Challenges and Issues of Modern Science, 3 (2024). ISSN: 3083-5704
URL: https://cims.fti.dp.ua/j/article/view/200
PURL: https://purl.org/cims/2403.020

Internet of Things (IoT) technologies: features, development prospects and potential threats

Daria Margaza, Yurii Yurchenko

Purpose. The article aims to explore the characteristics, development prospects, and possible threats associated with Internet of Things (IoT) technologies. With IoT rapidly integrating into multiple industries, understanding both its advantages and risks is crucial for future advancements. **Design / Method / Approach**. This research adopts a conceptual approach, analyzing selection of literature, case studies, and industry reports to synthesize the current state of IoT technologies. The study highlights technological developments, emerging applications, and possible security threats in different fields. **Findings**. The study reveals that IoT is driving innovation and efficiency across industries, including healthcare, manufacturing, and smart cities. However, it also underscores significant challenges, such as cybersecurity risks, data privacy concerns, and regulatory gaps that may hinder widespread adoption. **Theoretical Implications**. The research contributes to the theoretical understanding of IoT by addressing the need for comprehensive models that account for both the technological growth and the potential risks IoT poses, particularly in the context of security and ethical considerations. **Practical Implications**. For practitioners, this study offers actionable insights on deploying IoT solutions securely and effectively, with an emphasis on risk management. The findings also inform on how to develop regulations that ensure safe and sustainable IoT adoption. **Originality / Value**. This paper provides a balanced overview of IoT's potential benefits and inherent risks, offering a unique contribution by integrating various perspectives from technology development to societal implications, while addressing underexplored areas of IoT security. **Research Limitations / Future Research**. The study is limited by its reliance on secondary data sources. Future research could involve empirical investigations into the practical implementation and long-term effects of IoT technologies in specific sectors. **Paper Type**. Conceptual.

Keywords:

Internet of Things (IoT), development prospects, potential threats, security risks, data privacy concerns, cybersecurity

Contributor Details:

Daria Margaza, Undergraduate Student, State University of Trade and Economics: Kyiv, UA, D.Marhaza_FIT_6_21_B_d@knute.edu.ua

Yurii Yurchenko, Senior Instructor, State University of Trade and Economics: Kyiv, UA, y.yurchenko@knute.edu.ua

As IoT becomes an integral part of sectors such as healthcare, manufacturing, and smart cities, it is crucial to understand not only its benefits but also the risks and challenges associated with its widespread adoption. One of the key issues that emerges is the vulnerability of IoT systems to cybersecurity threats, data privacy concerns, and gaps in regulatory frameworks, all of which can impede further development and safe implementation.

Despite the growing body of literature on IoT, many aspects remain underexplored. Previous research has extensively examined the technological potential of IoT and its applications across various industries, yet there is a significant gap in understanding the security implications and long-term sustainability of these systems (Atzori et al., 2010). This research aims to address this gap by providing a balanced overview of IoT technologies, focusing on their unique characteristics, development prospects, and the potential threats that they pose. The study synthesizes existing knowledge while offering new insights into the theoretical and practical implications of IoT deployment, particularly in terms of risk management and policy development.

The structure of this article is organized as follows. The next section presents a detailed literature review, summarizing key findings and identifying gaps in the current research. This is followed by a conceptual analysis of IoT technologies, focusing on their technical features, potential applications, and the associated risks. The article then discusses the theoretical and practical implications of the research, offering recommendations for industry professionals and policymakers. Finally, the conclusion outlines the study's contributions and suggests directions for future research, emphasizing the need for empirical studies to further explore the challenges and opportunities presented by IoT.

Literature review

The Internet of Things (IoT) has emerged as a transformative technology, offering substantial advancements across various sectors. In industries such as healthcare, manufacturing, agriculture, and smart cities, IoT facilitates real-time data processing, automation, and improved operational efficiency. For instance, in the healthcare sector, IoT technologies have enabled enhanced patient monitoring and remote diagnostics, as noted by Williams in his 2018 study "The Impact of IoT in Modern Healthcare." Similarly, in the manufacturing sector, IoT-driven automation has improved predictive maintenance and supply chain management, as highlighted by Gupta in the paper "IoT in Smart Manufacturing Systems" (2019).

While the benefits of IoT are clear, the associated risks have become a focal point of recent studies. One major concern is the growing threat of cybersecurity breaches, as IoT devices often operate without sufficient security measures. Chen and Liu, in their 2021 work "Cybersecurity Vulnerabilities in IoT: A Growing Concern," discuss how weak encryption and lack of authentication protocols have made IoT systems particularly vulnerable to cyberattacks.

Despite the extensive research on IoT's potential, there remain significant gaps in understanding its long-term security implications. In particular, few studies have empirically analyzed how security threats evolve as IoT networks scale.

Brown's 2022 review, "Securing IoT Networks: A Call for Empirical Studies," emphasizes the need for large-scale studies to better comprehend the real-world risks. These gaps highlight the necessity for more comprehensive research into securing IoT systems while ensuring their sustainability and growth (Miorandi et al., 2012).

This study seeks to address these gaps by providing a balanced analysis of IoT technologies, focusing on both the potential benefits and the risks, particularly concerning security challenges. By building upon the existing literature, this paper aims to contribute valuable insights into IoT's development prospects, practical implications, and the future direction of IoT security research.

Conceptual analysis of IoT technologies

The Internet of Things (IoT) comprises a network of interconnected devices that communicate with each other through the internet, enabling real-time data collection, processing, and decision-making. The foundation of IoT lies in the seamless integration of hardware (sensors, actuators, and devices) and software (cloud computing, data analytics, and machine learning).

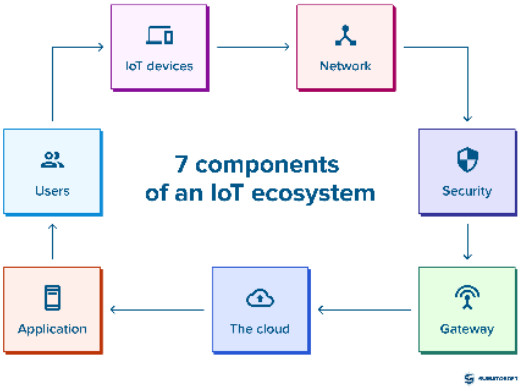

Figure 1 – An Example of IoT ecosystem (Source: Shamrei, 2023)

Technical features

IoT systems are characterized by several key technical features. First, connectivity enables devices to communicate and transfer data through protocols such as Wi-Fi, Bluetooth, and 5G networks. Sensors play a critical role by gathering environmental data, such as temperature, humidity, or motion, which is then processed by edge computing systems to make faster decisions closer to the source of data collection (Shamrei, 2023). Meanwhile, cloud computing ensures that vast amounts of data can be stored and processed efficiently. The use of artificial

intelligence (AI) and machine learning (ML) allows IoT systems to become more adaptive by identifying patterns in data and making predictive analyses (Presciuttini et al., 2024).

Potential implementation

The applications of IoT technologies are broad and span various industries:

– Smart cities. IoT enhances urban infrastructure by optimizing traffic flow, managing energy consumption, and monitoring environmental conditions. Smart lighting systems and waste management powered by IoT have been successfully implemented in cities like Barcelona and Singapore (Whaiduzzaman et al., 2022).

– Healthcare. IoT devices in healthcare, such as wearable health monitors, provide real-time data on patients' vital signs. This allows for remote diagnosis and personalized treatment plans, improving overall patient care (Wakili & Bakkali, 2024).

– Agriculture. IoT sensors in precision farming monitor soil conditions, crop health, and weather patterns, leading to improved crop yields and more efficient resource management (Gilchrist, 2016).

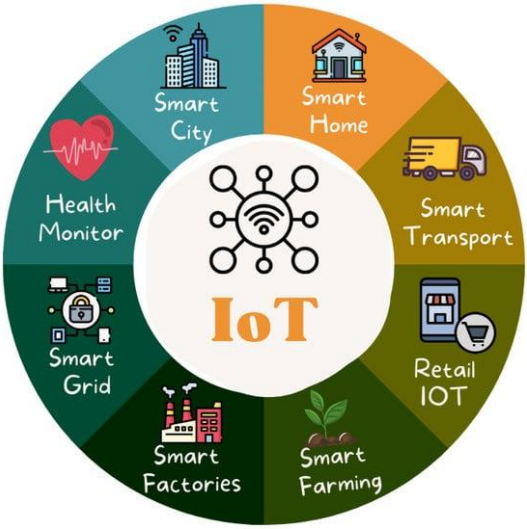

Figure 2 – Application of IoT supporting a variety of industries (Source: Whaiduzzaman et al., 2022)

Associated risks

Despite these advances, IoT is fraught with significant security risks. Cybersecurity vulnerabilities are a major concern as many IoT devices lack robust encryption and authentication measures, making them vulnerable to hacking, data

breaches, and Distributed Denial of Service (DDoS) attacks (Campos et al., 2016). Data privacy is another issue, with sensitive information being collected and stored by IoT systems, often without adequate user consent or regulatory oversight. Moreover, interoperability challenges arise when different IoT devices and platforms are not compatible, creating bottlenecks in large-scale deployment (Mohanta et al., 2020).

Theoretical and practical implications

The research into IoT technologies presents both theoretical and practical implications.

On the theoretical front, the study of IoT opens up discussions on the integration of complex networks, security protocols, and ethical considerations regarding data privacy. One of the major theoretical contributions is the need to develop comprehensive models that can address the security vulnerabilities inherent in IoT systems. Current models tend to focus on the benefits and functionality of IoT, but this research highlights the importance of incorporating security and ethical dimensions into the design of IoT systems from the ground up (Campos et al., 2016).

On the practical side**,** IoT technologies offer significant opportunities for businesses, governments, and industries. In sectors such as healthcare and manufacturing, IoT has already led to cost savings, improved efficiency, and better decision-making**.** However, the research underscores the practical need for industry professionals to implement strong cybersecurity measures and work closely with policymakers to establish regulatory frameworks that protect data privacy and ensure the safe use of IoT devices (Gilchrist, 2016).

Conclusion

This research highlights the significant potential of Internet of Things (IoT) technologies to transform industries such as healthcare, manufacturing, and smart cities by improving automation, efficiency, and decision-making. The study has demonstrated that IoT is driving innovation, yet its widespread adoption is hindered by critical security and privacy challenges (Miorandi et al., 2012).

One of the key contributions of this research is its focus on the cybersecurity vulnerabilities inherent in IoT systems. Weak encryption and insufficient security protocols leave IoT devices exposed to cyberattacks, raising concerns about data privacy and system integrity. As IoT ecosystems continue to grow, addressing these security issues will be crucial for the safe and sustainable deployment of IoT solutions (Campos et al., 2016).

This study contributes both theoretically and practically. The theoretical insights emphasize the need for comprehensive models that account for IoT's technological development while integrating robust security measures and ethical considerations. These models must be flexible enough to accommodate the rapid evolution of IoT technologies (Mohanta et al., 2020). Practically, the findings offer actionable recommendations for industry professionals, particularly in adopting secure IoT frameworks and collaborating with policymakers to develop effective

regulatory standards. Industry players must prioritize the development of security-first solutions, ensuring that cybersecurity is considered from the earliest stages of IoT system design and deployment (Kim et al., 2017).

The findings provide a foundation for future research, which should focus on empirical studies assessing the real-world implementation of IoT technologies, especially regarding their long-term impacts on cybersecurity, privacy, and regulatory compliance (Mekala et al., 2023). Future research should also explore emerging trends in IoT, such as the integration of artificial intelligence (AI) and machine learning (ML), and how these innovations may affect the security landscape. This will ensure that IoT's expansion continues in a secure and sustainable manner, benefiting industries and society at large (Presciuttini et al., 2024).

References

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

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Wakili, A., & Bakkali, S. (2024). Internet of Things in healthcare: An adaptive ethical framework for IoT in digital health. *Clinical EHealth, 7*, 92–105. https://doi.org/10.1016/j.ceh.2024.07.001

Gilchrist, A. (2016). *Industry 4.0*. Apress. https://doi.org/10.1007/978-1-4842-2047-4

Presciuttini, A., Cantini, A., Costa, F., & Portioli-Staudacher, A. (2024). Machine learning applications on IoT data in manufacturing operations and their interpretability implications: A systematic literature review. *Journal of Manufacturing Systems, 74*, 477–486. https://doi.org/10.1016/j.jmsy.2024.04.012

Kim, T., Ramos, C., & Mohammed, S. (2017). Smart City and IoT. *Future Generation Computer Systems, 76*, 159–162. https://doi.org/10.1016/j.future.2017.03.034

Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things, 11*, 100227. https://doi.org/10.1016/j.iot.2020.100227

Campos, J., Sharma, P., Jantunen, E., Baglee, D., & Fumagalli, L. (2016). The Challenges of Cybersecurity Frameworks to Protect Data Required for the Development of Advanced Maintenance. *Procedia CIRP, 47*, 222–227. https://doi.org/10.1016/j.procir.2016.03.059

Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications, 208*, 294–320. https://doi.org/10.1016/j.comcom.2023.06.020

Shamrei Y. (2023, September 4). *IoT Ecosystem: Top 7 Components*. SUMATOSOFT. https://sumatosoft.com/blog/iot-ecosystem-top-7-components

Whaiduzzaman, M., Barros, A., Chanda, M., Barman, S., Sultana, T., Rahman, Md. S., Roy, S., & Fidge, C. (2022). A Review of Emerging Technologies for IoT-Based Smart Cities. *Sensors, 22*(23), 9271. https://doi.org/10.3390/s22239271