industrial automation.

Table 6. Summary of Data Acquisition for IoT.

Ref.	Methods	Strengths	Limitations
[24]	Blockchain-based deep learning approach to process IoT data acquisition	Faster Transaction of Data: The proposed method uses a blockchain network to securely transmit data from the seed node to the destination node, which ensures faster data transaction. Enhanced Security: The use of a blockchain network enhances the security of the data being transmitted. Improved Accuracy: The use of a sparse autoencoder for disease prediction enhances the accuracy of the prediction. Efficient Feature Extraction: The sparse autoencoder is capable of extracting hidden features from the input data, even with a limited number of neurons in the hidden layer. Improved Performance: The proposed DNN-BC model showed improved performance compared to existing smart contract with DNN, distributed blockchain with DNN, and multifactor authentication with DNN classification in terms of packet delivery rate, throughput, delay, and energy efficiency.	Complexity: The proposed method involves a complex process of data collection, processing, and classification, which requires specialized knowledge to understand and implement. High-End Computing Requirements: The proposed method requires high-end computing resources, such as a high-end computing engine with a graphics acceleration unit, to run the simulations effectively. Limitations on the Number of Feature Maps: The sparse restrictions on the network may limit the number of feature maps that can be input into the output feature map, affecting the accuracy of the prediction.

4.6. Data acquisition

S. Hannah et al. [24] proposes a blockchain-based deep learning approach to process IoT data acquisition in cognitive data for remote health monitoring. The study focuses on classifying brain diseases such as Alzheimer's disease, mild cognitive impairment, and normal cognitive level as benign or malignant. The deep learning model is trained and tested on datasets such as OASIS-3 and UDS. The results show that the proposed method is accurate (98%) and fast in retrieving classified results, with an increased training accuracy of 0.539 and testing accuracy of 0.559. The authors aim to develop a real-time health monitoring system that can help in early diagnosis and treatment of cognitive impairments like Alzheimer's disease. The study focuses on improving the speed and delivery of healthcare data through blockchain technology and deep learning algorithms.

5. Discussion

In the current work, we comprehensively and thoroughly investigate several cutting-edge research published between 2021 and 2023, providing new and relevant issues and challenges for IoT. We give the main characteristics such as the category of the proposed methodology, the mechanisms used to improve the security and performance of the Internet of Things. In addition, the strengths and limitations (advantages and disadvantages) of this work are identified and exposed. This helps to identify problems that remain to be solved, clearly define the mainstream of research direction, and pave the way for new avenues of research for future researchers.

By way of example and without limitation, based on our review, some researchers can focus on optimization of a few works analyzed with the view to fix the shortcomings outlined, or combination of two approaches in order to take the advantages of each technique and eliminate or mitigate their flaws. Consequently, both aforementioned methodologies will certainly enhance the performance and security in IoT. Below, we afford relevant guidelines and the main conclusions drawn from the current study:

— Researchers should conduct comprehensive evaluations of their proposed solutions in realistic settings to demonstrate their effectiveness and scalability.
— Compatibility and interoperability with existing systems and devices should be considered in the design of IoT solutions.
— Researchers should explore the potential for enhancement and improvement through the incorporation of other emerging technologies or cybersecurity approaches.
— Consideration should be given to potential limitations or concerns related to privacy, security, or interpretability, and measures should be taken to address them.

6. Conclusion

Currently, it is recognized that the innumerable IoT entities connected in the whole will generally increase day by day. As a result, the IoT paradigm pervades many sectors such as education, surveillance, healthcare, agriculture, military, and commerce [25]. However, each layer of the IoT architecture is prone to various types of attacks and intrusions that could jeopardize the systems within the IoT. This is why the majority of scientific research is focused on the security and privacy aspect. And very often, the proposed methods do not take into account the performance of IoT components, which is low due to their characteristics.

In this article, we first give an overview of the architecture and application areas of the Internet of Things. Then we presented the major issues and challenges of the IoT. Due to resource constraints and complexity, traditional security and privacy approaches are unsuitable, being offered and tested on high-performance devices, and not secure enough for the Internet of Things (IoT). Thus, in the last part, recent works on the IoT have been deeply analyzed in order to bring out their strengths and limitations.

[1] Aqeel ur Rehman, Sadiq ur Rehman, Khan I. U., Moiz M., Hasan S. Security and privacy issues in IoT. International Journal of Communication Networks and Information Security. **8** (3), 147–157 (2016).

[2] Albishi S., Soh B., Ullah A., Algarni F. Challenges and solutions for applications and technologies in the internet of things. Procedia Computer Science. **124**, 608–614 (2017).

[3] Transforma Insights. Number of internet of things (iot) connected devices worldwide from 2019 to 2030, by vertical. Statista (2022).

[4] Merzouk S., Gandoul R., Marzak A., Sael N. Toward new data for IT and IoT projectmanagement method prediction. Mathematical Modeling and Computing. **10** (2), 557–565 (2023).

[5] Yadav G., Singh D. Internet of Things: A Comprehensive Survey. Wireless Personal Communications. **120** (4), 4341–4383 (2021).

[6] Al-Fuqaha M. A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. A Comprehensive Survey on Internet of Things (IoT): Concepts, Security, and Applications. IEEE Communications Surveys & Tutorials. **23** (3), 1846–1870 (2021).

[7] Purohit S. S., Palkar P. M. A Comprehensive Survey on Security and Privacy of IoT Networks. Journal of Network and Computer Applications. **189**, 103054 (2022).

[8] Chiba Z., Abghour N., Moussaid K., Lifandali O., Kinta R. A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks. Procedia Computer Science. **210**, 94–103 (2022).

[9] Chiba Z., Abghour N., Moussaid K., Lifandali O., Kinta R. Review of Recent Intrusion Detection Systems and Intrusion Prevention Systems in IoT Networks. 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). 1–6 (2022).

[10] Gazis V., Goertz M., Huber M., Leonardi A., Mathioudakis K., Wiesmaier A., Zeiger F. Vangelis Gazis Manuel Goertz Marco Huber Alessandro Leonardi. IoT: Challenges, projects, architectures. 2015 18th International Conference on Intelligence in Next Generation Networks. 145–147 (2015).

[11] Bataineh M. R., Mardini W., Khamayseh Y. M., Yassein M. M. B. Novel and Secure Blockchain Framework for Health Applications in IoT. IEEE Access. **10**, 14914–14926 (2022).

[12] Zhang H., Feng H., Hewage K., Arashpour M. Artificial Neural Network for Predicting Building Energy Performance: A Surrogate Energy Retrofits Decision Support Framework. Buildings. **12** (6), 829 (2022).

[13] Arumugam S., Subramanian A., Karuppiah M., Al-Jumaily A. M., Ramakrishnan S. A Secure and Privacy-Preserving Internet of Things Framework for Healthcare Applications. IEEE Access. **9**, 121527–121537 (2021).

[14] Chithaluru P., Stephan T., Kumar M., Nayyar A. An enhanced energy-efficient fuzzy-based cognitive radio scheme for IoT. Neural Computing and Applications. **34** (21), 19193–19215 (2022).

[15] Ahmed A., Abdullah S., Bukhsh M., Ahmad I., Mushtaq Z. An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain. IEEE Access. **10**, 11404–11419 (2022).

[16] Zhang X., Manogaran G., Muthu B. IoT enabled integrated system for green energy into smart cities. Sustainable Energy Technologies and Assessments. **46**, 101208 (2021).

[17] Tipantuña C., Hesselbach X. IoT-Enabled Proposal for Adaptive Self-Powered Renewable Energy Management in Home Systems. IEEE Access. **9**, 64808–64827 (2021).

[18] Shekari T., Cardenas A. A., Beyah R. MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. 31st USENIX Security Symposium (USENIX Security 22). 3539–3556 (2022).

[19] Alsmirat M. A., Alenezi M. Efficient Security Mechanism for Internet of Things Networks using Blockchain Technology. International Journal of Advanced Computer Science and Applications. **12** (5), 182–189 (2021).

[20] De Souza C. A., Westphall C. B., Machado R. B. Two-step ensemble approach for intrusion detection and identification in iot and fog computing environments. Computers & Electrical Engineering. **98**, 107694 (2022).

[21] Basati A., Faghih M. M. PPDAE: Efficient network intrusion detection in IoT using parallel deep autoencoders. Information Sciences. **598**, 57–74 (2022).

[22] Alkhateeb A. M., Alsahafi A. H., Alshamrani A. M., Almohammadi H. A. Real-time performance optimization of IoT-based systems using machine learning techniques. Sustainable Computing: Informatics and Systems. **32**, 100588 (2023).

[23] Khalid M. H., Ahmad I., Javaid N., Imran M. A., Alrajeh N. Performance Evaluation of LoRaWAN in IoT-based Industrial Automation. IEEE Access. **10**, 16138–16149 (2022).

[24] Hannah S., Deepa A. J., Chooralil V. S., Brilly Sangeetha S., Yuvaraj N., Raja R. A., Suresh C., Vignesh R., Yasir Abdullah R., Srihari K., Alene A. Blockchain-Based Deep Learning to Process IoT Data Acquisition in Cognitive Data. BioMed Research International. **2022**, 5038851 (2022).

[25] Tace Y., Elfilali S., Tabaa M., Leghris C. Implementation of smart irrigation using IoT and Artificial Intelligence. Mathematical Modeling and Computing. **10** (2), 575–582 (2023).

Недавнє дослідження викликів і проблем для Інтернету речей (IoT)

Гуеро А.-М. М., Чіба З., Абгхур Н.

Кафедра математики та інформатики, факультет наук Айн Чок,
Університет Хасана II Касабланки,
LIS Labs, Касабланка, Марокко

Інтернет речей (IoT) є однією з найбільш нових і революційних технологій цього століття. IoT — це мережа спеціалізованих пристроїв, які називаються "речі", що розгортаються та використовуються для збору, обробки та обміну реальними даними через Інтернет або інші мережі. У поєднанні з системами автоматизації пристрої IoT можуть допомогти керувати, контролювати та сповіщати користувачів про зміни в їхньому середовищі, допомагати їм приймати розумніші рішення, полегшувати повсякденне життя та сприяти розвитку економіки та промисловості. Тим не менш, експоненційне зростання обладнання IoT, а також відсутність загальних міжнародних стандартів призводять до величезних проблем, серед яких безпека та продуктивність. Дійсно, зі збільшенням кількості пристроїв старі методи керування підключеними пристроями стають невідповідними, це створює порушення безпеки. Крім того, обмежені ресурси пристроїв Інтернету речей, крім природи їхньої мережі, перешкоджають застосуванню потужних і складних заходів безпеки до них. Як наслідок, пристрої IoT є вразливими та схильними до багатьох загроз безпеці та вторгнень. У цій статті представлено огляд проблем і викликів IoT. Крім того, подано глибокий аналіз рішень, що запропоновані у літературі для вирішення цих проблем. Це допомагає означити проблеми, які все ще потребують вирішення, добре окреслює основний напрямок досліджень і розчищає шлях для нових напрямків досліджень для майбутніх дослідників. Нарешті, надаємо посібник або підтримку для науковців, які цікавляться Інтернетом речей.

Ключові слова: *Інтернет речей; виклики; питання; продуктивність IoT; безпека IoT.*