STM JOURNALS

International Journal of
Information Security Engineering

Volume 2, Issue 1, 2024
January–June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Conquering the IoT Frontier: Challenges Faced in India

Mayur Kesari[1,*], Neelu Kewat[1]

Abstract

The internet of things (IoT) represents a transformative force reshaping the landscape of connectivity and communication, ushering in an era marked by seamless machine-to-machine interactions and the fluid exchange of data across diverse devices and systems. This paper undertakes an extensive exploration of the prevailing state of IoT advancement within India, with a particular emphasis on delving into the multifaceted realms of security concerns, inherent challenges, and burgeoning opportunities. By scrutinizing the nuanced intricacies of IoT deployment in the Indian context, this study endeavors to furnish a comprehensive overview, elucidating the distinct risk factors and security intricacies endemic to the Indian milieu. Through a meticulous examination of these complexities, this paper aims to furnish stakeholders with a profound understanding of the obstacles impeding the widespread adoption of IoT technologies in India, thereby paving the way for informed decision making and strategic interventions. By elucidating the current landscape of IoT development, this paper not only identifies the challenges hindering progress but also endeavors to highlight the potential avenues for innovation and growth, thereby fostering a conducive environment for the proliferation of IoT technologies in the Indian subcontinent.

Keywords: Internet of things (IoT), widespread adoption, proliferation, IoT landscape, security

INTRODUCTION

In the coming years, the internet of things (IoT) is poised to usher in profound transformations in various aspects of our lives, including business models, trade standards, security, and infrastructure across the entire landscape of IT computing and networking systems. The IoT signifies an emerging technological frontier that is still in the initial phases of market evolution. This nascent technology promises to accelerate the concept of the "sharing economy," introducing innovative ways to monitor and manage everyday objects while enabling the sharing of small, cost-effective assets beyond the conventional realms of communities, airplanes, automobiles, and motorcycles.

As the IoT trend continues to evolve, it presents a multitude of unexplored applications that will pave the way for novel business models and revenue opportunities [1]. It enables devices and sensors to operate at unprecedented levels of efficiency, fostering the emergence of fresh uses, applications, services, and business models that were previously deemed economically unviable. Nevertheless, this technological upheaval comes with its set of difficulties and possible hazards, especially for well-established industries.

Today, IoT technology holds a prominent position among the top five technologies globally, as recognized by Gartner. Its extensive utilization extends to various sectors, ranging from smart homes and vehicle tracking to monitoring children and the elderly, as well as facilitating everyday routines [2]. Yet, the current landscape is marked by

***Author for Correspondence**
Mayur Kesari
E-mail: s1062220045@timscdrmumbai.in

Research Scholar, MCA, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR), Mumbai, Maharashtra, India

Received Date: February 29, 2024
Accepted Date: May 06, 2024
Published Date: May 22, 2024

Citation: Mayur Kesari, Neelu Kewat. Conquering the IoT Frontier: Challenges Faced in India. International Journal of Information Security Engineering. 2024; 2(1): 16–21p.

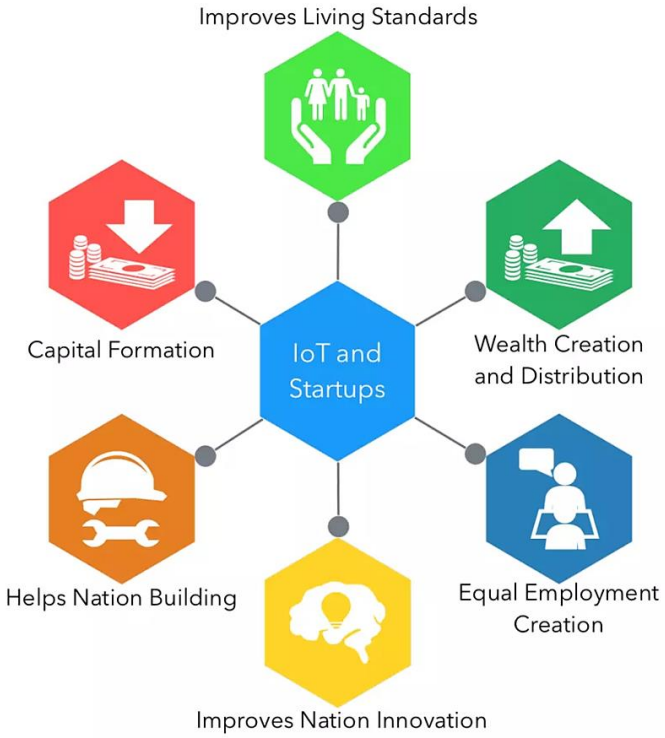

Figure 1. Scope of internet of things (IoT).

the proliferation of diverse IoT devices, and it is clear that the future holds the potential for an even more profound revolution as shown in Figure 1.

The following section of this paper will delve into the current state of IoT in India, focusing on the unique challenges, security considerations, and opportunities that this dynamic technology landscape presents.

ROLE OF INTERNET OF THINGS IN INDIA

Government initiatives, environmental support, and smart applications: In the journey toward the development of smart cities in India, government initiatives, environmental considerations, adherence to robust occupancy standards, and the burgeoning adoption of smart applications stand as pivotal drivers. According to data from the Indian government's Smart Cities Mission, substantial investments exceeding INR 2 lakh crores have already been channeled into smart city projects as shown in Figure 2. This commitment is set to further escalate, with an anticipated investment of INR 4.8 lakh crores by 2024.

The widespread adoption of IoT applications across diverse domains is evident, with businesses making substantial investments [3]. Significantly, attention has turned to crucial sectors such as Smart Water Management, Smart Waste Management, Healthcare, Smart Agriculture, Smart Environment, Smart Safety, and Smart Supply Chain, among others. However, the affordability of IoT solutions for a population exceeding a billion poses a considerable challenge, given India's penchant for thrift [4]. Moreover, the intricacies of the Indian infrastructure landscape, including intermittent power supply, environmental pollution, extreme temperatures, high humidity levels, dust, and gaps in telecom coverage, present formidable obstacles in the path of IoT implementation as shown in Figure 3.

The Indian government's Digital India Program stands as a top-priority initiative with the overarching goal of digitizing the nation and transforming it into a digitally empowered knowledge economy. This ambitious program is anticipated to serve as a compelling catalyst for the expansion of the IoT productivity ecosystem within India as shown in Table 1.

Figure 2. Future of internet of things (IoT) in India.

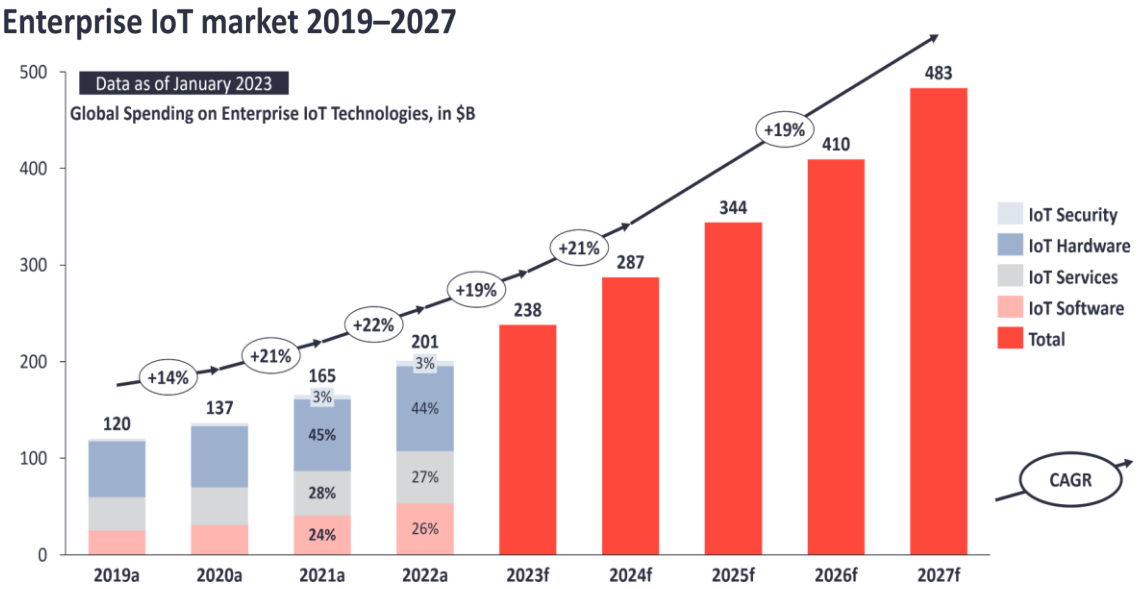

Figure 3. Market of internet of things (IoT) in India.

Table 1. The internet of things (IoT) productivity ecosystem.

S.N.	IoT Global	IoT India
1.	Globally, IoT market will rise to $ 75.4 billion in 2025.	IoT market in India is expected to grow to $ 16 billion with 2.9 billion units from current $ 5.9 billion and 200 million connected units.
2.	During 2016–2022, global expenses on IoT based products and services by initiatives are projected to reach $125 billion to $259 billion attaining a 16% CAGR.	During 2015–2022, IoT market in India is expected more than 28% to grow at a CAGR and business is expected to touch $300 billion by 2022.
3.	IoT will increase $10 to $15 trillion to global GDP in the next 20 years.	The Indian government's objective is to generate an IoT production in India of $ 15 billion by 2022.
4.	In 2022 automated driving and IoT-enabled vehicle will be increased globally.	In India, utility sector and oil sector slowly reach on top 5 sector like electronics and telecom, both are revenue-generating sectors.

CAGR, compound annual growth rate; GDP, gross domestic project.

CHALLENGES OF THE INTERNET OF THINGS

Security

Security is a fundamental pillar of the internet and is increasingly becoming a paramount challenge in the context of IoT. As the popularity of IoT continues to surge, the number of interconnected devices has grown from millions to tens of billions. With this expansion, the risk of exploiting security vulnerabilities has also surged. Particularly in the case of low-cost or less sophisticated devices, incomplete data streams may provide openings for data theft, which could have severe implications for people's health and safety. Additionally, numerous IoT deployments incorporate clusters of similar or closely matching devices. This uniformity multiplies the potential impact of a single security flaw, as it affects the entire group of devices that share the same characteristics.

Privacy

In the domain of IoT, essential elements include authenticity, trust, and confidentiality. Nevertheless, these considerations represent merely the surface of the issue. Additional necessities include determining access to specific facilities, preventing unauthorized transfers of data at certain times, and safeguarding business communications involving smart objects from potential adversaries. Notably, the data networks in India are both relatively lightweight and costlier compared to more advanced nations.

Furthermore, from an Indian perspective, the implementation of cloud storage procedures is still in its nascent stages. The practice of transmitting data to a cloud service for processing, which may involve third parties, further complicates the landscape. The aggregation of this knowledge also raises significant legal and regulatory challenges, especially in the realms of data security and privacy laws.

Standards

The absence of standardized guidelines and records within the realm of IoT can inadvertently enable uncontrolled and potentially disruptive activities by IoT devices. The proliferation of low-standard or cost-effective, hastily designed devices can have detrimental effects on networking resources. In the absence of clear standards to direct developers and manufacturers, there may be instances where products are created that operate in disruptive ways on the internet. The development of standardized methodologies is essential, as it ensures that technology can be widely accessible and adopted by all stakeholders. This, in turn, promotes growth and harmonizes the IoT landscape for the benefit of all.

Trained Workforce

The successful execution of any technology necessitates a team of experienced professionals possessing comprehensive knowledge of network infrastructure, hardware, software, and the specific technology in question. In the context of India, there exists a challenge where the workforce often perceives the proliferation of technology as a threat to job security, discouraging them from embracing new technologies. This reluctance to adapt or upskill creates significant hurdles for communities transitioning from legacy systems to IoT-enabled systems, leading to operational challenges.

Moreover, scalability, fault tolerance, and consistent power supply remain significant challenges in the Indian IoT landscape. These aspects require dedicated attention and robust solutions to ensure the seamless and reliable operation of IoT systems as shown in Table 2.

This survey is based upon the security issues and challenges face in India. Researchers face different problems like authenticity, interoperability, privacy, data confidentiality, low range of internet signal, power supply, power backup, fault tolerance, reliability, cost, poor support, and most important awareness and skills [2]. Here we discuss about some challenges and risk that already exists in India which must take care and improve by government, service providers.

Table 2. Exploring the landscape of internet of things (IoT): risks, security measures, and emerging challenges.

S.N.	Survey Done	Citation	Month, Year	Security and Risk Factors	Challenges Faced
1.	The internet of things for health care: a comprehensive survey	[5]	June, 2015	• Computational limitations • Memory limitations • Energy limitations • Scalability • Mobility • Communications media • Data protection	• Standardization • IoT healthcare platforms • Cost analysis • Technology transition • The low-power protocol • Scalability
2.	A survey: internet of things (IoT) technologies, applications and challenges	[6]	March, 2016	• Front end sensors and equipment • Networks • Backend of its system	• Scalability • Device heterogeneity • Energy optimized solution • Ubiquitous data exchange through wireless technology • Self-organization capabilities • Semantic interoperability and data management
3.	Internet of things: evolution, concerns and security challenges	[7]	March, 2016	• As IoT connects more devices together, it provides more decentralized entry points for malware • Trust and privacy.	• Standards and interoperability • Complexity, confusion and integration issues. • Internet connectivity and power requirement.
4.	Smart home analysis in India: an IoT perspective.	[8]	June, 2016	• Unique identification – low security at the server side. • Privacy • Authentication	• Reliability • Co-ordination among connected objects, • Integration of several devices increases the system complexity and connectivity problem. • Cost and storage • Self-organization of network so that there is no data loss due to network failure.
5.	Challenges and risk to implement IOT in smart homes: an Indian perspective.	[9]	November, 2016	• Risk is to store the sensitive data either on local server or to use VPN (virtual private network) in case using the remote server of vendor. • When security system based on the CCS (centralized controlled system) for processing, application and data storage, then a risk of central point of failure is increase. • Hacking, DoS (denial of service), updation, virus, password based attacks and phishing	• Internet connectivity, consistency and accessibility of necessary signals bandwidth. • Cost of technology. • Poor supporting organizational setup. • IoT adoption due to nonexistence of well-trained staff. • Lack of awareness of IoT systems, services and applications.
6.	Health care systems using internet of things.	[10]	December, 2016	• Data security causes concerns in the implementation of IoT in healthcare.	• Lack of electronic health record (EHR) system integration. • IoT data alone may not be as meaningful if it is not within the context of a full health record. • Constant changes in hardware and connectivity technology.

CONCLUSION

The future of IoT holds immense promise, despite the challenges it brings, particularly in managing the vast volumes of data it generates, complexities in detection, communications, and control, and the critical need for heightened awareness. With each passing day, the growth of IoT technology only accelerates. It is anticipated that the future of IoT will move towards a seamless, all-encompassing, and ubiquitous presence. To navigate this landscape successfully, service organizations must adhere to a set of criteria, emphasizing interoperability, awareness, expertise, teamwork, energy, sustainability, privacy, trust, confidentiality, and security.

IoT has rapidly evolved into a significant force in the information industry, promising to improve the quality of life. This paper has delved into some of the most critical issues and challenges of IoT, specifically from the Indian perspective, shedding light on what's been accomplished and the areas that require further refinement. Potential enhancements include the development of a unified, seamless, and universal internet connectivity solution, standardization with a focus on interoperability, and ongoing research on energy sustainability, privacy, and security. In the forthcoming years, addressing these challenges will be a bold and pivotal step forward, enhancing the landscape of commerce, industry, and academia.

REFERENCES

1. Ishaq K, Farooq SS. Exploring IoT in smart cities: practices, challenges and way forward. arXiv preprint arXiv:2309.12344. August 25, 2023. Available at https://arxiv.org/pdf/2309.12344
2. Yadav EP, Mittal EA, Yadav H. IoT: challenges and issues in Indian perspective. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Nainital, India, February 24–25, 2018. pp. 1–5.
3. Shanmuganathan H, Mahendran A. Current trend of IoT market and its security threats. In: 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, September 24–25, 2021. pp. 1–9.
4. Kamienski C, Soininen JP, Taumberger M, Dantas R, Toscano A, Salmon Cinotti T, Filev Maia R, Torre Neto A. Smart water management platform: IoT-based precision irrigation for agriculture. Sensors. 2019; 19 (2): 276.
5. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. IEEE Access. 2015; 3: 678–708.
6. Shah SH, Yaqoob I. A survey: internet of things (IOT) technologies, applications and challenges. 2016 IEEE Smart Energy Grid Engineering (SEGE), Oshawa, Ontario, Canada, August 21–24, 2016. pp. 381–385.
7. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: evolution, concerns and security challenges. Sensors. 2021; 21 (5): 1809.
8. Vyas C, Patil S. Smart home analysis in India: an IoT perspective. Int J Computer Appl. 2016; 144 (6): 29–33.
9. Roshan R, Ray AK. Challenges and risk to implement IOT in smart homes: an Indian perspective. Int J Computer Appl. 2016; 153 (3): 16–19.
10. Gapchup A, Wani A, Gapchup D, Jadhav S. Health care systems using internet of things. Int J Innov Res Computer Commun Eng. 2016; 4 (12): 20896–20903.

