Research Journal of Education, Teaching and Curriculum Studies
Vol. 2 No. 1 (2024): ISSN (Online): 2958-8626
DOI: https://doi.org/10.58721/rjetcs.v2i1.463
Internet of Things security and privacy in Higher Education Institutions in Developing Countries

Internet of Things security and privacy in Higher Education Institutions in Developing Countries

Ruth Nthenya Wambua
United States International University–Africa, Kenya

Article History
Received: 2024-01-07
Revised: 2024-02-29
Accepted: 2024-03-12
Published: 2024-03-17

Keywords
Developing countries
Education
Internet of Things
Privacy
Security

How to cite:

Wambua, R. N. (2024). Internet of Things security and privacy in Higher Education Institutions in Developing Countries. *Research Journal of Education, Teaching and Curriculum Studies,* 2(1), 1- 7.

Abstract
Technological breakthroughs like the Internet of Things (IoT) technology have tremendously impacted today's world and have led to changes in many spheres of life, including education. With the pervasiveness of IoT devices, learning and academic institutions are already integrating IoT into educational activities. Nonetheless, despite the numerous technological advancements and the demand for high-quality education for everyone, IoT's adoption and impact on education are still in their infancy. On the other hand, with the number of connected items having reached billions and still growing, there is cause for concern regarding the Internet of Things' potential for serious privacy violations, considering it is one of the most potent technologies for creating, modifying, and sharing data. Therefore, to emphasise the thematic areas and prospects for additional research related to the security and privacy of the Internet of Things (IoT) and within Higher Education Institutions (HEIs), this study explores the security and privacy of IoT in the context of HEIs within developing countries.

Introduction

The adoption of IoT in education has a favourable impact on teaching excellence, access to resources, connectivity between universities, and learning excellence (Mircea et al., 2021). Further, most people are now much more technically connected than before, with a majority being owners of smartphones and devices that connect to the internet and to each other (Gómez et al., 2013).

Considering that educational technology continues to progress alongside technological advances, ensuring and enforcing quality and equitable education is necessary. Technology integration, including IoT in education, should remain a conscious move for sustainable education for all (Bal et al., 2021 Wambua and Oboko, 2015). Consequently, enforcing the United Nations Sustainable Development Goals (SDGs) targets on education.

The adoption of IoT in education is beneficial in that it results in a positive influence on excellence in teaching, on additional resources, on intra- and extra-university connectivity, and on excellence in

learning (Mircea et al., 2021). Moreover, students with disabilities are exposed to more accessible learning environments through wireless assistive technology and IoT. On the other hand, technological challenges threaten IoT in education. For instance, limited memory, bandwidth, and energy would limit the technological demands of IoT on education. In addition, a case where a lot of data must be communicated to students who need more resources would lead to communication overhead. Furthermore, the heterogeneous hardware encompassing the IoT landscape results in varied educational outputs (Bright, 2021).

For effectiveness, IoT teaching methods should include a practical component and incorporate hardware and software designs that would significantly reduce the teaching workload and improve data management (Wang, 2015). In the education setup, the Internet of Things includes four core technologies, namely RFID, sensor, intelligence, and nanotechnology, embodied in classroom teaching, extracurricular learning, and educational management (Wang N and Wang J, 2018).

IoT's perceived usefulness depends on how well IoT respects the privacy and choices of the users. It is therefore critical to understand that rights of privacy and respect for user privacy are important in ensuring users' confidence in IoT (Weber, 2015. On the other hand, it is important to enforce security measures across all the integrated technologies within an IoT ecosystem (Andrea et al., 2015). Therefore, the following discusses the privacy and security concerns around IoT in HEIs in developing countries.

Privacy concerns around IoT

The education setup includes varied users, data, and information, and the integration of IoT results in the interconnection of people and devices (Tawalbeh et al., 2020. IoT devices collect a large amount of data and information and carry a big potential of privacy threats, especially regarding data use and access. The ever-present intelligence-integrated artefacts that allow the sampling and distribution of information in any place bring about concerns about privacy in IoT since this means that surveillance and tracking of people can occur at any location (Tawalbeh et al., 2020; Weber, 2015).

In addition to IoT devices, users surround themselves with sensor-equipped devices that often passively collect data concerning users' daily activities. With these devices connected to the internet and sharing data between various devices, more concerns about privacy arise. For instance, how is the data collected, where is it stored after it is collected, and how is it used? Other questions may arise, including who owns and accesses the data (Foltz & Foltz, 2020).

Concerns of privacy in IoT are multifaceted and include technical, regulatory, and social aspects. Privacy challenges could also be categorised into privacy leakage, data storage and processing availability, and trustworthy and dependable control (Padyab & Ståhlbröst, 2018). In light of technological advances, if poorly thought out, these concerns would have a detrimental effect on education (Bright, 2021).

Security concerns around IoT

The Internet of Things in Higher Education Institutions and elsewhere integrates existing network infrastructure and network technologies (Weber, 2015). This means that the network security challenges and threats of every network technology used will, by default, be passed onto the IoT system using the technologies. In addition, additional security threats are likely to arise from the

existence and collaboration of various technologies and the open standards and protocols created for IoT (Andrea et al., 2015).

The devices on IoT are controlled and monitored, and they even communicate with one another over the internet. Furthermore, the amount of data generated from IoT makes them vulnerable to security attacks. With multiple devices converging to form IoT, there is a risk that any of the devices in this kind of environment could be used to launch an attack on the environment , in this case, the education environment.

Security concerns raised on IoT include confidentiality, which refers to the data security services that ensure only authorised users can access the data. Data collected from IoT may reveal sensitive data regarding individuals. For instance, on the Internet of Medical Things (IoMT), details about an individual's medical information may be received. Attackers can use passive attacks to dissolve or gather information about an individual (Hasan et al., 2021). This is where an attacker can intercept communication in IoT to use it maliciously (Papaioannou et al., 2020). Secondly, there is integrity, which ensures that information being exchanged between devices is original and not modified or fabricated by hackers. In IoT, various factors may affect data originality. For instance, servers may crash or fail server nodes. The man-in-the-middle attack is an attack that can jeopardise the integrity of data in IoT since an attacker will interpose communication between two devices and may modify the data without being noticed (Deep et al., 2020). The malicious node injection is another concern regarding the integrity of data in IoT (Papaioannou et al., 2020). In this attack, the attacker will inject a malicious node between two or more nodes. These nodes can then modify the data and pass the wrong information to other nodes. Attackers can use more than one node to perform this kind of attack. It is classified as the most dangerous attack since it stops the service and modifies data.

In addition, there is availability, whereby data and services are accessible to the users whenever required. The main goal is to ensure that services are not denied to authorised users. The entire system, together with the IoT devices, should be available, including the properties of scalability and survivability Papaioannou et al., 2020). Denial of service attacks is one-way services can be made unavailable. In this attack, the attacker bombards an IoT network with more traffic data than it can handle, making it impossible for other users to use the network (Mena et al., 2018). The distributed denial of service attacks may also be used by attackers on affected IoT networks, which affects all network users, thus blocking legitimate users from accessing their networks. This surrenders access to the system to the attackers, which may allow access to databases and sensitive data to unauthorised people in the long run. Consequently, it is messing up the education processes within such an environment.

Methodology

This study employs qualitative research methodology to emphasise the thematic areas and prospects for additional research related to the security and privacy of the Internet of Things (IoT) and within Higher Education Institutions (HEIs). In this case, the methodology entails reviewing and analysing related literature on privacy and security around IoT in the context of HEIs.

Discussion

In the context of IoT security and privacy in HEIs in developing countries, the following discussion discusses presented solutions to improve IoT privacy and security and the noted research gaps.

Presented solutions to improve the privacy and security of IoT

Education is a key pillar in an economy, and integrating IoT should ensure that key security and privacy concerns are considered for diverse user and information management (Habib et al., 2021). Most of the privacy concerns raised on IoT in education are related to data collection, access, storage, ownership, and access to the data. There is no doubt that IoT brings implications for institutions and social and cultural environments. With the risk of privacy loss, establishing a framework for IoT governance to address data privacy challenges is critical (Weber, 2015). Further, dedicated policies and legislation to guide and govern education for students with disabilities and regulatory mechanisms to address evolving IoT security risks will go a long way (Brass & Sowell, 2021).

In addition to the development of a framework, a few technologies have been developed to achieve the privacy goal. They are referred to as Privacy-Enhancing Technologies (PETs). These technologies include virtual private networks, transport security layer, DNS security extension, onion routing, and private information retrieval. The objectives of these technologies are to ensure the security of communication. In addition, PETs also preserve user identity when other parties do not need this information (Weber, 2015).

Further to the PETs, privacy by design (PbD) is an important protection strategy. The approach stipulates seven principles that should be adhered to in technology design. These are proactive approaches to privacy, privacy as the default setting, privacy embedded in technology design, full functionality, end-to-end security spanning the lifecycle of a device, visibility and transparency that will allow users to verify privacy claims and respect for privacy (Weber, 2015). Blockchain technology is also another way that has been proposed and is still being explored as a way of enhancing privacy and security in IoT (Skwarek, 2017).

On security, Blockchain is a technology that stores and transmits transparent and secure information, operates without a central control body, and could help resolve security issues in IoT. Blockchain is a decentralised network through which everyone engages with the other party in one way or the other. It is a database that contains the history of all exchanges carried out between users and creators. Because the database is secure and distributed, it is shared by its various users without intermediaries, allowing everyone to check the validity of the chain (Bagheri & Movahed, 2016). Therefore, to help secure the IoT and reduce barriers to adoption, blockchain technology on IoT in education infrastructure is recommended.

Identified research gaps within IoT privacy and security

Among the outstanding issues identified regarding IoT privacy concerns is the legal framework necessary for ensuring privacy in IoT. Research needs to be carried out involving both legal practitioners and computer science practitioners to ensure that the legal framework does not obstruct the implementation of IoT in HEIs in developing countries; rather, it should be a facilitative framework that will protect users and academia by respecting their rights to privacy.

Further studies should be conducted to design a simplified and usable privacy notice in IoT devices. This will enhance transparency that is part of the PbDs. These studies should also consider usable security, privacy, and human-computer interactions concepts (Al-Ameen et al., 2021).

In addition, a study should be conducted to identify the level of user awareness of IoT privacy risks. This is necessitated by the privacy paradox, which shows that user behaviour does not match user

expectations. Finally, a study needs to be conducted whose output will be a framework for training users on privacy issues in IoT in HEIs in developing countries.

On the other hand, blockchain is a new technology that has the potential to resolve some of the security and privacy concerns we have in IoT. Studies should be conducted to check how this can be implemented to secure IoT.

Conclusion

Technological advancements in education and the integration of the Internet of Things (IoT) in HEIs fortify the development of intelligent systems for diverse information management. Dedicated policies, legislation, and frameworks to guide and govern education will go a long way.

On the other hand, the enormous attack surface presented by the billions of interconnected IoT devices increases the vulnerability of its infrastructure. Therefore, to secure these IoT devices, manufacturers should incorporate security management applications to manage provisioning, device configuration, security measure configurations, security policies, security event monitoring responses, and patch management, thus enhancing their confidentiality, integrity, and availability.

In addition, blockchain technology offers complete data storage, reliable information interaction, trusted node authentication, and other security features for IoT infrastructure. The technology uses asymmetric encryption to ensure data security and privacy by implementing all transactions anonymously with the trusting mechanism. Hence, enforcing good integration of IoT in HEIs in developing countries. A detailed categorisation of the privacy and security concerns of IoTs in HEIs in developing countries is recommended for further study.

References

Al-Ameen, M. N., Chauhan, A., Ahsan, M. A. M., & Kocabas, H. (2021). A look into user's privacy perceptions and data practices of IoT devices. *Information & Computer Security*, *29*(4), 573–588. https://doi.org/10.1108/ICS-08-2020-0134

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180–187. https://doi.org/10.1109/ISCC.2015.7405513

Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. In *Journal of Network and Computer Applications* (Vol. 49, pp. 112–127). Academic Press. https://doi.org/10.1016/j.jnca.2014.11.011

Bagheri, M., & Movahed, S. H. (2016). The Effect of the Internet of Things (IoT) on Education Business Model. *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, 435–441. https://doi.org/10.1109/SITIS.2016.74

Bal, A., Waitoller, F. R., Mawene, D., & Gorham, A. (2021). Culture, context, and disability: A systematic literature review of cultural-historical activity theory-based studies on the teaching and learning of students with disabilities. *Review of Education, Pedagogy, and Cultural Studies*, *43*(4), 293–337. https://doi.org/10.1080/10714413.2020.1829312

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation and Governance*, *15*(4), 1092–1110. https://doi.org/10.1111/rego.12343

Bright, D. (2021). An integrative review of the potential of wireless assistive technologies and internet of things (IoT) to improve accessibility to education for students with disabilities. *Assistive Technology*, 1–8. https://doi.org/10.1080/10400435.2021.1956639

Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Bashir, A. K. (2020). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.3935

Foltz, C. B., & Foltz, L. (2020). Mobile users' information privacy concerns instrument and IoT. *Information & Computer Security*, *28*(3), 359–371. https://doi.org/10.1108/ICS-07-2019-0090

Gómez, J., Huete, J. F., Hoyos, O., Perez, L., & Grigori, D. (2013). Interaction System based on Internet of Things as Support for Education. *Procedia Computer Science*, *21*, 132–139. https://doi.org/10.1016/j.procs.2013.09.019

Habib, K., Kai, E. E. T., Saad, M. H. M., Hussain, A., Ayob, A., & Ahmad, A. S. S. (2021). Internet of Things (IoT) Enhanced Educational Toolkit for Teaching Learning of Science, Technology, Engineering and Mathematics (STEM). *2021 IEEE 11th International Conference on System Engineering and Technology, ICSET 2021 - Proceedings*, 194–199. https://doi.org/10.1109/ICSET53708.2021.9612579

Hasan, M. K., Ghazel, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., Abdel-Khalek, S., & Alkhassawneh, H. M. (2021). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. In *IET Communications*. John Wiley and Sons Inc. https://doi.org/10.1049/cmu2.12301

Mena, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. In *Information Security Journal* (Vol. 27, Issue 3, pp. 162–182). Taylor and Francis Inc. https://doi.org/10.1080/19393555.2018.1458258

Mircea, M., Stoica, M., & Ghilic-Micu, B. (2021). Investigating the Impact of the Internet of Things in Higher Education Environment. *IEEE Access*, *9*, 33396–33409. https://doi.org/10.1109/ACCESS.2021.3060964

Mohammad, Z., Qattam, T. A., & Saleh, K. (2019). Security Weaknesses and Attacks on the Internet of Things Applications. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 431–436. https://doi.org/10.1109/JEEIT.2019.8717411

Padyab, A., & Ståhlbröst, A. (2018). Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. *Digital Policy, Regulation and Governance*, *20*(6), 528–544. https://doi.org/10.1108/DPRG-05-2018-0023

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4049

Skwarek, V. (2017). Blockchains as security-enabler for industrial IoT-applications. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 301–311. https://doi.org/10.1108/APJIE-12-2017-035

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Wambua, R. N., & Oboko, R. (2015). ELearning for persons with visual disabilities: Case of low vision. In *Handbook of Research on Educational Technology Integration and Active Learning*. https://doi.org/10.4018/978-1-4666-8363-1.ch012

Wambua, R. N., & Ondiek, C. O. (2022). Implications of Internet of Things (IoT) on the Education for students with disabilities: A Systematic Literature Review. *International Journal of Research Publications*, *102*(1). https://doi.org/10.47119/IJRP1001021620223320

Wang, J. (2015). The design of teaching management system in universities based on biometrics identification and the Internet of Things technology. *2015 10th International Conference on Computer Science & Education (ICCSE)*, 979–982. https://doi.org/10.1109/ICCSE.2015.7250393

Wang, N., & Wang, J. (2018). Research and Practice on Innovative Methods of Ideological and Political Education for College Students Based on Internet of Things + Technologies*. *Educational Sciences: Theory & Practice*. https://doi.org/10.12738/estp.2018.5.137

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law and Security Review*, *31*(5), 618–627. https://doi.org/10.1016/j.clsr.2015.07.002