Journal of Informatics
Electrical and Electronics Engineering, 2021,
Vol. 02, Iss. 03, S. No. 002, pp. 1-8
ISSN (Online): 2582-7006

Issues and Challenges of Internet of Things: A Survey

Humra Khan[1], Pawan Singh[2]

[1,2]Amity School of Engineering and Technology, Amity University (AUUP), Lucknow, (Uttar Pradesh), India.
[1]khanhumra024@gmail.com, [2]pawansingh51279@gmail.com

How to cite this paper: H. Khan and P. Singh, "Issues and Challenges of Internet of Things: A Survey," *Journal of Informatics Electrical and Electronics Engineering*, Vol. 02, Iss. 03, S No. 002, pp. 1–8, 2022.

https://doi.org/10.54060/JIEEE/002.03.002

Received: 02/10/2021
Accepted: 02/11/2021
Published: 27/11/2021

Abstract

The Internet of things (IoT) paradigm has impacted the current high-tech lifestyle greatly. To name a few: smart cities, smart transportation, smart industries, pollution and energy control all owe their existence to IoT. Expansive research and investigations have been conducted for the implementation of IoT and this implementation without a doubt comes along with a lot of challenges. Such challenges and issues must be overcome in order to attain the full potential of IoT. This research paper aims to discuss the various issues and challenges faced in the field of IoT especially the ones pertaining to security and privacy. Aside from the challenges, the paper dives into the probable solutions for dealing with all the key issues of IoT along with the architecture and important application domains of IoT.

Keywords

Internet of Things (IoT), Challenges in IoT, Security issues, Security attacks, Privacy Issues

1. Introduction

The Internet of Things (IoT) can be described as a network of "things" which are physical objects (devices) embedded with electronics, software, sensors\receptors and network connectivity that permits these things to collect, store and interchange data. The Internet of Things (IoT) is a rising paradigm that allows communication among digital devices and receptors via the internet in order to facilitate our lives [1].

The Internet of Things uses smart devices along with the Internet to provide innovative solutions to various challenges and troubles pertaining to numerous commercial, government and public/private industries around the world. In other words, the Internet of Things is an innovation that brings together many smart devices, intelligent systems, frameworks and sensors. It unprecedentedly implements quantum and nanotechnology with storage, detection and processing speed. Extensive experimentation has been conducted which is available as academic articles across all mediums to exhibit the prospective efficacy and applicability of IoT transformations.

2. Architecture

IoT machine structure can be explained as a four-degree procedure wherein facts flow from sensors connected to “things” through a network and ultimately to a company data centre or the cloud for processing, evaluation and storage. Its implementation is done in four major layers:

1) Perception/Sensing Layer – It accepts and processes data through physical objects (detectors and actuators) and then emits it all through the network.
2) Network Layer – It transmits the information from the perception layer to the data processing system through internet/network gateways.
3) Data processing Layer – It analyses and pre-processes data prior to passing it to the data centre. In data centres, the data is accessed, monitored and managed by software applications often termed as business applications
4) Application Layer –The data is managed and is used by end-user applications like agriculture, defence, health care, farming, etc.

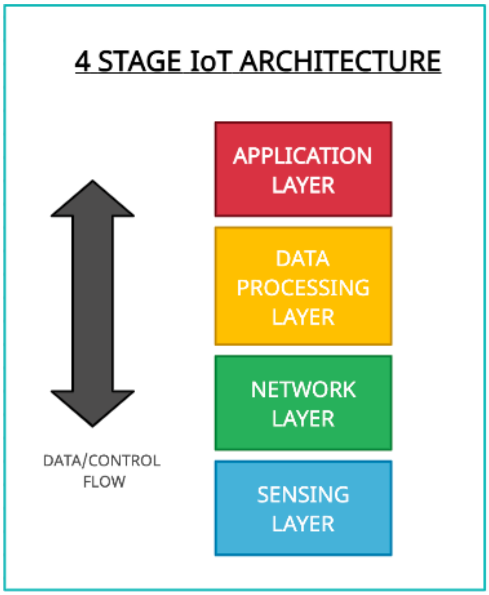

Figure 1. 4 Stage of IoT Architecture

3. Methodology

There can be several courses of action to implement an IoT system such as the agile model, Kanban model, scrum model, waterfall model, ignite model. The most used model is the scrum. The base idea common among all of them involves the following steps-

1) Recognition and foundation of requirements of system and software
2) Analysis of business schemes, rules and regulations.
3) Development of code.
4) Testing with various subjects and debugging.
5) Installation of the finished system.

Figure 2 [2] illustrates the aforementioned in detail.

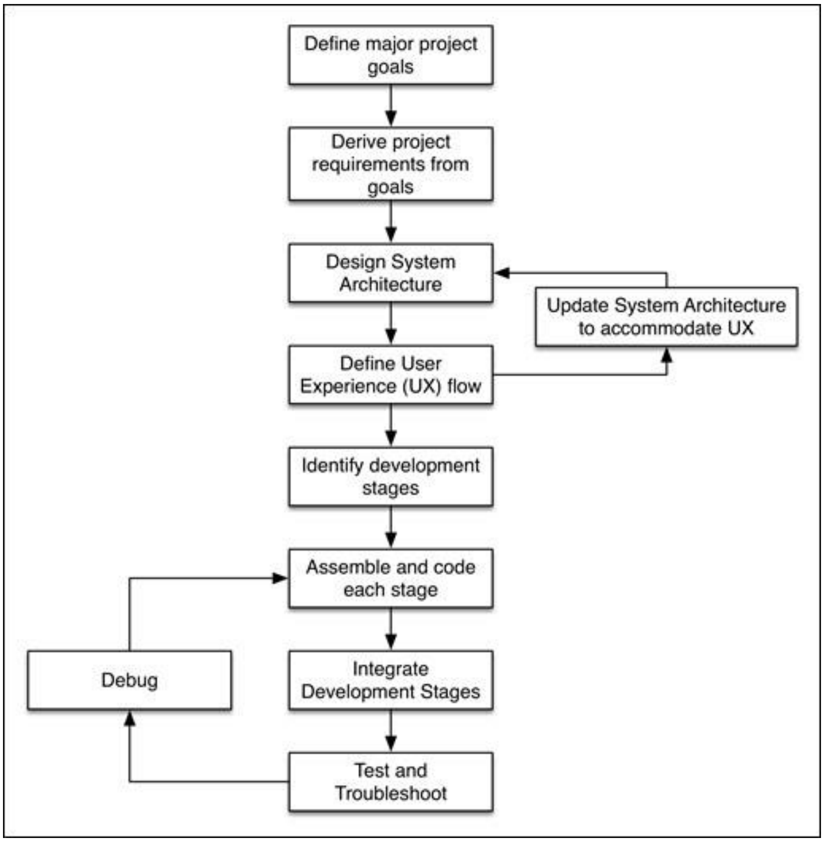
Define major project goals
Derive project requirements from goals
Design System Architecture
Update System Architecture to accommodate UX
Define User Experience (UX) flow
Identify development stages
Assemble and code each stage
Debug
Integrate Development Stages
Test and Troubleshoot

Figure 2. IoT Methodology

4. Application and Implementation of IoT

With technology on the rise, efforts to implement and integrate IoT into our day to day lives has been growing greatly. To tackle the urbanization issues in the cities, the notion of a smart city stands among the major applications of IoT. It provides a smart solution for energy consumption, infrastructure demand, healthcare and mobility. By the year 2022, the smart h smart home business is estimated to be over 100 billion dollars [3]. Thus research is being immensely carried out in the concept of Smart Home System (SHS) and Energy Management System (EMS). In this system, each home device is interfaced with an object associated with the IoT system, which is a data acquisition module with a distinct IP address resulting in a large mesh wireless network of devices [4]. As the name suggests, SHS/EMS will not only provide ease of use for every appliance to the owner of the house but also mitigate energy consumption.

Aside from smart homes, smart vehicles also come under the concept of the smart city. Current cars are facilitated with smart electronics and sensors that operate its major parts [5]. The IoT aims towards advancing the innovative systems of smart car which utilizes wireless communication between cars and drivers to ensure predictive maintenance and a safe driving experience. Other useful applications of IoT for the development of smart cities are visually summed up in Fig-3.

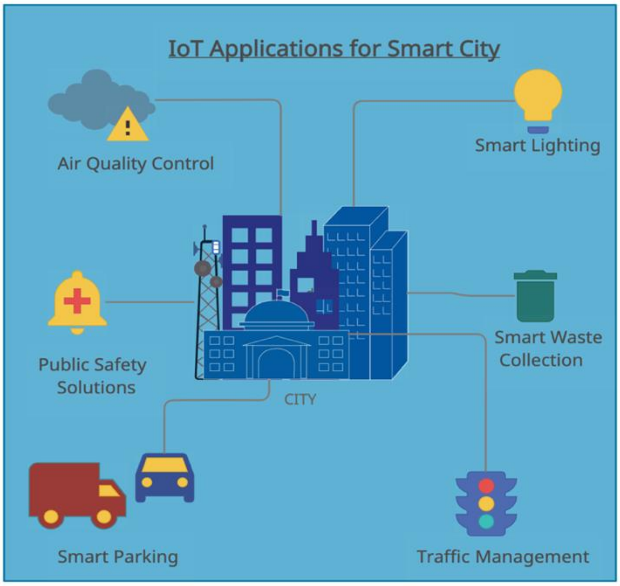

Figure 3. 4 IoT Applications for Smart City

Other implementations of IoT can be divided into consumer, commercial, industrial, infrastructure spaces and Military. Consumer applications include Eldercare, smart home. Commercial applications comprise medical and healthcare, transportation and building automation. Industrial applications cover the area of agriculture, manufacture and food. Infrastructure applications can be installed in Metropolitan scale deployments, energy management monitoring systems. Lastly, Military applications include high-end technologies such as the Internet of Battlefield Things (IoBT) and Ocean of Things.

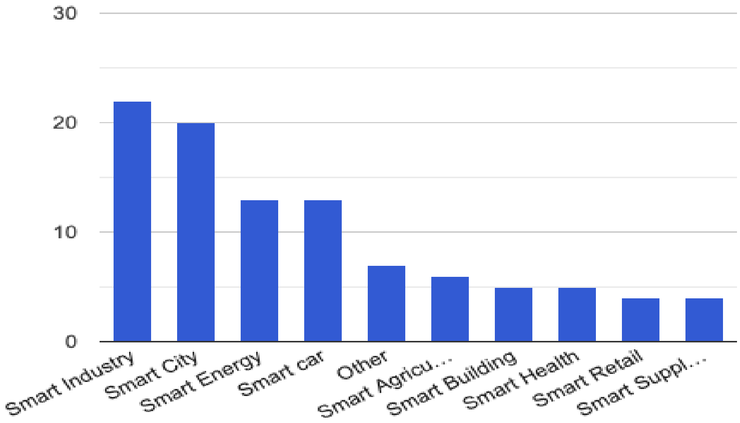

Figure 4. Global Division of IoT Applications

5. Challenges faced in IoT

While being a revolutionary technology, IoT has to deal with its own reasonable amount of challenges. The transfer of data among linked devices is a complex process and pose various issues for IoT developers.

5.1. Interoperability and Connectivity Issues-

Interoperability can be summed up as the propensity of an IoT system to communicate and interchange information among its components. It is a crucial feature is to access all of the IoT paradigm´s potential. The problems regarding inter operability surface due to the diverse character and environment of different technologies implemented for the development of IoT. Interoperability can be divided into four echelons namely, technique, connotation, configuration and syntax [6,7]. Hence, to tackle the aforementioned issue, researchers have passed certain countermeasures that are also known as interoperability handling approaches. These include adapters/gateways based, a service-oriented architecture based etc.

The connection of varied devices is also a major challenge since it resists the very structure of current communication models as currently, we rely on the centralised, server/client paradigm for connecting different nodes in a network. Such an issue will have to be resolved by decentralising IoT networks partly through using fog computing models.

5.2. Scalability and Availability Issues-

Scalability is a system's ability to upscale or downscale without compromising in its execution. The leading challenge is to support an oversizing variety of electronics with varying cache, processor, bandwidth and storage capacity [8]. An approach to solve this matter is through the integration of cloud-based IoT systems which provide ample support for scaling.

Another major challenge is the availability of services and resources to the original parts disregarding their location, time and size. Hence, for an undisturbed availability of resources, a definitive data transfer medium is needed.

5.3. Ethical, Law and Regulatory Issues-

As the IoT evolves, several real-world problems are being solved, but it has also created serious ethical and judicial complications namely: data security, trust and safety, privacy protection, etc. Therefore, there are certain instructions to sustain the standard, ethical values and to ward off any individual from committing such violations. Furthermore, it has been noticed that the majority of IoT consumers support government-imposed regulations regarding data privacy, protection and security due to scepticism in IoT technology.

5.4. Security And Privacy Issues-

Affairs pertaining to security as well as privacy are the major criterion to earn trust in IoT Systems. Security threats and challenges in IoT are the biggest concern the corporate coders have to deal with due to innumerable threats, cyber-attacks, risks and vulnerabilities of the system [9]. These arise due to inadequate authorization and authentication, poor transport layer encryption, insecure software, firmware and network interface [10]. Moreover, Security in IoT can be branched into the following divisions -

a) System Security: System security majorly centres around the whole of IoT system to recognise numerous security challenges, to layout distinct security frameworks and to offer adequate guidelines pertaining to security.

b) Application security: Application Security works to manipulate security troubles as per the specified requirements.

c) Network security: Network security dives into protecting the network for the communication of various IoT devices [11].

IoT systems are also prone to various kinds of attacks which aim at compromising the security of IoT devices or networks.

These attacks have active or passive nature and can be physical, encryption-based, DoS, firmware hijacking, ransomware, botnets, man in the middle, etc. The attacks can be further divided into the subsequent modules [12]-

1) Attacks based on Protocol: They are the types of attacks that are utilizing the internalised structure based on protocols of the IoT constituents that affect the correspondence channel and the dispatch mechanism of the embedded framework. These are divided into subsections:

a) Attacks based on communication protocols: This explains the forms of exploitation that occur during transitions through nodes. These include flood attacks, key, pre shred attacks and sniffing attacks.

b) Attacks based on the network protocol: This explains the manipulation that occurs when the connection is initiated. Attacks include sniffing attacks, selective forward attacks, and wormhole attacks.

2) Attacks based on data: These include threats related to the authentic data memos and packets transmitted at the node locations. Hash collision, DoS (Denial of Service) malicious node VM creation and exposure of data are some of the vulnerable security exploits.

Different levels of attacks can also be designated as four kinds based on their behaviour and proposed solutions to threats.

1) Low-level attack: When an attacker tries to attack a certain network but the attack is unsuccessful.
2) Medium-level attack: When an intruder or a sniffer eavesdrops on the medium without amending the integrity of the data.
3) High-level attack: When an attack is carried out on a network that changes the integrity of the data or does some modifications in the data.
4) Extreme High-Level Attack: When an intruder attacks a network by attaining illegal access and performing an illicit operation, blocking the network, sending a mass of junk messages, or making the network unavailable [13].

To assure the security of the IoT networks, each layer of the IoT architecture must be required to have security mechanisms in order to forestall security dangers and assaults [14]. Various protocols are coherently developed and implemented on each communication channel layer in order to warrant security and data protection in IoT-based systems. Few of the cryptographic protocols integrated in the middle of the application layer and transport layer to offer security measures in numerous systems involve the Secure Socket Layer and Datagram Transport Layer Security [15-21].

Privacy, on the flip side, is also a major concern that enables users to have the guarantee of safety while using IoT based applications. It is, therefore, necessary to support authentication and warranty in a network securely in order to initiate communication among trust contingents. Another obstacle is the wavering privacy guideline for each of the objects which communicate within the IoT system. Thus, the privacy guidelines for each object deployed in the system should be checked before the data is transferred.

Table 1. Security threats at each iot layer

Perception layer (RFID, WSN, RSN)	**Network layer** (LAN, Core Network, Access Network)	**Application layer** (IoT Applications Cloud Platform)
Unauthorised access	Public key and Private key	Remote configuration
Availability	Routing attack	Mis-configuration
Selfish attack	DOS	Security management
Malicious code	Malicious Code	Management system
Spoofing attack	Transmission threat	
DOS		
Transmission threat		
Routing attack and Data Breach		

6. Discussion and Conclusion

This paper has elucidated how security concerns relating to the IoT space have evolved. Thus, we conclude how IoT security still requires considerable work before it is ready for widespread public acceptance. The most common persistent concerns deal with privacy, identification, authentication, authorization and the lack of management methods (i.e., compliance). Data protection in the IoT is of the utmost priority as the devices used, often collect private personal data. Numerous steps are being undertaken to secure sensitive user data through authentication methods such as:

i. Knowledge-based authentication that is using information specific to every user.

ii. Authentication based on the user's own knowledge with smart cards or access cards and

iii. Physical characteristics such as fingerprint, eye scans, etc.

However, these measures have still been unsuccessful in revamping themselves to the heterogeneous and resource-limited environment of the IoT. Moreover, noteworthy work has been accomplished to conform to the presently practised protocols for IoT purposes or to develop wholly fresh ones for easy encryption and secure network transmission. The weakest aspect of IoT security right now is authentication and authorization. The increasing impact of IoT in day to day lives makes authentication and security essential.

The public nature of many IoT systems, being very open makes them particularly vulnerable to malicious attacks. This can be witnessed by the often inadequate security of the devices themselves. Radio wave communication is susceptible to many types of attacks, ranging from eavesdropping to DoS attacks. The dearth of compliance methods exacerbates the transport layer and creates additional pressure on the systems. If security continues to be a serious concern in the IoT, it could ultimately prevent end-user adoption of the technology and thus mitigate this field's development. Therefore, along with research, review efforts are also needed to help device manufacturers, regulators, and implementers prioritize their efforts in developing IoT security strategies.

References

[1] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” *J. Big Data*, vol. 6, no. 1, 2019.

[2] *Packtpub.com*.[Online].Available: https://subscription.packtpub.com/book/application-development/9781783285938/10/ch10lvl1sec65/the-design-methodology-for-iot-projects. [Accessed: 01-Nov-2020].

[3] M.-D. González-Zamar, E. Abad-Segura, E. Vázquez-Cano, and E. López-Meneses, “IoT technology applications-based smart cities: Research analysis,” *Electronics (Basel)*, vol. 9, no. 8, p. 1246, 2020.

[4] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, “A smart home energy management system using IoT and big data analytics approach,” *IEEE trans. consum. electron.*, vol. 63, no. 4, pp. 426–434, 2017.

[5] *Www.ti.com*. [Online]. Available: http://www.ti.com/technologies/internet-of-things/overview.html. [Accessed: 02-Nov-2021].

[6] *Etsi.org*.[Online].Available:https://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf. [Accessed: 02-Nov-2020].

[7] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in internet of things: Taxonomies and open challenges,” *Mob. Netw. Appl.*,

vol. 24, no. 3, pp. 796–809, 2019.

[8] C. Pereira and A. Aguiar, “Towards efficient mobile M2M communications: survey and open challenges,” *Sensors (Basel)*, vol. 14, no. 10, pp. 19582–19608, 2014.

[9] Z. B. Babovic, J. Protic, and V. Milutinovic, “Web performance evaluation for internet of things applications,” *IEEE Access*, vol. 4, pp. 6974–6992, 2016.

[10] “HP study finds alarming vulnerabilities with Internet of things (IoT) home security systems,” *Www8.hp.com*. [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1909050. [Accessed: 02-Nov-2020].

[11] M. Abdur, S. Habib, M. Ali, and S. Ullah, “Security issues in the internet of things (IoT): A comprehensive study,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017.

[12] Rachit, S. Bhatt, and P. R. Ragiri, “Security trends in Internet of Things: a survey,” *SN Appl. Sci.*, vol. 3, no. 1, 2021.

[13] R. Roman, P. Najera, and J. Lopez, “Securing the internet of things,” *Computer (Long Beach Calif.)*, vol. 44, no. 9, pp. 51–58, 2011.

[14] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014.

[15] *Ietf.org*. [Online]. Available: https://www.ietf.org/rfc/rfc2246.txt. [Accessed: 02-Nov-2020].

[16] S.-H. Ju, H.-S. Seo, S.-H. Han, J.-C. Ryou, and J. Kwak, “A study on user authentication methodology using numeric password and fingerprint biometric information,” *Biomed Res. Int.*, vol. 2013, p. 427542, 2013.

[17] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved,” IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, 2019.

[18] M. Misra and P. Singh, “Energy Optimization for Smart Hous-ing Systems,” Journal of Informatics Electrical and Elecrtonics Engineering, vol. 01, no. 5, pp. 1–6, 2020.

[19] R. Yadav, Department of ECE, ASET, Amity University Lucknow Campus, India, and K. K. Singh, “Study on design and simulation of temperature control system,” Journal of Informatics Electrical and Electronics Engineering (JIEEE), vol. 2, no. 1, pp. 1–4, 2021.

[20] S. Yadav, Department of ECE, ASET, Amity University Lucknow Campus, India, and K. K. Singh, “Smart environmental health Monitoring System,” Journal of Informatics Electrical and Electronics Engineering (JIEEE), vol. 2, no. 1, pp. 1–5, 2021.

[21] A. Rani, V. Prakash, and M. Darbari, “A Proposal for Architectural Framework Using Internet of Things with Fog Computing for an Air Quality Monitoring Sys-tem,” Journal of Informatics Electrical and Elec-tronics Engineering, vol. 02, no. 023, pp. 1–14, 2021.