iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** X **Month of publication:** October 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.74493

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue X Oct 2025- Available at www.ijraset.com*

# Analyzing User Experience Barriers within IoT-Integrated Smart Environments

Dr. Diwakar Ramanuj Tripathi[1], Hitesh Gautam Pillewan[2], Dr. Vrushali Pramod Parkhi[3]
[1]*Head, Department of Computer Science,* [2]*Research Scholar,* [3]*Officiating Principal*
[1, 2, 3]*S.S. Maniar College of Computer & Management, Nagpur*

***Abstract:*** ***The Internet of Things (IoT) is becoming advanced gradually regarding the touchpoints and user experiences within smart environments. Even though this seems to promote ubiquitous computing and efficiency through the elimination of users, there are adverse user experience (UX) situations within the IoT domain. This paper addresses these matters by focusing on specific issues; usability concerns, privacy issues and the need for context. Continuing by analyzing and evaluating existing papers, this work aims at identifying important UX barriers in smart home environments and other IoT systems as well in order to provide solutions regarding their design and usability. To confirm these central UX themes, some mixed method consisting one data analysis from user surveys and observational method was used. The results suggest that usability issues related to the design, lack of standardization and security issues prevent adoption by users. Suggestions are made on how to improve UX designs within the IoT environment going forward. Even though IoT devices bear a promise of enriching a task and *enhancing user convenience, it often becomes quite difficult for users to carry out the task simply because of vaguely defined interactions, and IoT platforms that are not cohesive, incoherent IoT systems that are security model centric instead of user centric. The direction of the next step of research is oriented on the design concentrating on people, personalization, and interaction simplification in order to increase user pleasure and effectiveness of the system. This review is a part of the ongoing initiation concerning the understanding of UX in the IoT.***

***Keywords: Smart Environments, Human–Computer Interaction (HCI), Privacy and Security, Intelligent Spaces, User-Centered IoT Design.***

## I. INTRODUCTION

The internet of things IoT is transforming the ways of human experiences and relationships with objects as it incorporates the connection of normal things to the internet facilitating efficiency and automation of logics. IoT provides many areas with enhanced features of ease of operation, safety and improved functions such as smart homes, cities, health care, and industrial operation. The concept where all devices are wireless, intelligent and hardworking enough to recollect and predict common user needs is close to becoming real. Despite the benefits associated with IoT, its adoption often encounters User Experience (UX) issues. The more the IoT systems become popular, the more there are many devices one needs to control or operate, most of the time belonging to different manufacturers and offered with different brand names, which results to a rather jarring experience. Furthermore, serving the varied demographic and the range of technologies the users can comprehend creates a barrier to designing and building self-evident platforms and inbuilt systems. Privacy and security are also important consideration of user interaction as for a lot of people gather and watch these devices do not sit well with their concept of IoT systems.

Since these devices are capable of gathering and processing extensive private user information, it raises issues on how users feel about lack of transparency and over control of them affecting user acceptance and trust.

## II. LITERATURE REVIEW

The rise of IoT has created an unprecedented level of connectivity between the physical and digital worlds. Previous research has examined various aspects of IoT, focusing on technical elements like interoperability, security, and infrastructure. However, there is an increasing need to investigate IoT from the standpoint of human factors and UX design.

De Russis and Corno (2016) found that while voice assistants—such as Google Assistant and Amazon Alexa— have significantly improved the usability of smart home devices, they still present challenges in certain situations. Users often feel frustrated when these voice interfaces fail to understand complex or context-specific commands. Additionally, users face difficulties when switching between voice, gesture, and touch input methods, which are necessary for operating various devices.

This inconsistency can lead to confusion, especially when the system behaves unexpectedly or when transitioning between devices requires a mental adjustment to grasp different input modalities.

©IJRASET: All Rights are Reserved 

In a study by Zeng et al. (2017), the increasing variety of devices and platforms in IoT environments was highlighted as potentially overwhelming for users, particularly those with limited technical knowledge. The fragmentation of ecosystems, where different devices may operate on separate platforms, forces users to navigate multiple interfaces and interaction methods. This disjointed experience hampers the creation of a seamless, user- friendly interaction model, especially when managing several devices at once.

Verma et al. (2020) argue that these usability challenges significantly hinder the widespread adoption of smart home technologies. Despite the convenience they offer, the steep learning curve associated with managing complex IoT ecosystems discourages many users, particularly those who are not tech-savvy. Regarding multimodal interaction and cognitive load, the use of various modes—such as voice, gesture, and touch—to interact with IoT systems introduces additional challenges. De Russis and Corno (2016) noted that multimodal systems often misinterpret user intent, especially when switching between interaction methods. For instance, a voice command followed by a gesture may not be processed accurately by the system, leading to user frustration. The inconsistency in performance across different modalities complicates the user experience, as users must remember the correct input method for each device and context. This increases cognitive load, requiring more mental effort to operate smart environments.

Zeng et al. (2017) emphasize that for non-technical users, managing the specific interaction patterns or modalities associated with each device can be overwhelming. The lack of standardization across devices exacerbates this issue, as each system demands users to adapt to different interaction techniques. With the growing number of IoT devices in homes and workplaces, navigating these diverse interaction methods creates significant usability challenges, contributing to user frustration and diminished satisfaction with the technology. Privacy and data security concerns are among the most pressing issues in IoT-enabled environments, directly affecting the overall user experience. Roman et al. (2018) pointed out that users often have limited control over their data in smart environments, leading to fears of unauthorized access, data misuse, and surveillance. As IoT devices collect extensive personal data, anonymization techniques designed to protect user identities are not always effective due to the richness of the data generated. Even anonymized data can often be re-identified, particularly when combined with other datasets, increasing privacy risks.

Choi and Lee (2019) examined privacy concerns among IoT users and found that the continuous data collection inherent in IoT systems poses significant threats to user trust. They argue that the pervasive surveillance capabilities of IoT devices, such as smart cameras, motion sensors, and connected appliances, can create a sense of constant monitoring for users. This lack of transparency and control over personal data diminishes user trust in the system, ultimately harming the overall user experience. If users feel they have no control over their data or are uncertain about how their information is being utilized, they are less likely to fully embrace IoT technologies, despite their functional advantages.

Parker et al. (2021) analyzed the role of contextual awareness in enhancing user experience in IoT environments. The study revealed that while IoT systems aim to adapt to user preferences and environmental changes, many devices still struggle to do so seamlessly. For instance, smart lighting systems may fail to adjust accurately to ambient light conditions, and smart thermostats might not respond to sudden temperature changes, leading to a disconnect between user expectations and system performance.

De Russis and Corno (2016) emphasize that current IoT systems face challenges in understanding user intent within specific contexts. Devices often rely on user intervention to clarify commands or adjust settings, which contradicts the goal of creating autonomous, self-sufficient smart environments.

Parker et al. (2021) suggest that to improve user experience, IoT systems should develop more advanced contextual awareness algorithms capable of anticipating user needs and autonomously adapting to changes in the environment without requiring constant input from the user. In addressing the UX challenges identified in the literature, researchers propose several strategies to enhance interaction and user satisfaction in IoT environments.

Verma et al. (2020) recommend simplifying interaction models by creating more intuitive, standardized interfaces to reduce cognitive load on users. They also advocate for prioritizing cross-platform compatibility to alleviate the fragmentation present in IoT ecosystems. Enhancing device interoperability would allow users to control multiple devices through a single interface, thereby improving the overall user experience. Regarding privacy, Choi and Lee (2019) propose greater transparency in data collection and processing practices. By providing users with more control over their data and clearly explaining how their information is utilized, designers can rebuild trust and mitigate privacy concerns. Privacy-by-design principles should be integrated into IoT systems to ensure that user data is protected from the outset, rather than as an afterthought.

Parker et al. (2021) recommend investing in advanced AI and machine learning techniques to improve the contextual awareness of IoT devices. Developing systems that can better understand and predict user behavior would enable IoT environments to be more responsive to user needs, ultimately enhancing usability and user satisfaction.

## III. PROBLEM STATEMENT

While IoT technology offers numerous advantages, its usability remains a significant barrier to user adoption. Users frequently encounter difficulties in understanding and controlling IoT systems due to complex interfaces, lack of interoperability, and insufficient security measures. Additionally, widespread privacy concerns regarding data collection persist. If these challenges are not addressed, the user experience in IoT-enabled smart environments will continue to be subpar, limiting the true potential of IoT systems.

## IV. RESEARCH METHODOLOGY

This study utilized a mixed-method approach to investigate the UX challenges in IoT-enabled environments, combining qualitative and quantitative data collection techniques.

## V. DATA COLLECTION

### *A. Surveys*

A survey was conducted with 83 users of smart home devices to gather quantitative data on their experiences, preferences, and challenges. Analysis Table Based on Each Section of the User Experience Questionnaire Regarding Challenges in Understanding and Controlling IoT Systems:

Table 1: Analysis table based on each section of the user experience questionnaire

| Type | Question | Possible Answers | Analysis Focus |
|---|---|---|---|
| Section A: General Information | | | |
| Multiple-choice (single select) | 1. Age | 18–25, 26–35, 36–45, 46–55, 56+ | Distribution of Age among IoT users |
| Multiple-choice (single select) | 2. Gender | Male, Female, Other | User Gender specification |
| Multiple-choice (single select) | 3. How long have you been using IoT devices? | Less than 6 months, 6–12 months, 1–2 years, More than 2 years | User Experience with IoT Devices |
| Multiple-choice (multi-select) | 4. Which of the following IoT devices do you use? | Smart home devices, Wearables, Smart appliances, Connected vehicles, IoT healthcare devices, Other | Category of Device usage frequency |
| Section B: User Experience with IoT Devices | | | |
| Multiple-choice (single select) | 5. Rate ease of setup | Very easy, Easy, Neutral, Difficult, Very difficult | Setup difficulty and user experience |
| Multiple-choice (single select) | 6. Have you had difficulties controlling IoT devices? | Yes, No; If Yes: Complex interface, Unclear instructions, Confusing app navigation, Lack of technical knowledge | Common control challenges, issue frequency, and types of difficulties |
| Likert scale (1–5) | 7. Interface intuitiveness (scale 1–5) | 1 (Not intuitive) – 5 (Very intuitive) | Level of intuitive experience with device interfaces |
| Multiple-choice (single select) | 8. Frequency of switching apps/ platforms | Never, Rarely, Sometimes, Often, Always | Frequency of platform switching and its impact on ease of use |
| Multiple-choice (single select) | 9. Interoperability issues between IoT devices | Yes, No; If Yes: Devices not syncing, Control difficulties, Multiple apps, Compatibility issues | Problems related to multi-device interoperability |

| | | | |
|---|---|---|---|
| Section C: Security and Privacy Concerns | | | |
| Likert scale | 10. Concern about IoT security | Not concerned, Slightly concerned, Moderately concerned, Very concerned, Extremely concerned | Security awareness and concern levels |
| Multiple-choice (single select) | 11. Experience with security breaches | Yes, No | Occurrence of security breaches among users |
| Multiple-choice (multi-select) | 12. Main security concerns | Hacking, Insecure data transmission, Weak passwords, Device malfunction, Other | Security concerns most significant to users |
| Multiple-choice (single select) | 13. Awareness of data collection by IoT devices | Very aware, Somewhat aware, Neutral, Not very aware, Not aware at all | Level of data awareness among users |
| Likert scale | 14. Concern about privacy | Not concerned, Slightly concerned, Moderately concerned, Very concerned, Extremely concerned | User concern levels about data privacy |
| Multiple-choice (multi-select) | 15. Specific privacy concerns | Data sharing without consent, Continuous data collection, Location tracking, Lack of control over personal data | Main privacy concerns regarding IoT |
| Section D: User Feedback and Recommen-dations | | | |
| Multiple-choice (multi-select) | 16. UI improvements desired | Simpler setup, More intuitive controls, Better device integration, Easier app navigation, Other | Main areas for UI/ UX improvement in IoT devices |
| Multiple-choice (multi-select) | 17. Security improvements desired | Improved encryption, Better privacy controls, Regular updates, Multi-factor authentication, Other | Desired improvements for IoT security and privacy |
| Multiple-choice (single select) | 18. Recommend IoT devices despite challenges? | Yes, No, Maybe | Willingness to recommend IoT devices despite existing challenges |
| Open-ended | 19. Additional comments | Text | User suggestions or concerns not covered in previous questions |

Above table categorizes each question by its type (e.g., multiple-choice, Likert scale) and focuses on the analysis that can be derived from the answers, such as ease of use, security concerns, and areas for improvement in IoT systems.

## VI. DATA ANALYSIS

Data collected from surveys were analyzed using descriptive statistics, focusing on the frequency of challenges such as usability issues, security concerns, and device interoperability. Qualitative data from interviews and observations were analyzed using thematic analysis to identify recurring UX themes.

1) Complexity: 70% of respondents reported difficulties in setting up devices, 60% found the interface confusing, and 50% struggled with understanding device controls.
2) Interoperability: 45% experienced issues syncing devices from different manufacturers, 35% had trouble controlling multiple devices simultaneously, and 25% encountered compatibility problems.
3) Security and Privacy: 65% were concerned about hacking, 55% were worried about data collection, and 40% had privacy concerns related to location tracking.

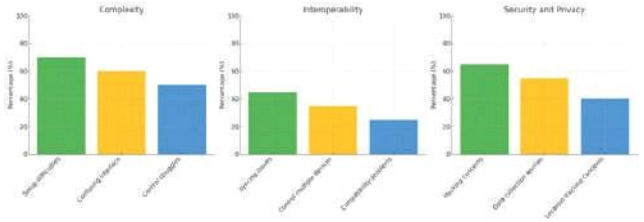



Fig. 1: Graphical Representation of Analysis

### A. *Case Study*

A smart home environment featuring multiple connected IoT devices (smart thermostat, lighting system, smart fridge, etc.), each emitting data or signals. Overlaying the image are visual representations of UX challenges, such as:

1) Complexity: A tangle of wires or app interfaces connecting devices, symbolizing confusing interactions.
2) Privacy Concerns: A data cloud with an eye icon, representing user surveillance concerns, hovering over the devices.
3) Interoperability Issues: Different devices with puzzle pieces that don't quite fit together, symbolizing fragmented integration.
4) Security Concerns: A padlock with cracks or a warning symbol indicating security vulnerabilities.

The smart home setting would be modern, with users interacting (or struggling to interact) with the devices, highlighting the challenges of usability and seamlessness.

## VII. FINDINGS

The survey results indicated that 65% of users faced challenges in setting up and configuring IoT devices, underscoring the complexity of user interfaces. Additionally, 58% expressed concerns about privacy, particularly regarding the constant data collection by smart devices. The observational study revealed that users frequently struggled with the interoperability of various IoT devices from different manufacturers. Many participants had to switch between multiple apps, which negatively affected the seamlessness of their smart home experience. Interviews confirmed that security concerns were a significant barrier to broader adoption, with 70% of respondents indicating reluctance to adopt more IoT devices due to perceived risks.



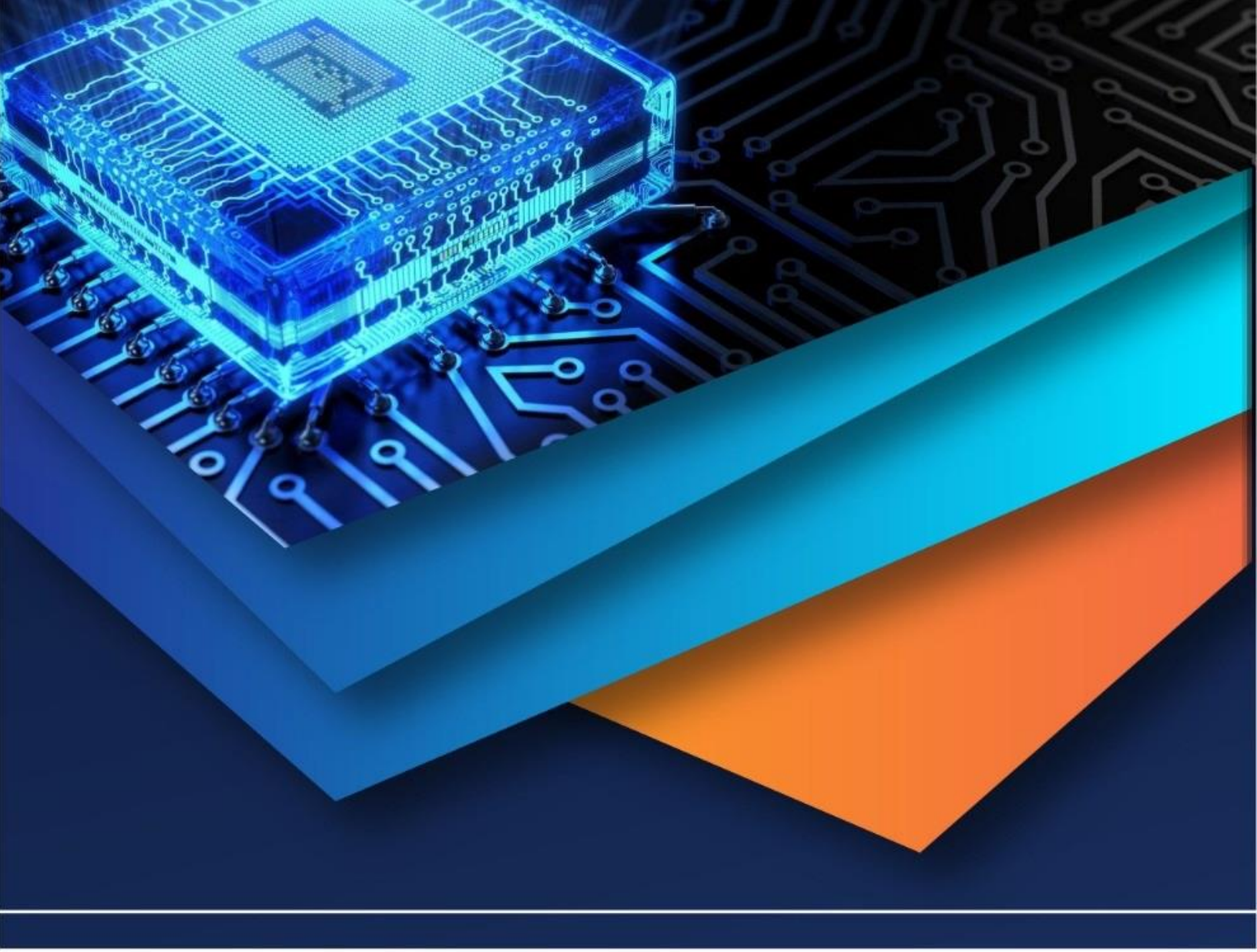

Fig. 2: Breakdown of the key UX challenges identified: Complexity (40%), Privacy Concerns (25%), Interoperability (20%), and Security (15%).

## VIII. CONCLUSION

The findings of this study suggest that while IoT systems hold great potential, it is crucial to address existing UX challenges to enhance adoption and user satisfaction. The most significant factors affecting the user experience were complexity, privacy issues, and interoperability challenges. To improve future IoT designs, it is essential to prioritize user-friendly interfaces, provide greater transparency regarding data collection, and implement stronger security measures. Furthermore, standardizing IoT platforms could significantly reduce the disjointed experience users face when interacting with different devices.

## REFERENCES

[1] Choi, J., & Lee, H. (2019). Privacy in IoT: User Concerns and Design Implications. Journal of Interactive Computing, 23(3), 177-189.
[2] Parker, L., Stevens, M., & Patel, S. (2021). Contextual Awareness in IoT: A User Experience Perspective. IoT Design Journal, 45(6), 401-410.
[3] Verma, S., et al. (2020). Usability Challenges in Smart Home Devices: A Review. Proceedings of the IoT Forum, 122-135.
[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095
[5] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
[6] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31. https://doi.org/10.1016/j. comcom.2014.09.008
[7] Coskun, A., Kaner, G., & Bostan, B. (2018). Interaction design for IoT systems: A human-centered design approach. Journal of Ambient Intelligence and Smart Environments, 10(5), 351-370. https://doi. org/10.3233/AIS-180493
[8] Fenn, J., & Raskino, M. (2019). Mastering the hype cycle: How to choose the right innovation at the right time (2nd ed.). Harvard Business Review Press.
[9] Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart objects as building blocks for the Internet of Things. IEEE Internet Computing, 14(1), 44-51. https://doi.org/10.1109/MIC.2009.14
[10] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440. https:// doi.org/10.1016/j.bushor.2015.03.00
[11] Loh, J., & Srivastava, J. (2019). Enhancing user experience in IoT-based smart environments: Challenges and recommendations. ACM Computing Surveys, 52(1), 1-34. https://doi.org/10.1145/3282430Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. Computer Communications, 89-90, 5-16. https://doi. org/10.1016/j.comcom.2016.03.015.
[12] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 16(1), 414-454. https://doi. org/10.1109/SURV.2013.042313.00197.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)