# MAJOR IOT CHALLENGES AND CRITICAL ISSUES IN REAL WORLD

**Abstract**

Internet of Things is the Connections based on embedded technologies that contained physical objects in real world and is used to communicate and interact with the inner states or the external surroundings, rather than people to people interaction , Major role of IoT machine to machine communication. We focus the status of IoT growth in real world and also contains vital security issues and challenges. IOT based technologies be it in the field of Banking, Agriculture, Healthcare, Mobility, Traffic control, Navigation, Smart home, Smart community, Smart city, Social media and Education have been well researched upon. IOT based scenarios are required for the Special needs, Politics , Journalism, Entertainment, Retail, Manufacturing, e-Governance and Surveillance .There are several security issues, threats and critical challenges with IOT based living scenarios in real world. The paper presents views on Living Scenarios of IOT based real world applications, Critical thinking and cyber laws which regulate the IOT powered systems.

**Keywords:** Internet of Things , Security issues , Challenges and Cyber laws

**Authors**

**Ghanshyam Singh**
Professor
Department of Electronics and Communication Engineering
Jayamukhi Institute of Technological Sciences
Narsampet Warangal, India.

**Shafiqul Abidin**
Associate Professor
Department of Computer Science
Aligarh Muslim University
Aligarh, Uttar Pradesh, India

 

## I. INTRODUCTION

In the forthcoming years, the Internet of Things (IoT) will have a profound impact on business models, security, infrastructure, and trade standards within the realm of IT computing and networking systems. IoT represents an emerging technological frontier that is still in its nascent stages of market development. It holds the potential to accelerate the "sharing economy," introducing novel approaches for the management and tracking of small-scale items, as well as facilitating the sharing of new, modestly priced commodities like community resources, aircraft, cars, and motorcycles. As these trends continue to evolve, IoT will give rise to entirely new applications grounded in IoT principles, thereby catalyzing innovative business models and profit opportunities. This transformation will drive IoT devices and sensors to increasingly granular levels, fostering the creation of fresh real-world applications, services, and IoT-based business models that were previously economically unviable. Nevertheless, it may pose challenges and disrupt existing industries. IOT based technologies be it in the field of – Banking, Agriculture , Healthcare , Mobility, Traffic control, Navigation, Smart home, Smart community , Social media , Education . In depth research for IOT based scenarios are required for - Social media , Special needs , Manufacturing, e-Governance and Surveillance . There are several security issues and challenges with IOT based living scenarios . This paper presents views on Living Scenarios of IOT based real world applications, Critical thinking and cyber laws that may regulate the IOT powered systems.

## II. LITERATURE SURVEY

IOT offers a multidisciplinary perspective and is essential to providing benefits in a number of areas, including industrial, medical, transportation, and environmental. IOT has been approached differently by academicians and researchers in terms of particular elements and areas of interest. Figure 1 reports numerous applications of IoT potentials that demonstrate the main potential and power of IOT.

## III. SECURITY ISSUES AND CHALLENGES OF THE ITERNET OF THINGS WITH IOT BASED MAJOR POTENTIAL REAL WORLD APPLICATIONS

1. **Major Challenges of IOT and Key Issues:** The proliferation of IoT-based systems across multiple facets of human existence and the incorporation of recent data transfer technologies among embedded devices have introduced complexity and led to significant challenges in the realm of IoT. These reported challenges are also formidable obstacles in the development of IoT in highly technologically advanced societies. As technology continues to advance, the demands and hurdles faced by IoT-based systems are on the rise. Consequently, the evolution of IoT necessitates a proactive approach to address emerging issues and offer effective solutions for the challenges at hand.

    - **Security:** Security concerns are a central and indispensable aspect of real-world applications based on the Internet of Things (IoT), representing a significant challenge for the IoT. With the advancement of future technologies, the IoT landscape is expanding from millions of devices to the scale of thousands of billions. As the number of connected IoT devices increases, most IoT ecosystems will comprise groups of similar or closely related devices. This homogeneity amplifies the potential

 

impact of any single security vulnerability due to the sheer quantity of IoT devices sharing similar advantageous characteristics. This article introduces a dynamic approach for data-centric IoT applications in the context of cloud computing platforms or services. Meeting the demands of massive IoT applications running on cloud computing platforms or services necessitates efficient solutions involving appropriate IoT devices, software configurations, and infrastructure. Academics, researchers, and IoT developers are actively engaged in seeking solutions that account for the diversity of platforms and both homogeneous and heterogeneous natures of IoT devices. A primary objective of secure sensor networks is to enhance data privacy, safeguard against attacker interference, and ensure authentication. Notably, two well-regarded SSN services, namely TinySec and ZigBee, offer efficiency and reliability. ZigBee, while providing higher security, consumes more energy, whereas TinySec has lower security but is more energy-efficient in comparison. The MiniSec IoT Architecture also supports low power consumption and high security.

- **B.Privacy:** In the realm of IoT devices, factors like Authenticity, trustworthiness, and Confidentiality hold paramount importance. Additionally, there are other essential requirements, such as the need for discriminating access to specific facilities, preventing the sharing of certain IoT devices at particular times, and ensuring the security of business communications involving smart objects against potential adversaries. Data networks remain fragile and comparatively expensive, particularly in comparison to more developed nations. In the context of India, cloud storage operations are still in the early stages of development. The transmission of secure data to a cloud service for processing sometimes involves the engagement of a third party. Reports from surveys, news articles, and daily news coverage highlight the legal and regulatory challenges that data protection and privacy laws face due to information leaks.

- **Trust Management:** One of the main problems with IOT is trust management. Without having to worry about the unpredictability of IOT-critical issues and users, trust management enables people to comprehend and trust IOT services and apps. The ability to integrate devices and services from many heterogeneous platforms to provide dependable and effective IOT services is a key component of interoperability in IOT devices.

## 2. Scalability , Availability and Reliability

- **Scalability:** If additional services, equipment, and devices are added to a system without causing performance issues, the system is considered stable. Supporting a vast number of devices with different processing speeds, bandwidths, and storage capacities is one of the IOT's main challenges. Scalability is the ability of cloud-based IOT systems to generate enough support for expanding the IOT infrastructure or network by adding more devices, storage, and computing power as required.

- **Availability:** The availability is yet another crucial factor that needs to be taken into account. In the layered IOT framework, both scalability and availability must be implemented simultaneously. As a result, this worldwide dispersed IOT network or

 

infrastructure inspires a fresh method for creating an efficient IOT framework that fully satisfies global requirements.

- **Reliability:** For real-world IOT applications, quality of service parameters like availability, cost, power consumption, security, and service time are crucial and required.

- **Quality of Services :** The term "quality of service" refers to the metric used to assess the effectiveness, caliber, and performance of Internet of Things devices, systems, and architecture.

- **Useful resource compartment:** The records are kept alive by the statistical assistance. Specialized holders include those for software, hardware, servers, systems, physical objects like documents, CDs, DVDs, and people.

- **Critical facts resource :** Large aid is most likely to cause an association significant harm if its security measures are compromised.

- **Hazard:** A risk is an occurrence that has the potential to negatively impact an advantage or mitigate it. It is farmed when a risk-actor takes advantage of a vulnerability.

- **Effect:** The significant or irreversible effect of a danger materializing on an advantage.

- **Risk:** Combining threat and effect results in risk. A threat is the possibility of suffering long-term harm or bad luck; it is formed by an event, a consequence, and a vulnerability.

- **Mitigation:** the interest of lowering the risk factor's seriousness or decreasing the hazard's association by applying different strategies.

## IV. ENVIRONMENTAL , HEALTH CARE AND EMERGING ECONOMY

IOT devices are wholeheartedly dedicated to fostering public and financial benefits, as well as addressing societal needs. This extends to a broad spectrum of public services, including the maintenance of water quality and the promotion of economic and environmental sustainability. One of the significant challenges associated with the environmental impact of IOT devices is their energy consumption, which is escalating rapidly due to the proliferation of internet-enabled services. The adoption of low-energy-consumption IOT devices underscores a commitment to green technologies aimed at generating ample energy for future-efficient devices. This not only promotes environmental friendliness but also has positive implications for human health. Figure 1 illustrates the Internet of Things Approach for Real-World Applications that leverage advancements in future technology.

 

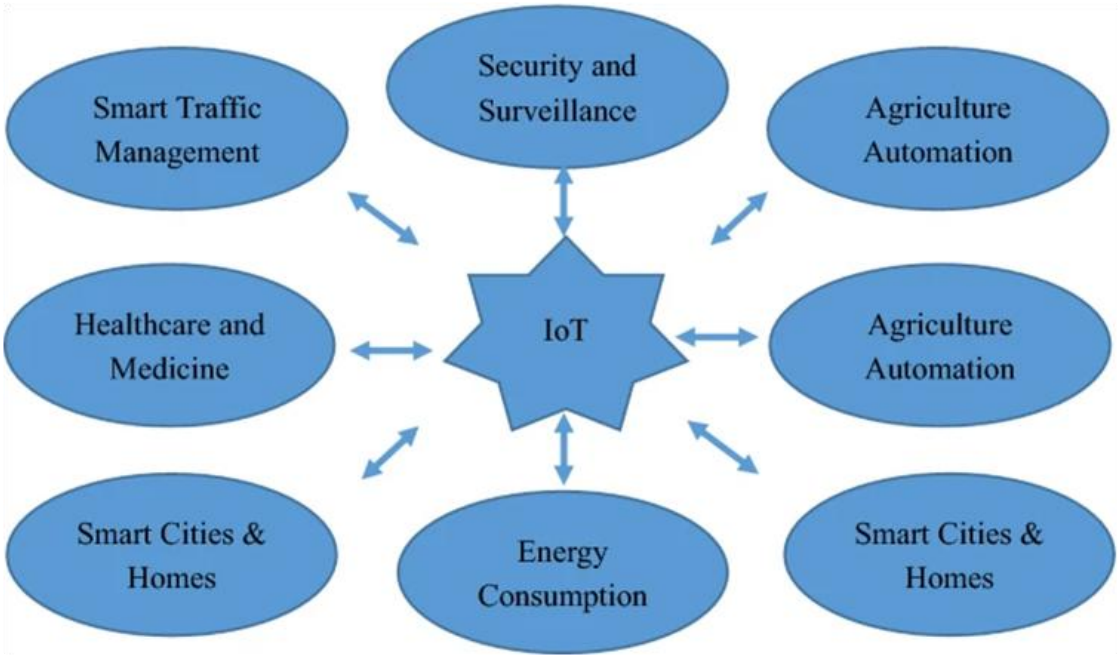


**Figure 1:** Internet of Things Approach for Real World Applications Employing Future Technology Enhancement

## V. DYNAMIC AND STATIC APPROACH OF INTERNET OF THINGS FOR FUTURE ADVANCEMENT OF TECHNOLOGIES

The IOT network or infrastructure comprises five layers, each serving a distinct role in the functioning of IOT systems. The architectural layers in IOT include i) Network layer, ii) Perception layer, iii) Business layer, iv) Middle layer, and v) Application layer. The Perception layer is situated at the base of the IOT infrastructure and encompasses physical devices like RFID chips, sensors, barcodes, and other tangible objects interconnected within the IOT network. These interconnected devices gather data and transmit it to the Network layer. The Network layer serves as the transmission medium for relaying data from the Perception layer to the information processing system. Data transmission may employ various wired or wireless mediums, including Wi-Fi, 3G/4G/5G/6G, and Bluetooth, among others.

The Middle layer is of paramount importance as it grapples with security and privacy challenges posed by a multitude of cyber threats, risks, and vulnerabilities within the IOT system. Privacy-related issues at the device level are attributed to factors like inadequate authorization and authentication, insecure software, web interfaces, and subpar transport layer encryption. Privacy and security hold significant value as fundamental parameters for both dynamic and static approaches to the Internet of Things in the pursuit of advancing future technologies and building trust in IOT systems across all dimensions. Embedding security mechanisms at each layer of the IOT infrastructure is essential for thwarting security breaches and threats. Several protocols have been developed and efficiently implemented across transmission channels at each layer to ensure security and privacy within IOT systems. The datagram transport layer security and secure socket layer are the one of cryptographic protocols that implemented between the application layer and transport layer to provide safe

 

security solutions in various IOT systems. The Global Market Share of IOT Based Real World Applications is reported in figure 2.

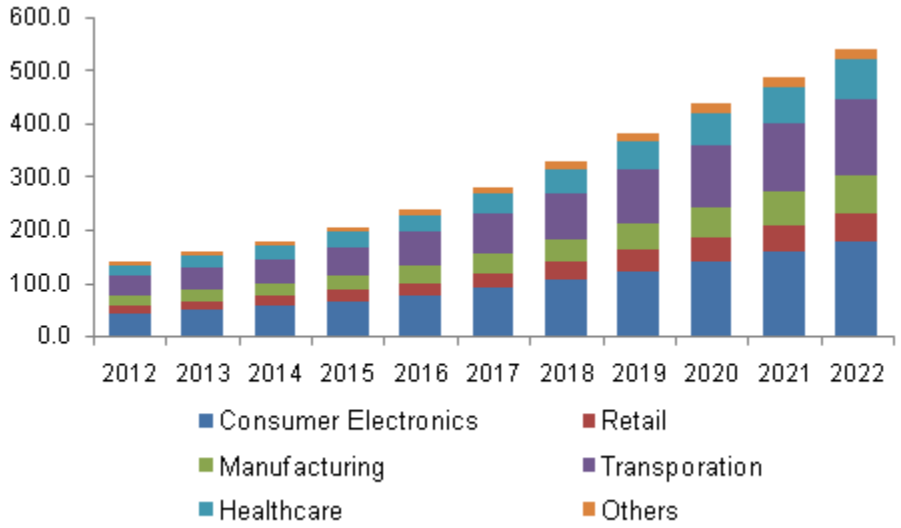


**Figure 2:** The Global Market Share of IOT Based Real World Applications

The major IOT based real world applications are reported in figure 3. Therefore is a requirement to provide smart solutions for mobility or migration , healthcare, energy ,infrastructure ,smart city ,smart home and smart agriculture. Today's academicians and researchers are focused on smart city , it is the critical issue and one major important application in the areas of researchers in the field of IOT developers. IOT developers fields explore several critical issues for examples are i) Air Quality Management 2) Traffic Management 3) Smart Parking 4) Smart Waste Collection and Smart Lightning. IOT is working hard to tackle and provide solutions for these challenging issues. Therefore the need for improvement smart city infrastructures with the development of urbanizations have provided opportunities for entrepreneurs in the various fields of smart city technologies. We reported IOT enabled technologies have played vital role for the development of sustainable smart home as well as smart cities.

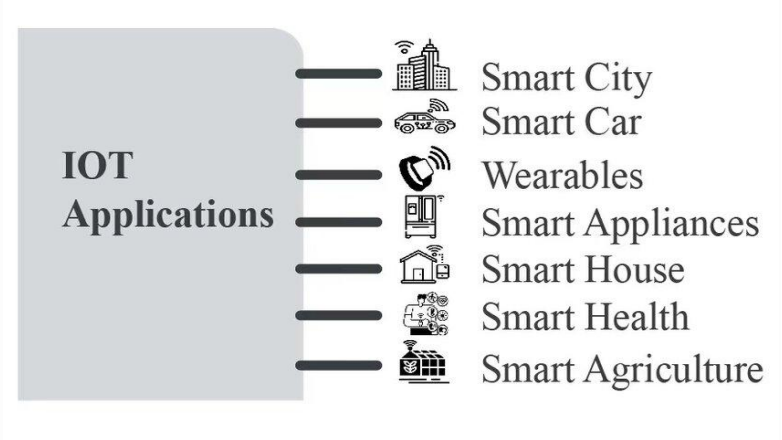


**Figure 3:** IOT Based Real World Projects

 

## VI. CYBER LAW AND ETHICS

Cyber law state that it is legal system that includes Cyberspace , Computer system, Internet ,different aspects of information technology and cybercrime may includes such as False documentation , Forgery, Forgery pre planned for cheating ,Reputation damage , Child pornography , Hacking , Denial of service attack, Virus dissemination, Computer forgery, Fraud card , Phishing , Spoofing , Email bombing , Virus attack, Trojan attack and Presenting a forgery documents as genuine etc. The fastest-growing infrastructure in daily life today is the internet. The modern technological environment is transforming humanity through the use of numerous cutting-edge technology. These new technologies make it difficult for us to effectively protect our personal information, which is why cybercrimes are growing daily. The security and privacy of our data will always be the most important security precautions that every firm takes. In the real world in which we currently live, all information is kept in digital or cyber form. All users of social networking sites can engage with friends and family in a safe environment. Cybercriminals should keep focusing on social media sites in order to obtain personal information from home users.

## VII. PERFORMANCE EVALUATION OF AN IOT SYSTEMS EMPLOYING FUTURE ENHANCEMENT TECHNOLOGIES

The performance evaluation of an IOT systems for feature enhancement technologies have following advantageous are described as

1. In today's business landscape, companies of all sizes are gradually embracing cloud services, signifying a gradual shift toward cloud adoption.

2. This emerging technique poses a significant challenge to cybersecurity, as it allows data traffic to bypass traditional inspection points. Furthermore, with the proliferation of cloud-based applications, policies for web applications and cloud services must evolve to prevent the loss of valuable information.

3. As users become more social in an increasingly interconnected world, businesses must explore innovative methods to safeguard personal information. Social media plays a crucial role in cybersecurity and can contribute to various personal cyber threats.

4. The adoption of social media among employees is skyrocketing, paralleled by an increased threat of cyberattacks. Given that social media and social networking sites are integral parts of daily life for most individuals, they have become attractive platforms for cybercriminals seeking to hack private information and steal valuable data.

5. In today's world, various cybersecurity techniques are predominantly employed, including 1. Access Control and Password Security, 2. Data Authentication, 3. Firewalls, 4. Anti-Virus Software, and 5. Malware Scanners.

6. The internet is often likened to the world's largest library, containing information on a wide array of topics and subject areas. Therefore, using this information correctly and legally is always essential.

7. Avoid accessing others' accounts using their passwords.

 

8. Never attempt to send malware to other systems with the intention of causing corruption.

9. Refrain from sharing your personal information with anyone, as there is a high risk of misuse, potentially leading to trouble.

10. This article covers the full range of technologies required to ensure the smooth functionality of IoT systems, with a particular focus on cloud security as a solution.

11. Many IoT systems are inadequately designed and implemented, employing diverse protocols and technologies, resulting in complex configurations.

12. Logging and audit standards have not been defined for IoT devices.

13. Best practices for incident response activities related to IoT are not readily available.

14. Security concerns surrounding IoT systems have already become a significant challenge, garnering the attention of prominent tech firms and government agencies worldwide.

15. Hacking incidents involving baby monitors, drug infusion pumps, smart fridges, and cameras represent significant security concerns stemming from the future of IoT systems.

## VIII. CONCLUSION

We conclude that IOT leverages smart gadgets and the internet to offer creative answers to important problems facing industry, government, and private sectors. By growing the use of IOT devices and improving future technologies, we can achieve a significant revolution in our daily lives. One of the actual uses of IOT is the smart city, which combines smart homes. Home appliances, air conditioning, heating, audio video streaming devices, and security systems are all made possible by the Internet of Things. IOT is therefore entirely committed to bringing about new financial and societal advantages as well as advancement for people and society.

## IX. SUMMARY

In this paper, we primarily address the current state of IOT devices, including potential applications and significant obstacles. Global scholars, researchers, and developers have taken notice of the new technological developments in IOT services. Researchers, academics, and IOT developers are collaborating to improve technologies on a massive scale that will benefit society to the greatest extent possible. We examine the numerous IOT problems and inadequacies of current technology approaches in this article. In order to create a better model, academics, researchers, and developers should be considered. We'll also talk about big data analytics, which can help make more precise decisions that can be applied to the creation of better IOT systems.

 

## REFERENCES

[1] Guan, W and Pei, Z. (2022),“ An Integrated Social-Technical Framework of Smart City based on Internet of Things and Cloud Computing. ICIT '22: Proceedings of the 2022 10th International Conference on Information Technology: IoT and Smart City.Pages 197–203. https://doi.org/10.1145/3582197.3582231

[2] Lian, Y. (2021) ,“ Smart Education: Education Reform in the Age of Intelligence. ICEEL '21: Proceedings of the 2021 5th International Conference on Education and E-Learning. Pages 41–45. https://doi.org/10.1145/3502434.3502478

[3] Magnus, JP, Lopez, MG and Govea, JMO. (2021) ,“ Remote Challenge-Based Education through IoT.DSDE '21: 2021 4th International Conference on Data Storage and Data Engineering. February 2021. Pages 117–128. https://doi.org/10.1145/3456146.3456165

[4] Jean, D. Stein, G and Ledeczi, A. (2021) ,“ Hands-On IoT Education with Mobile Devices. IPSN '21: Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021, Pages 390–391. https://doi.org/10.1145/3412382.3458778

[5] Baykal, G, Mechelen, MV and Eriksson, E. (2020) ,“ Collaborative Technologies for Children with Special Needs: A Systematic Literature Review. CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. April 2020. Pages 1–13. https://doi.org/10.1145/3313831.3376291

[6] Prakash, S and Gunalan, I. 2020. A new business model for digital governance of public records using blockchain. ICEGOV '20: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. September 2020. Pages 124–128. https://doi.org/10.1145/3428502.3428518

[7] Venkatraman, S, Overmars, A, Fahd, K, Parvin, S and Kaspi, S. 2020. Security Challenges for Big Data and IoT. BDET 2020: Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology. January 2020. Pages 1–6. https://doi.org/10.1145/3378904.337890

[8] Ramesh, M.N. (2019) ,“ Integration of participatory approaches, systems, and solutions using IoT and AI for designing smart community: Case studies from India. TESCA'19: Proceedings of the 1st ACM International Workshop on Technology Enablers and Innovative Applications for Smart Cities and Communities. Pages 4–5. https://doi.org/10.1145/3364544.3371501

[9] Mishra, D, Pande, T, Agarwal, KK, Abbas, A, Pandey, A and Yadav, RS. (2019) ,“Smart agriculture system using IoT. ICAICR '19: Proceedings of the Third International Conference on Advanced Informatics for Computing Research. June 2019. Article No.: 39. Pages 1–7. https://doi.org/10.1145/3339311.3339350

[10] Celestrini, J, Rocha, RN, Saleme, EB, Santos, Cs, Filho, J G and Andreao, RV. (2019) ,“ An architecture and its tools for integrating IoT and BPMN in agriculture scenarios. SAC '19: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. Pages 824–831. https://doi.org/10.1145/3297280.3297361

[11] Hedestig, U, Skog, D and Soderstrom, M. (2018) ,“ Co-producing public value through IoT and social media. dg.o '18: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. Article No.: 22. Pages 1–10. https://doi.org/10.1145/3209281.3209349

[12] Khawla, M and Tomader, M. (2018) ,“ A Survey on the Security of Smart Homes: Issues and Solutions. ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment. Pages 81–87. https://doi.org/10.1145/3289100.3289114

[13] Salim, J, Hammoudeh, M, Raza, U, Adebisi, B and Ande, R. (2018) ,“ IoT standardisation: challenges, perspectives and solution. ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. June 2018. Article No.: 1. Pages 1–9. https://doi.org/10.1145/3231053.3231103

[14] Diaz, JSS, Zambrano, EC and Zapater, JJS. (2018) ,“ State of the art about use of IoT in education. EATIS '18: Proceedings of the Euro American Conference on Telematics and Information Systems. Article No.: 22. Pages 1–5. https://doi.org/10.1145/3293614.3293655

[15] He, JS, Ji, S and Bobbie, PO. (2017) ,“ Internet of Things (IoT)-based Learning Framework to Facilitate STEM Undergraduate Education. ACM SE '17: Proceedings of the SouthEast Conference. Pages 88–94. https://doi.org/10.1145/3077286.3077321

[16] Ayele, WY and Skielse, GJ. (2017) ,“ Social media analytics and internet of things: survey. IML '17: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. Article No.: 53. Pages 1–11. https://doi.org/10.1145/3109761.3158379

[17] Xiao, B. (2017) ,“ Self-evolvable knowledge-enhanced IoT data mobility for smart environment. IML '17: Proceedings of the 1st International Conference on Internet of Things and Machine Learning. Article No.: 28. Pages 1–14. https://doi.org/10.1145/3109761.3109789

 

[18] Balakrishnan, S, Vasudevan, H and Murugesan, R.K. ,"Smart Home Technologies: A
[19] Kahlert, M and Constantinides, E. (2017) ," The relevance of technological autonomy in the customer acceptance of IoT services in retail. ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing.. Article No.: 12. Pages 1–7. https://doi.org/10.1145/3018896.3018906
[20] Loi, F, Sivanathan, A, Gharakheili, HH, Radford, A and Sivaraman, V. (2017) ," Systematically Evaluating Security and Privacy for Consumer IoT Devices. IoTS&P '17: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. Pages 1–6. https://doi.org/10.1145/3139937.3139938
[21] Conti, M, Natale, G, Heuser, A, Poppelman, T and Mentens, N. (2017) ,"Do we need a holistic approach for the design of secure IoT systems? CF'17: Proceedings of the Computing Frontiers Conference. May 2017. Pages 425–430. https://doi.org/10.1145/3075564.3079070
[22] Ferati, M, Kurti, A, Vogel, B and Raufi, B. (2016) ," Augmenting requirements gathering for people with special needs using IoT: a position paper. CHASE '16: Proceedings of the 9th International Workshop on Cooperative and Human Aspects of Software Engineering. Pages 48–51. https://doi.org/10.1145/2897586.2897617

 