



# University of Essex

Research Methods and Professional Practice

## Literature Review

Challenges of implementing IoT in secondary schools in  
developing countries – Poor Nations

Haseeb Abdulhak

STUDENT ID: 12687995



## Table of Contents

Introduction.....	1
Benefits of IoT in Education .....	1
Challenges of Implementing IoT in Secondary Schools in Developing Countries .....	2
Conclusion .....	5
References.....	7

## Introduction

The phenomenon known as the IoT describes a vast, interconnected network of gadgets that are linked together and engage in communication with one another with the Internet, the primary goal of the IoT idea is to turn ordinary devices into intelligent, autonomous appliances that can be controlled online at any time and from any location (Sreekantha et al., 2020). Remote sensing and control of items is made possible by the IoT, opening possibilities for the integration of computer systems with the real world to increase productivity and accuracy (Ramson et al., 2020). IoT possesses the capability to revolutionize many facets of society. The sector of education, particularly secondary school, is one area where the IoT has the potential to make a significant difference. However, there are issues that need to be resolved when introducing IoT in secondary schools in impoverished nations.

Implementation of IoT technology in secondary education in developing countries presents both challenges and opportunities. The educational system in developing country such as Saudi Arabia is swiftly adopting new technology to raise the standard of instruction and promote student learning (Alharbi et al., 2019). However, in developing countries, the application of IoT in education remains in its early phases (Madni et al., 2022).

This literature study intends to critically review the issues with adopting IoT in secondary schools in developing countries, particularly in poor nations.

## Benefits of IoT in Education

IoT technology may be employed to gather and utilize data to improve educational outcomes, assist in the achievement of learning objectives, and promote operational efficiency in schools (Suduc et al., 2018). In addition, monitoring of student physiological data alongside the estimation of their attention and involvement are two areas where IoT sensors and devices are used (Yeh et al., 2020). IoT items may be integrated in schools as instructional tools and end products to support successful efficient instruction and practical learning (Fidai et al., 2019). In contrast, Asad et al. (2022) argue that the application of IoT devices extends beyond educational processes, it facilitates managing campus resources such as safeguarding education premises, reduce the power consumption, heat control, and facial detection. Which is agreed by Vinayachandra & Krishna Prasad (2020), by utilizing less

energy, the use of IoT in the creation of an intelligent educational environment can reduce energy consumption.

#### Challenges of Implementing IoT in Secondary Schools in Developing Countries

Previous studies showed many challenges facing developing countries to adopt Internet of Things technology in secondary education. One of these challenges is related to hardware, such as inadequate infrastructure, where the accessibility of the Internet and a dependable network, energy supply, and device availability are critical in the functioning of Internet of Things technology.

Dagnaw & Tsige (2019) highlight that when it comes to enabling IoT, one of the most pressing issues is Internet connectivity, the IoT necessitates faultless and appropriate connection between all things, which requires high Internet speed, constant energy source, and stable infrastructure. Similarly, LÓPEZ-VARGAS et al. (2020) state that connectivity is one of the most significant barriers to spreading IoT in poor nations. Considering the people in developing countries still struggle for basic life requirements such as water and electricity, , it could be argued that Internet access is a far demand, which may hinder schools' capacity to properly integrate IoT into their teaching processes. In contrast, Ali et al. (2023) find Internet connectivity and inadequate infrastructure have insignificant effect on the rates of implementation within higher education institutions. According to UNICEF-ITU report (2020) “Two thirds of the world’s school-age children have no internet access at home”. Furthermore, it is expected that the number of people living without electricity will increase in 2022, reaching nearly 775 million in the world, especially in developing countries (IEA, 2022).

Another key challenge is the economic challenges, which cause a shortage of financial resources in the education sector, and thus result in a lack of investment in purchasing equipment and implementing the appropriate infrastructure. IoT installation is frequently expensive, requiring not only the purchase of equipment but also maintenance, security measures, and training. The significant expenses involved with IoT adoption might be prohibitive for schools in developing nations.

Purchasing programmable robots and toys costs instructors thousands of dollars, and the majority of public educational institutions do not have the funds to do so (Fidai et al., 2019).

Safdar et al. (2019) indicated the financial resources serve as essential in integrating IoT devices and equipment in the educational setting, an adequate budget will enable the use of appropriate IoT equipment. Dagnaw & Tsige (2019) support the view, the financial challenges such as the high cost of purchase, maintenance, and sustainability, for example the sensor device which is the basis for the expensive and often proprietary IoT technology, affects its widespread deployment in developing countries. Despite the implementation of IoT will assist to preserve paper and printed materials, the IoT technology will necessitate three costly components which are hardware, software, and application (Aljaseim, 2021).

While technology must be practical and easy to use, it must also be cost effective. When the advantages of technology are unknown, this making adoption harder, the expenditure of technology is typically linked to the usefulness of IoT use, and as such, it remains a substantial obstacle throughout the deployment phase (Khan et al., 2023). The adoption of the Internet of Things in secondary education may not have immediate economic benefits, but it can certainly enhance the quality of education and provide long-term advantages to students and their nations.

Additionally, security and privacy concerns considered significant when it comes to IoT environment. When IoT devices are installed in education environments, their ability to capture personal information without authorization presents serious privacy concerns. According to Bitdefender Report (2023), many IoT devices come with cameras, microphones, and other sensors that might collect data on users without their knowledge or consent, which could lead to privacy violations. Sultana and Tamanna (2021) called attention to the security and privacy concerns that emerge because of IoT devices gather and analyze pupils and teachers' data and store them online, which might jeopardize their privacy. The IoT system generates vast amounts of data due to the ubiquity of devices and their autonomous decisions, users maybe unclear about how the acquisition, use, and sharing of data (van Deursen et al., 2021). In the same context, Tawalbeh et al. (2020) emphasize none of the recognized obstacles has a greater impact on IoT adoption than security and privacy, the reason for the privacy worries stems from the widespread use of the intelligent devices where data collection and conveyance can occur almost anywhere in IoT.

In other hand, Mercan et al. (2020) emphasize as the number of assaults on IoT devices has grown, one of the most significant barriers to widespread adoption is security, suggests

using original, known-brand devices reduces the likelihood of being targeted via compromised devices. They argue that IoT implementation should take a comprehensive strategy that addresses the whole lifecycle, including security at all levels from design through deployment as well as the device firmware should be updated on a frequent basis to implement available fixes. However, they fail to consider communication attacks such as eavesdropped, where the network connection being utilized for transmitting the data is insecure and might potentially be observed or intercepted by a hostile hacker.

Original and brand IoT devices are not immune to hacking. Indeed, many networks already include weak devices that are easily compromised, including devices from various manufacturers. Arina & Anatolie (2021) argue that IoT devices firmware updates and upgrades, and patch installation are normally handled centrally, however compromised communications can allow attackers to change packages, therefore, attackers can alter the contents of the update package by installing their own applications, via which they can subsequently get access. In addition, a large-scale investigation by Zhao et al. (2022) on IoT device vulnerabilities discovered that a considerable number of devices contain N-day vulnerabilities, and some of these susceptible devices, including those from well-known manufacturers, may have already been infected by botnets. They discovered that all companies that provide automated update procedures for their devices resulted low vulnerability rate. In contrast, they highlighted that despite suppliers have previously released patched firmware, majority of customers have yet to upgrade their firmware. Moreover, include security during the IoT manufacturing life cycle will improve the protection but will rise the cost of devices which is not affordable to countries with financial limitation. Security is crucial in the IoT scenario, but it is difficult to manage in an economical manner owing to smart items' low processing capabilities (Bodei & Galletta, 2016). According to Ho-Sam-Sooi et al. (2021), security and privacy are significant factors that can impact the price of IoT gadgets and security influences customer purchasing behavior. However, they find that higher risk-aware Customers are more inclined to think about security and privacy while making IoT purchases. The right to privacy is uncontested in developed countries, but not in developing countries, where cultural, religious, economic, and notably developmental policy variables all play a role in this status in addition to the lack of data protection regulation (Knopp, 2019).

Security measures are critical for safeguarding IoT systems from cyber-attacks and assuring their integrity, it is critical to balance security measures with low-cost equipment. To address privacy and security concerns in developing countries, manufacturers and regulators must collaborate on cost-effective solutions as well as governments, organizations, and politicians must work together to increase awareness and promote best practices in the digital era.

Another challenge is related to human (the lack of skilled personnel, resistance to change, lack of awareness). Based on the technological environment, Altameem (2020) addressed the key IoT issues in developing nations, IT professionals play a crucial role in the ongoing progress of IoT systems, adequate IT skills are needed to improve the likelihood of adoption. Adoption of technology poses several challenges, including managing complex digital data, guaranteeing data security and dependability, dealing with the complexity of new technologies, assuring access to technology, and responding to changing demands (Mohammadian, 2019). The successful implementation of IoT requires a trained and skilled workforce with technical expertise, to provide user-friendly and easily accessible services, the associated workforce must be efficient, it is evident from literature that the deficiency in technical proficiency among employees can have negative effects on the system (Sharma et al., 2020). Instructors deem training to be indispensable due to the dearth of qualified computer instructors who can move from traditional teaching methods to modern electronic learning platform based on IoT, the benefits of deploying IoT or smart devices in high education are not generally known by students and teachers (Madni et al., 2022). IoT acceptance and prospective applications are still limited, particularly in developing countries, even though several educational institutions have implemented IoT on their campuses (Al-Emran et al., 2019). Students showed less interest in digital learning, together with a high e-learning cost is another reason why they are less inclined to use it frequently (Saputra et al., 2020). Therefore, lack of knowledge and comprehension of the advantages of IoT can lead to unwillingness to abandon old ways of doing things which known as resistance to change.

## Conclusion

Internet of Things have the capability to enhance the learning experience of secondary school pupils. However, Introducing the Internet of Things (IoT) into secondary schools in developing countries faces several challenges, including financial constraints, insufficient training and technical assistance, concerns about security and privacy, a lack of consistent

Wi-Fi connectivity, issues with interoperability and scalability, resistance to change, and a lack of resources and assistance.

Addressing these issues is critical for the effective implementation of IoT in secondary education in developing countries. IoT solutions require stable energy and communications infrastructure, but many emerging countries struggle with outdated infrastructure, poor communication channels, and internet connectivity issues. Financial restriction challenge has direct relationship with the technical challenges, as the high cost of IoT systems will eventually lead to the lack of developed countries' developed infrastructure and reliable Internet; and with security and privacy challenges, as the focusing on providing solutions at the beginning of its life cycle will affect the price of IoT system. Finally, the effective implementation of complicated IoT solutions necessitates talented instructors, staff, and students who are motivated and skilled in their utilization, otherwise equipment may malfunction or not be used.

Future research should concentrate on finding effective solutions for overcoming these barriers, as well as boosting the acceptance and implementation of IoT in education in developing countries.



## References

- Al-Emran, M., Malik, S. I. & Al-Kabi, M. N. (2019) A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges. *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* : 197-209. DOI: [http://dx.doi.org/10.1007/978-3-030-24513-9\\_12](http://dx.doi.org/10.1007/978-3-030-24513-9_12).
- Ali, J., Madni, S. H. H., Jahangeer, M. S. I., & Danish, M. A. A. (2023) IoT Adoption Model for E-Learning in Higher Education Institutes: A Case Study in Saudi Arabia. *Sustainability* 15(12): 9748. DOI : <https://doi.org/10.3390/su15129748>.
- Alharbi, O., Alshammari, Y., Aldosari, M. O. & Albazie, H. A. (2019) The Issues and Advantages of the Use of New Technology in Saudi Education: A Literature Review. *Advances in Social Sciences Research Journal* 6 (8): 290–295. Available from: <https://journals.scholarpublishing.org/index.php/ASSRJ/article/view/6941/4417> [Accessed 1 July 2023].
- Aljaseim, R.S.D.S. (2021) Measuring the Readiness of applying Internet of Thing in the managing education process at high schools in Basra. *International Journal of Advanced Engineering, Management and Science* 7(7): 45-56. DOI: <https://doi.org/10.22161/ijaems.77.8>.
- Altameem, A. (2022) The Challenges of Internet of Things Adoption in Developing Countries: An Overview Based on the Technical Context. *Computer Science & Technology Trends*. DOI: <https://doi.org/10.5121/csit.2022.121910>.
- Arina, A. & Anatolie, A. (2021) Analysis of IoT security issues used in Higher Education Institutions. *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH* 09(05): 2277–2286. DOI: <https://doi.org/10.47191/ijmcr/v9i5.01>.
- Asad, M. M., Naz, A., Shaikh, A., Alrizq, M., Akram, M., & Alghamdi, A. (2022) Investigating the impact of IoT-Based smart laboratories on students' academic performance in higher education. *Universal Access in the Information Society*. DOI: <https://doi.org/10.1007/s10209-022-00944-1>.

Bitdefender (2023) *THE 2023 IOT SECURITY LANDSCAPE REPORT*. Available from: <https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf> [Accessed 16 July 2023].

Bodei, C. & Galletta, L. (2016) The cost of securing IoT communications. *ICTCS* 1720: 163-176. Available at: <https://ceur-ws.org/Vol-1720/full12.pdf> [Accessed 17 July 2023].

Dagnaw, G.A. & Tsige, S.E. (2019) Impact of Internet of Thing in Developing Country: Systematic Review. *Internet of Things and Cloud Computing* 7(3): 65. DOI: <https://doi.org/10.11648/j.iotcc.20190703.12>.

IEA (2022) For the first time in decades, the number of people without access to electricity is set to increase in 2022. Available from: <https://www.iea.org/commentaries/for-the-first-time-in-decades-the-number-of-people-without-access-to-electricity-is-set-to-increase-in-2022> [Accessed 20 July 2023].

Fidai, A., Kwon, H., Buettner, G., Capraro, R. M., Capraro, M. M., Jarvis, C., Benzor, M. & Verma, S. (2019) Internet of Things (IoT) Instructional Devices in STEM Classrooms: Past, Present and Future Directions. *2019 IEEE Frontiers in Education Conference (FIE)*. Available from: <http://dx.doi.org/10.1109/fie43999.2019.9028679> [Accessed 3 July 2023].

Ho-Sam-Sooi, N., Pieters, W. & Kroesen, M. (2021) Investigating the effect of security and privacy on IoT device purchase behaviour. *Computers & Security*, 102: 102132. DOI: <https://doi.org/10.1016/j.cose.2020.102132>.

Khan, S., Singh, R., Khan, S., & Ngah, A. H. (2023) Unearthing the barriers of Internet of Things adoption in food supply chain: A developing country perspective. *Green Technologies and Sustainability* 1(2): 100023. DOI: <https://doi.org/10.1016/j.grets.2023.100023>

Lopez-Vargas, A., Fuentes, M. and Vivar, M. (2020) Challenges and Opportunities of the Internet of Things for Global Development to Achieve the United Nations Sustainable Development Goals. *IEEE Access* 8: 37202-37213. DOI: <http://dx.doi.org/10.1109/ACCESS.2020.2975472>.

Knopp, C. (2019) Privacy Perception in Developing Countries. Available from: <https://doi.org/10.13140/RG.2.2.19821.95209> [Accessed 19 July 2023].

Madni, S. H. H., Ali, J., Husnain, H. A., Masum, M. H., Mustafa, S., Shuja, J., Maray, M. & Hosseini, S. (2022) Factors Influencing the Adoption of IoT for E-Learning in Higher Educational Institutes in Developing Countries. *Frontiers in Psychology*. Available from: <http://dx.doi.org/10.3389/fpsyg.2022.915596> [Accessed 4 July 2023].

Mercan, S., Akkaya, K., Cain, L., & Thomas, J. (2020) Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain. *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*. DOI: <https://doi.org/10.1109/ithings-greencom-cpscom-smartdata-cybermatics50389.2020.00048>.

Mohammadian, H. D. (2019) IoT – a Solution for Educational Management Challenges. *2019 IEEE Global Engineering Education Conference (EDUCON)*. Available from: <http://dx.doi.org/10.1109/educon.2019.8725213> [Accessed 8 July 2023].

Ramson, S.R.J., Vishnu, S. & Shanmugam, M. (2020) Applications of Internet of Things (IoT) – An Overview. *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)* : 92-95. DOI: <https://doi.org/10.1109/ICDCS48716.2020.243556>.

Safdar, M., Hafeez, A., Safdar, G. A. & Abdul Malik, M. (2019) Promises and Challenges of IoT in Education. *09. Pan-Commonwealth Forum 9 (PCF9), 2019*. Available from: <https://oasis.col.org/server/api/core/bitstreams/cd97b020-93ff-4c6c-b145-47589c9f1769/content> [Accessed 6 July 2023].

Saputra, R., Isnaini, N., Adhy, S., Bahtiar, N., Abidin, Z. & Suharto, E. (2020) Factors Influencing Student's Adoption of ELearning in Indonesian Secondary Schools. *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*. Available from: <http://dx.doi.org/10.1109/icicos51170.2020.9299109> [Accessed 6 July 2023].

Sreekantha, D. K., Koujalagi, A., Girish, T. M. & Sairam, K. V. S. S. S. S. (2020) Internet of Things (IoT) Enabling Technologies and Applications—A Study. *Advances in Intelligent Systems and Computing* : 1425-1442. Available from: [http://dx.doi.org/10.1007/978-981-15-3514-7\\_107](http://dx.doi.org/10.1007/978-981-15-3514-7_107) [Accessed 5 July 2023].

- Sharma, M., Joshi, S., Kannan, D., Govindan, K., Singh, R., & Purohit, H. C. (2020) Internet of Things (IoT) Adoption Barriers of Smart Cities' Waste management: an Indian Context. *Journal of Cleaner Production* 270: 122047. DOI: <https://doi.org/10.1016/j.jclepro.2020.122047>.
- Suduc, A.-M., Bizoi, M. & Gorghiu, G. (2018) A Survey on IoT in Education. *Revista Romaneasca pentru Educatie Multidimensionala* 10 (3): 103-111. Available from: <http://dx.doi.org/10.18662/rrem/66> [Accessed 8 July 2023].
- Sultana, N. & Tamanna, M. (2021) Exploring the benefits and challenges of Internet of Things (IoT) during Covid-19: a case study of Bangladesh. *Discover Internet of Things* 1(1). DOI: <https://doi.org/10.1007/s43926-021-00020-9>.
- Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020) IoT Privacy and Security: Challenges and Solutions. *Applied Sciences* 10(12): 4102. DOI: <https://doi.org/10.3390/app10124102>.
- Van Deursen, A. J. A. M., Van Der Zeeuw, A., De Boer, P., Jansen, G., & Van Rompay, T. (2021) Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage. *Information, Communication & Society* 24(2): 258-276. DOI: <https://doi.org/10.1080/1369118X.2019.1646777>.
- Vinayachandra & Krishna Prasad, K. (2020) Application of IoT in the Development of Intelligent Education System – A Thematic Literature Review. *International Journal of Management, Technology, and Social Sciences* 5 (1): 124-146. Available from: <https://doi.org/10.5281/zenodo.3775850> [Accessed 7 July 2023].
- Yeh, J. H.-J., Bartholio, C., Shackleton, E., Costello, L., Perera, M., Yeh, K. & Yeh, C. (2020) Environmentally Embedded Internet-of-Things for Secondary and Higher Education. *2020 3rd International Conference on Information and Computer Technologies (ICICT)*. Available from: <http://dx.doi.org/10.1109/iciict50521.2020.00092> [Accessed 5 July 2023].
- Zhao, B., Ji, S., Lee, W.-H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L., & Beyah, R. (2022) A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Transactions on Dependable and Secure Computing* 19(3): 1826-1840. DOI: <https://doi.org/10.1109/TDSC.2020.3037908>.