Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 1, February 2026, pp. 595~603
ISSN: 2302-9285, DOI: 10.11591/eei.v15i1.10464

Security challenges in the internet of things for higher education: a study of vulnerabilities and emerging solutions

Kamal Elhattab[1], Driss Naji[2], Abdelouahed Ait Ider[3], Abdelali Joumad[4], Abdelkbir Ouisaadane[5], Karim Abouelmehdi[6]

[1]Department of Computer Science, EST of Sidi Bennour, Chouaib Doukkali University, El Jadida, Morocco
[2]TIAD Laboratory, Department Computer of Science, Faculty of Science and Technique, Sultan Moulay Slimane University, Beni-Mellal, Morocco
[3]ISIMA Laboratory, Department Computer of Science, Faculty of Polydisciplinary, Ibnou Zohr University, Taroudant, Morocco
[4]LAROSERI Laboratory, Department Computer of Science, Faculty of Science, Chouaib Doukkali University, El Jadida, Morocco
[5]LIMATI Laboratory, Department Computer of Science, Faculty of Science and Technique, Sultan Moulay Slimane University, Beni-Mellal, Morocco
[6]ELITES Laboratory, Department Computer of Science, Faculty of Science, Chouaib Doukkali University, El Jadida, Morocco

Article Info

Article history:

Received Apr 12, 2025
Revised Oct 7, 2025
Accepted Dec 6, 2025

Keywords:

Artificial intelligence
Challenges
Higher education
Internet of things
Security

ABSTRACT

The growing use of internet of things (IoT) technologies in higher education is transforming how institutions manage infrastructure, deliver teaching, and engage with students. While these advancements offer considerable benefits, they also introduce significant security risks. Common threats include weak access controls, insufficient data protection, outdated software, exposure to denial-of-service (DoS) attacks, and lack of physical safeguards for connected devices. This study provides a comprehensive review of these vulnerabilities within academic environments and proposes a security framework adapted to the specific operational and technical realities of universities. Unlike generic approaches, this research focuses on the unique challenges of higher education, such as decentralized information technology (IT) structures, limited resources, and diverse user groups. The main contribution lies in identifying and evaluating security measures that are both effective and applicable in academic contexts. These include encryption methods, identity verification techniques, secure update mechanisms, and intelligent systems for detecting abnormal behavior. The analysis is supported by case examples from real institutions, illustrating both successes and limitations of current practices. This work aims to guide educational institutions in improving the resilience of their IoT systems. It also outlines areas for future research, particularly in the development of lightweight and scalable security solutions suited to the evolving needs of smart learning environments.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Kamal Elhattab
Department of Computer Science, EST of Sidi Bennour, Chouaib Doukkali University
El Jadida, Morocco
Email: kamal.elhattab@gmail.com

1. INTRODUCTION

Over the last few years, the internet of things (IoT) has increasingly touched all the different sectors or industries that it drives, among which is higher education [1]-[5]. Universities and colleges are now beginning to adopt IoT in campus functioning, resource allocation, and eventually the learning experience. Smart devices that include environmental sensors, digital attendance, and connected classroom systems are

now employed in administrative and pedagogical innovations. Notwithstanding the advantages, the proliferation of IoT in the academic environment brings huge added cybersecurity risks. Unlike information technology (IT) systems, IoT networks consist of a multitude of different and often poorly secured devices. This complexity is further exacerbated in higher education institutions by open network policies, a variety of user profiles, and a combination of personal and institutional devices. Hence, these conditions pose various threats such as unauthorized access, denial-of-service (DoS) attacks, data breaches, and physical tampering on devices. Earlier studies have elaborated on general vulnerabilities to IoT, proposing some solutions for industrial and urban contexts, but academic institutions have not yet been covered in their specific security challenges. Most of the studies are mostly on technical solutions without regard to the different operational and organizational characteristics of universities, such as decentralized management, open access networks, and, finally, the coexistence of educational infrastructure and research. Thus, this space in the literature opens up an argument around the focused look at IoT security in higher education. This paper seeks to fill this gap by assessing the most important vulnerabilities that characterize academic IoT spaces and the expected modern approaches to the requirements imposed by this sector. It has three main contributions; first, it proposes an elaborate classification of typical security vulnerabilities in IoT devices within education institutions second, it establishes modern solutions in other domains such as health care and smart cities, converses the relevance of such solutions in educational environments, and, third, it offers practical recommendations contextualized to the bounds of universities, inclusive of limited budgets, technical complexity, and acceptance by the different stakeholders. To guide the reader throughout the analysis, the rest of the paper is organized as follows: section 2 deals with the method, section 3 presents major findings and proposed solutions, and section 4 provides a conclusion with future directions and implications for policy and practice.

2. METHOD

This study adopts a hybrid methodological approach that combines a systematic literature review with a comparative analysis of security mechanisms applied in IoT systems. The objective is to identify, categorize, and evaluate the most relevant vulnerabilities and corresponding mitigation strategies suitable for higher education environments.

2.1. Data collection and selection criteria

A structured search strategy was applied to gather relevant academic and technical publications focused on IoT security in higher education. The databases consulted include IEEE Xplore, ScienceDirect, and Google Scholar (see Table 1). The inclusion criteria were based on the relevance of content, quality of source, publication date, and empirical evidence (see Table 2). This process resulted in the selection of a refined corpus of publications that formed the basis for the vulnerability analysis and solution evaluation.

Table 1. Article selection criteria

Database	Article	Type
IEEE Xplore	[6]-[15]	Conference
ScienceDirect	[16]-[33]	Article
Google Scholar	[9], [34]-[50]	Article and Conference

Table 2. Article selection criteria

Criterion	Description
Relevance	Direct focus on IoT security within academic or educational contexts
Publication source	Indexed in recognized scientific journals or conferences
Recency	Published within the last 5 years to ensure technological relevance
Empirical content	Inclusion of experimental data, case studies, or applied methods
Technical contribution	Clear focus on cybersecurity approaches, frameworks, or evaluations

2.2. Vulnerability identification and classification

Based on the selected literature, vulnerabilities were identified and grouped into five major categories, each representing a distinct type of risk observed in IoT deployments within academic institutions. The classification supports structured analysis and helps prioritize areas requiring urgent attention (see Table 3). These categories guided the next phase of analysis, where mitigation strategies were matched to each vulnerability type.

Table 3. Classification of key IoT vulnerabilities in higher education

Vulnerability category	Description
Authentication and access control	Weak passwords, lack of multi-factor authentication (MFA), and poor privilege separation
Data confidentiality	Inadequate or absent encryption mechanisms for personal or sensitive data
Software/firmware weaknesses	Lack of timely updates or patch management and use of outdated firmware
Denial of service (DoS)	Attacks disrupting system availability through resource saturation
Physical security risks	Unauthorized physical access or tampering with connected IoT devices

2.3. Comparative analysis of mitigation strategies

To identify applicable solutions, a comparative analysis was conducted on techniques implemented in other domains, such as healthcare, smart cities, and industrial IoT. Only those with high adaptability to educational environments were retained (see Table 4). Each of these methods was assessed for technical feasibility, cost-effectiveness, ease of deployment, and alignment with the IT capacity of higher education institutions.

Table 4. Overview of emerging security solutions

Security solution	Key mechanism and application
End-to-end encryption (E2EE)	Ensures data confidentiality during transmission using advanced encryption standard (AES) and transport layer security (TLS)
MFA	Requires multiple credentials for user/device verification
Role-based access control (RBAC)	Restricts access based on predefined user roles
Blockchain integration	Ensures data integrity and traceability through immutable logs
AI-based anomaly detection	Uses machine learning to detect unusual device behavior in real time
Secure firmware updates	Implements encrypted and validated update processes

2.4. Validation through case studies

The practical relevance of the identified solutions was validated through documented case studies from universities that have implemented advanced IoT security frameworks. The objective was to examine real-world adoption, outcomes, and limitations (see Table 5). The analysis of these cases demonstrated the positive impact of proactive security policies but also highlighted ongoing challenges such as integration complexity, maintenance overhead, and limited awareness among staff.

Table 5. Institutional case study examples

Institution	Solution implemented	Observed impact
University A	E2EE	Improved protection of sensitive student information
University B	MFA	Reduced incidence of unauthorized system access
University C	Blockchain for IoT logging	Enhanced traceability and accountability in device usage
University D	AI for anomaly detection	Early detection of potential threats in connected systems
University E	Automated firmware updates	Minimized vulnerabilities from outdated device software

3. RESULTS AND DISCUSSION

This section presents the main findings of the study, focusing on the primary security challenges in higher education IoT environments and the effectiveness of emerging countermeasures. The results combine literature insights with institutional experiences and provide a discussion of practical implications, barriers, and future considerations.

3.1. Identified internet of things security challenges in academic environments

According to the study, institutions of higher education face serious security issues vis-à-vis deploying IoT systems. These vulnerabilities violate confidentiality, integrity, and availability, all of which pertain to campus infrastructure and data. Authentication and access control, in fact, are found lacking in numerous environments. The devices apparently operate with weak credential policies, such as default or shared passwords, and without solid identity verification frameworks. This basically increases the threat of unauthorized access, especially in open and decentralized university networks. Data confidentiality, another cardinal issue, is jeopardized since sensitive academic and personal information is usually transmitted or stored without encryption. On the other hand, weak or improperly implemented security layers expose this data to interception, unauthorized access, and leakage. Software and firmware vulnerabilities also exist in abundance. Most institutions struggle with IoT device updates, leaving their systems vulnerable to exploits

already patched in other sectors for a long time. In some cases, outdated firmware persists simply because of compatibility and cost considerations. Another significant threat is DoS attacks. IoT networks are either flooded with malicious traffic or the weaknesses of the system are exploited to interrupt critical academic services and business models. Thirdly, the physical security of devices is often neglected. IoT sensors and nodes located in open-access facilities such as lecture halls and laboratories are at risk of tampering by malicious actors to disrupt operations or steal data directly from the hardware. These security challenges are summarized in the Table 6.

Table 6. Summary of observed security challenges

Challenge category	Description
Authentication and access control	Weak credential policies, default passwords, and insufficient identity management
Data confidentiality	Lack of encryption for sensitive academic and personal data
Firmware and software vulnerabilities	Unpatched devices, delayed updates, and use of insecure legacy firmware
DoS attacks	Disruption of services due to traffic flooding or resource exhaustion
Physical tampering	Lack of physical safeguards allowing unauthorized manipulation or theft

3.2. Evaluation of emerging security solutions

Different security mechanisms have been analyzed worldwide for their applicability in an academic IoT ecosystem response to these vulnerabilities. Effective data conveyed between devices will remain confidential and protected from interception through E2EE (for instance, using the AES and TLS protocols). However, implementation might add latency and require more computational power. MFA and RBAC are enhancing user verification mechanisms and providing better access to specific resources. Through this, the chances of unauthorized access are lessened, especially related to sensitive academic systems. With all these benefits, however, institutions face challenges in the uptake of MFA within the faculty, staff, and student body due to usability concerns. Above all, blockchain has proved its worth as a potential technology to manage identity and integrity of transactions in an IoT network. Its decentralized structure would guarantee the immutability of data and its ability to produce verifiable audit trails between devices. But because of the economic and complex nature, it could limit deployment on a large scale for an institutional resource. The artificial intelligence (AI)-based anomaly detection has proactive monitoring potential as it can sense abnormal behavior or threat occurrence in real time with its correlating response. It would, however, definitely improve the response to the threat, but it requires high-quality training data for performance and may flag some false positives if mis calibrated. Finally, secure firmware update mechanisms will keep the system intact. Updating may be automated and encrypted to shield devices from known exploitable vulnerabilities, but the real technical challenge to IT departments is how to best ensure compatibility and distribution over the different IoT devices. The Table 7 compares these emerging solutions.

Table 7. Comparative evaluation of security approaches

Security approach	Addressed vulnerability	Strengths	Limitations
E2EE (AES, TLS)	Data confidentiality	Ensures secure data exchange	Requires computational resources; potential latency
MFA and RBAC	Authentication and access control	Strengthens login and authorization	Usability and adoption challenges among users
Blockchain	Identity and transaction integrity	Immutable audit trail; tamper-proof	High implementation cost; scalability concerns
AI-based anomaly detection	Behavior-based threat detection	Real-time threat identification	False positives; needs training data
Secure firmware updates	Software vulnerabilities	Reduces exposure to known exploits	Device compatibility and update distribution complexity

3.3. Institutional case insights

Realistically, the implementation of such security measures across many educational institutions holds significant real-life examples. For instance, by deploying blockchain technology within the smart building structure, Stanford University could secure sensor readings. Such security creates open and tamper-proof logging for device interaction, making the entire system more trustworthy. An example would be the installation of anomaly detection systems based on AI in research laboratories at the Massachusetts Institute of Technology (MIT). They allow real-time detection of suspicious activities, therefore significantly decreasing the chances of intrusions going unnoticed while facilitating faster incident responses. MFA was introduced at those institutions for access to learning platforms and administration tools. The strategy has

reduced successful credential attacks, especially among remote users. However, the success of these implementations has not reached strategic scale. They continue to constitute barriers to widespread adoption: financial constraints, technical integration problems, and low user training. Typically, universities would set up these isolated little projects in one department rather than institution-wide, thanks to governance and budget fragmentation.

3.4. Critical discussion

The evaluation shows that a gap clearly exists between the presence of an effective security solution and its actual application in higher education. Many IoT devices that find their place in such environments were not originally designed to have security integrated; instead, retrofitting becomes next to impossible. And without a modular architecture, there is great difficulty in attaching encryption or authentication modules after deployment. In other aspects, decentralized control of IT infrastructure by most universities poses challenges for a uniform application of security protocols. Each department may adopt different tools or standards, as such causing differences and vulnerabilities in that institution. Investment in advanced or complex solutions like blockchain or AI is further hindered by barriers/errors such as cost and unavailability of trained personnel. While security awareness among administrators is slowly but gradually growing, enforcement of policies on institutional cybersecurity is inconsistent. In some instances, it seems that declared priorities do not match resource allocation for long-term security planning. Most of the chances of reducing such risks rest within a proactive and security-by-design approach towards the procurement and deployment of IoT systems. Security mechanisms are instead required to be incorporated from the onset of system development rather than appending them once they have already been exposed to vulnerabilities. Furthermore, secure and automated update frameworks should ensure the emergence of new threats. Also potentially involved are cross-institutional cooperation and a regulatory framework for shared guidelines and security standards across universities to improve alignment, reduce duplication of effort, and elevate baseline security across the sector.

3.5. Implications for practice and research

This paper presents a number of practical recommendations. First, institutions should preferentially consider native security features when looking at IoT solutions. The procurement processes should consider the security compliance of functions, where possible; universities should adopt centralized and functional security frameworks in federated IT environments. Staff training and awareness are equally crucial. Campaigns should include training to educate both the IT team and end users on the security risks and train them to use the advanced technologies, such as anomaly detection platforms and identity management systems. In addition, the institutions should invest in automated firmware management systems to cut back on manual errors and guarantee timely updates. Future studies in the field would include the lightweight security protocols that would be able to work with the limitations of low-power IoT devices used in academia. The development of further research may well increase adaptive access control systems to reflect the dynamic behavior of students and staff. Governance models that would address the institutional inertia toward adopting the best of cybersecurity practices should be further examined. To the core, modern security measures can be very important and possible to integrate with the academic IoT scenario. With a harmonized policy, technical foresight, and investment in a strategic program, universities will be able to benefit immensely in the area of improving how resilient their interconnected infrastructures are.

4. CONCLUSION

While offering many positive changes such as operational efficiency, greater student engagement, and modernization of academic infrastructure, it also poses various security risks with changing dimensions and complex nature. The findings of the study revealed that the main issues revolve around weak authentication practices, insufficient data protection, outdated firmware, vulnerability to DoS attacks, and poor physical security of IoT devices. These threats can be addressed using possibilities offered by few emerging technologies, including E2EE, advanced authentication protocols, blockchain for identity management, and AI-based anomaly detection. Case studies and industry-specific adaptations in the thesis show that it is best to integrate security solutions during the design phase together with proactive update management to reduce exposure to threats. Yet, several hurdles remain, including cost limitations, some degree of training for users, and the de facto decentralized IT management in academic institutes. Together, these slow down the process of bringing advanced security frameworks on board and lead to inconsistent implementations of best practices across departments. Future work should continue to explore the possibilities of customization for interoperable security systems according to the varied environments found in educational institutions. It is also imperative to consider how quantum technologies and lightweight cryptographic methods could be employed, particularly as IoT devices become even more widespread and

complex. A unified approach is to be taken by the government, academia, and the industry to secure scalable, sustainable, and standardized security strategies toward smart learning environments.

ACKNOWLEDGMENTS

We express our sincere gratitude to the Chouaib Doukkali University College for the invaluable scientific support it extended to us. We salute the staff of the journal for their criticism, which contributed greatly to the development of this paper.

FUNDING INFORMATION

This work was supported by the ELITES laboratory, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco. The authors also acknowledge the financial support from the TIAD Laboratory, Faculty of Science and Technology, Sultan Moulay Slimane University, Beni-Mellal, Morocco, and the ISIMA laboratory, Polydisciplinary Faculty, Ibnou Zohr University, Taroudant, Morocco. No other financial support was received for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Kamal Elhattab	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Driss Naji	✓	✓	✓						✓					✓
Abdelouahed Ait Ider		✓	✓		✓				✓					
Abdelali Joumad	✓			✓				✓		✓				
Abdelkbir Ouisaadane	✓	✓			✓	✓	✓		✓	✓				
Karim Abouelmehdi						✓				✓		✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

The research was conducted in accordance with relevant ethical standards and regulations.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] E. Saraswat, N. Maurya, S. Mishra, and R. Sharma, "The Role of IoT in Transforming Education: Opportunities, Challenges, and Future Directions for Smart Education Systems," in *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, 2024, pp. 578-583, doi: 10.1109/IC3I61595.2024.10828984.

[2] H. Mattiello, F. D. Mohammadian, and D. Assante, "IoT-education policies on national and international level regarding best practices in German SMEs," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, Porto, Portugal, 2020, pp.

1848-1857, doi: 10.1109/EDUCON45650.2020.9125148.
[3] T. M. Okediran, O. R. Vincent, A. O. Agbeyangi, A. Abayomi-Alli, and O. J. Adeniran, "Solving the House Numbering Problem in Nigeria: Internet of Things (IoT) As An Emerging Solution," in *2022 5th Information Technology for Education and Development (ITED)*, Abuja, Nigeria, 2022, pp. 1-5, doi: 10.1109/ITED56637.2022.10051271.
[4] D. Tsipianitis, M. Filippou, K. Lavidas, and V. Komis, "Real-time Monitoring of IoT-based Educational Aquatic Microecosystem," *Procedia Computer Science*, vol. 257, pp. 801-808, 2025, doi: 10.1016/j.procs.2025.03.103.
[5] R. Tahsin, S. B. A. Rantu, M. Rahman, S. Salman, and Md. R. Karim, "Towards the adoption of AI, IoT, and Blockchain technologies in Bangladesh's maritime industry: Challenges and insights," *Results in Engineering*, vol. 25, pp. 1-14, Mar. 2025, doi: 10.1016/j.rineng.2024.103825.
[6] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.
[7] A. Qasim, G. A. E. Refae, S. Eletter, and A. R. Al-Chahadah, "Harnessing The Power of the Internet of Things (IoT) to Achieve an Agile Business Education Model: A Visionary Paper," in *2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Gandia, Spain, 2021, pp. 1-4, doi: 10.1109/IOTSMS53705.2021.9704939.
[8] D. Sharma, P. Anawade, S. Gahane, and Y. Patil, "Security and Privacy Considerations in IoT-Based Livestock Monitoring Systems," in *2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET)*, Nagpur, India, 2024, pp. 1-6, doi: 10.1109/ICICET59348.2024.10616284.
[9] M. Mircea, M. Stoica, and B. Ghilic-Micu, "Investigating the Impact of the Internet of Things in Higher Education Environment," in *IEEE Access*, vol. 9, pp. 33396-33409, 2021, doi: 10.1109/ACCESS.2021.3060964.
[10] A. Muhaimeen, K. Aadithiyaprasana, A. Ranjith, S. P. Sasirekha, R. Reshma, and N. Mekala, "Enhancing IoT Security with Federated Deep Learning Techniques," in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2023, pp. 1081-1087, doi: 10.1109/ICCES57224.2023.10192688.
[11] M. S. M. Shah, Y. -B. Leau, Z. Yan, and M. Anbar, "Hierarchical Naming Scheme in Named Data Networking for Internet of Things: A Review and Future Security Challenges," in *IEEE Access*, vol. 10, pp. 19958-19970, 2022, doi: 10.1109/ACCESS.2022.3151864.
[12] X. Yang *et al*., "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3321-3332, Mar. 2022, doi: 10.1109/JIOT.2021.3098007.
[13] M. Dave, "Internet of Things Security and Forensics: Concern and Challenges for Inspecting Cyber Attacks," in *2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS)*, Kottayam, India, 2022, pp. 1-6, doi: 10.1109/ICNGIS54955.2022.10079829.
[14] T. R. Gadekallu *et al*., "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964-988, 15 Jan.15, 2022, doi: 10.1109/JIOT.2021.3119639.
[15] D. S. P. Raj, S. H. Kishore, S. Curle, I. J. Kavitha, and A. Fathima, "IoT-Based Language Learning Devices for Remote English Education: Challenges and Opportunities," in *2024 International Conference on Emerging Research in Computational Science (ICERCS)*, Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICERCS63125.2024.10894762.
[16] J. S. Yalli, M. H. Hasan, L. T. Jung, and S. M. Al-Selwi, "Authentication schemes for Internet of Things (IoT) networks: A systematic review and security assessment," Internet Things, vol. 30, p. 101469, Mar. 2025, doi: 10.1016/j.iot.2024.101469.
[17] Ansari *et al*., "A Detailed Review of Current AI Solutions for Enhancing Security in Internet of Things Applications," *Computers, Materials & Continua*, vol. 83, no 3, p. 3713-3752, 2025, doi: 10.32604/cmc.2025.064027.
[18] A. Razaque, S. Hariri, A. M. Alajlan, and J. Yoo, "A comprehensive review of cybersecurity vulnerabilities, threats, and solutions for the Internet of Things at the network-cum-application layer," *Computer Science Review*, vol. 58, p. 100789, Nov. 2025, doi: 10.1016/j.cosrev.2025.100789.
[19] Y. Wang and D. Fan, "Security authentication protocol for online English teaching system based on Internet of Things," *Alexandria Engineering Journal*, vol. 122, pp. 533-542, May 2025, doi: 10.1016/j.aej.2025.03.011.
[20] Z. Mahdi, N. Abdalhussien, N. Mahmood, and R. Zaki, "Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms," *Computers, Materials & Continua*, vol. 80, no 2, pp. 2139-2159, 2024, doi: 10.32604/cmc.2024.053542.
[21] K. Alhumaid, K. Ayoubi, M. Khalifa, and S. Salloum, "Factors Determining Acceptance of Internet of Things in Medical Education: Mixed Methods Study," *JMIR Human Factors*, vol. 12, no. 1, Jan. 2025, doi: 10.2196/58377.
[22] A. M. Norouzzadeh, S. P. Toufighi, J. Vang, and A. Edalatipour, "Adoption of internet of things in residential smart homes: A structural equation modeling approach," *Sustainable Futures*, vol. 9, pp. 1-12, 2025, doi: 10.1016/j.sftr.2025.100665.
[23] M. U. Tariq, "Chapter 22 - Challenges and solutions of Internet of Things security in the age of connectivity," in H*uman-Centric Integration of 6G-Enabled Technologies for Modern Society*, 2025, p. 327-344, doi: 10.1016/B978-0-443-27434-3.00022-2.
[24] M. Y. Hsieh, "An empirical investigation into the enhancement of decision-making capabilities in corporate sustainability leadership through Internet of Things (IoT) integration," *Internet Things*, vol. 28, pp. 1-15, Dec. 2024, doi: 10.1016/j.iot.2024.101382.
[25] A. Coiduras-Sanagustín, E. Manchado-Pérez, and C. García-Hernández, "Understanding perspectives for product design on personal data privacy in internet of things (IoT): A systematic literature review (SLR)," *Heliyon*, vol. 10, no 9, pp. 1-19, May 2024, doi: 10.1016/j.heliyon.2024.e30357.
[26] A. Jokic *et al*., "A convolutional neural network-enhanced attack detection framework with explainable artificial intelligence for internet of things-based metaverse security," *Engineering Applications of Artificial Intelligence*., vol. 158, p. 111358, Oct. 2025, doi: 10.1016/j.engappai.2025.111358.
[27] A. Waqar, L. A. Alharbi, F. A. Alotaibi, I. Othman, and H. Almujibah, "Impediment to implementation of Internet of Things (IOT) for oil and gas construction project Safety: Structural equation modeling approach," *Structures*, vol. 57, p. 105324, Nov. 2023, doi: 10.1016/j.istruc.2023.105324.
[28] K. Kumar, A. Verma, and P. Verma, "IoT-HGDS: Internet of Things integrated machine learning based hazardous gases detection system for smart kitchen," *Internet Things*, vol. 28, p. 101396, déc. 2024, doi: 10.1016/j.iot.2024.101396.
[29] A. Sadeghi-Niaraki, "Internet of Thing (IoT) review of review: Bibliometric overview since its foundation," *Future Generation Computer Systems*, vol. 143, pp. 361-377, Jun. 2023, doi: 10.1016/j.future.2023.01.016.
[30] Y. Lan, L. Li, and H. Peng, "A verifiable efficient federated learning method based on adaptive Boltzmann selection for data processing in the internet of things," *Journal of Systems Architecture*, vol. 168, p. 103523, Nov. 2025, doi: 10.1016/j.sysarc.2025.103523.
[31] M. Lefoane, I. Ghafir, S. Kabir, and I.-U. Awan, "Internet of Things botnets: A survey on Artificial Intelligence based detection techniques," *Journal of Network and Computer Applications*, vol. 236, p. 104110, Apr. 2025, doi: 10.1016/j.jnca.2025.104110.
[32] H. U. Khan, M. Abbas, O. Alruwaili, S. Nazir, M. H. Siddiqi, and S. Alanazi, "Selection of a smart and secure education school

system based on the internet of things using entropy and TOPSIS approaches," *Computers in Human Behavior*, vol. 159, p. 108346, Oct. 2024, doi: 10.1016/j.chb.2024.108346.
[33] A. T. Somnathe, N. Gopinath, G. Deena, R. Anandh, S. Kumar, and K. S. Tiwari, "Cyber Security Challenges and Effective Security Measures for IOT-based Intelligent Healthcare Systems," *Recent Advances in Electrical & Electronic Engineering*, vol. 18, no. 6, pp. 735-747, Jan. 2025, doi: 10.2174/0123520965276302240115075612.
[34] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, "Security threats of social internet of things in the higher education environment," *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Emerging Technologies for Connected and Smart Social Objects*, 2019, p. 151-171, doi: 10.1007/978-3-030-24513-9_9.
[35] H. Aldowah, S. Ul Rehman, S. Ghazal, and I. N. Umar, "Internet of Things in Higher Education: A Study on Future Learning," *Journal of Physics: Conference Series*, vol. 892, pp. 1-11, Sep. 2017, doi: 10.1088/1742-6596/892/1/012017.
[36] J. M. Fernández-Batanero, M. Montenegro-Rueda, J. Fernández-Cerero, and E. L. Menéses, "Adoption of the Internet of Things in higher education: opportunities and challenges," *Interactive Technology and Smart Education*, vol. 21, no 2, pp. 292-307, Apr. 2024, doi: 10.1108/ITSE-01-2023-0025.
[37] A. (Lachi) Arina and A. Anatolie, "Analysis of IoT security issues used in Higher Education Institutions," *International Journal of Mathematics and Computer Research*, no. 5, pp. 2277-2286, 2025, doi: 10.47191/ijmcr/v9i5.01.
[38] G. S. Matharu, P. Upadhyay, and L. Chaudhary, "The Internet of Things: Challenges & security issues," in *2014 International Conference on Emerging Technologies (ICET)*, Islamabad, Pakistan, 2014, pp. 54-59, doi: 10.1109/ICET.2014.7021016.
[39] R. N. Wambua, "Internet of Things security and privacy in Higher Education Institutions in Developing Countries," *Research Journal of Education, Teaching and Curriculum*, vol. 2, no 1, pp. 1-7, Mar. 2024.
[40] C. O. Turcu and C. Elena, "Industrial Internet of Things as a Challenge for Higher Education," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no 11, pp. 1-6, 2018, doi: 10.14569/IJACSA.2018.091108.
[41] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: Evolution, Concerns and Security Challenges," *Sensors*, vol. 21, no 5, pp. 1-33, Jan. 2021, doi: 10.3390/s21051809.
[42] M. Charytanowicz, E. Milosz, W. Suszyński, R. Stęgierski, and E. Łukasik, "Internet of things as a challenge for higher education," in *INTED2021 Proceedings*, 2021, pp. 5120-5129, doi: 10.21125/inted.2021.1053.
[43] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions," *Wireless Personal Communications*, vol. 119, no 3, pp. 2603-2637, Aug. 2021, doi: 10.1007/s11277-021-08348-9.
[44] N. Letting and J. Mwikya, "Internet of Things (IoT) and quality of higher education in Kenya; A literature review," *Internet Things*, 2020.
[45] R. G. Saadé, J. Zhang, X. Wang, H. Liu, and H. Guan, "Challenges and Opportunities in the Internet of Intelligence of Things in Higher Education—Towards Bridging Theory and Practice," *IoT*, vol. 4, no 3, p. 430-465, Sep. 2023, doi: 10.3390/iot4030019.
[46] I. Florea, L. C. Ruse, and R. Rughinis, "Challenges in security in Internet of Things," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Targu-Mures, Romania, 2017, pp. 1-5, doi: 10.1109/ROEDUNET.2017.8123739.
[47] S. I. M. Ali and M. Nihad, "Internet of Things for Education Field," *Journal of Physics: Conference Series*, vol. 1897, no 1, pp. 1-10, May 2021, doi: 10.1088/1742-6596/1897/1/012076.
[48] A. A. Zainuddin *et al*., "Trends and Challenges of Internet-of-Things in the Educational Domain," *Malaysian Journal of Science and Advanced Technology*, pp. 81-88, Jul. 2021, doi: 10.56532/mjsat.v1i3.17.
[49] K. Zeeshan, T. Hämäläinen, and P. Neittaanmäki, "Internet of Things for Sustainable Smart Education: An Overview," *Sustainability*, vol. 14, no 7, pp. 1-15, Jan. 2022, doi: 10.3390/su14074293.
[50] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things Security: Challenges and Key Issues," *Security and Communication Networks*, vol. 2021, no 1, pp. 1-11, 2021, doi: 10.1155/2021/5533843.

BIOGRAPHIES OF AUTHORS

Kamal Elhattab received a Ph.D. degree in Computer Science from the Faculty of Science, Chouaib Doukkali University, El Jadida, Morocco, in 2024. Currently, he is enrolled in the ELITES Laboratory at the same university, where his research focuses on the internet of things (IoT) and artificial intelligence. His work aims to advance the integration of IoT and AI technologies, contributing to the development of innovative solutions in these fields. He can be contacted at email: kamal.elhattab@gmail.com.

Driss Naji received a doctoral degree in Computer Science from the Faculty of Science and Technics, Sultan Moulay Slimane University, Beni Mellal, Morocco, in 2024. Currently, he is enrolled in the TIAD Laboratory at the same university, where his research focuses on AI and IoT. His work aims to advance the integration of AI and IoT technologies, contributing to the development of innovative solutions in these fields. He can be contacted at email: naji.drisss@gmail.com.

Abdelouahed Ait Ider received a Ph.D. degree in Computer Science from the Faculty of Sciences and Technologies, Sultan Moulay Slimane University, Beni-Mellal, Morocco, in 2018. Professor of Computer Science at Polydisciplinary Faculty of Taroudant, Ibnou Zohr University, Morocco. His research spans artificial intelligence, machine learning, data science, and computer vision, with a focus on deep learning. He can be contacted at email: a.aitider@uiz.ac.ma.

Abdelali Joumad received a Ph.D. degree in Mathematics applied to Computer Science from the Faculty of Science, Chouaib Doukkali University, El Jadida, Morocco, in 2024. Currently, they are enrolled in the LAROSERI Laboratory at the same university, where their research specializes in advanced computational methods for image analysis, with a particular focus on probabilistic modeling and machine learning techniques. His work explores the integration of hidden Markov models, deep learning architectures, and hybrid frameworks to address complex challenges in image segmentation and pattern recognition. He can be contacted at email: ajoumad@yahoo.fr.

Abdelkbir Ouisaadane in Computer Science and Researcher in Artificial Intelligence at Sultan Moulay Slimane University (USMS) in LIMATI Laboratory, received a B.Sc. degree in Mathematics and Computer Science and an M.Sc. degree in applied mathematics from the Faculty of Science and Technics Beni Mellal, Morocco, in 2010 and 2014, respectively. He is currently Professor of Mathematics and Researcher in Computer Science and Signal Processing from Sultan Moulay Slimane University, Morocco. His research interests include speech and speaker recognition, noise robust signal processing, Arabic speech processing, automatic speech recognition in noisy and reverberant environments, spoken language systems, machine learning, noise robustness, HMM and neural models for speech applications, IT systems, machine learning, data modeling, and web services, and innovative educator training. He can be contacted at email: abdelkbir.ouisaadane@gmail.com.

Karim Abouelmehdi received the Ph.D. degree in Computer Science from Faculty of Science, Chouaib Doukkali University, El Jadida, Morocco, in 2017. He worked as an Assistant Professor with the Chouaïb Doukkali University. He is currently an Associate Professor with the Department of Computer Science, Faculty of Sciences, Chouaïb Doukkali University. His research interests include network security, big data, the internet of things, artificial intelligence, and machine learning. He can be contacted at email: karim.abouelmehdi1@gmail.com.