Towards the development of a secure IoT health system for Africa: A bibliometric review

Ida S. TOGNISSE[1], Pélagie HOUNGUE[1], Jules DEGILA[1], Hénoc SOUDE[1], Ife DANSOU[1] and Isaac MBUMBA[1]

[1]*Institut de Mathématiques et de Sciences Physiques (Université d'Abomey-Calavi), Benin*

Abstract

The Internet of Things (IoT) is a technology that is gaining increasing ground around the world and is involved in most areas of activity. In the healthcare sector, IoT devices play an important role, providing relevant information that can be used to make decisions in real time. As a result, the reliability of the collected, analyzed, and processed data is a vital element to ensuring the reliability of this system used in a field such as healthcare, where the consequences of errors can be fatal. However, the data in this system are often exposed to attacks. Therefore, it is important to find appropriate technology and mechanisms to ensure data security. In this work, our objective is to conduct a study of the existing situation in order to understand how to effectively secure IoT data used in smart health. To achieve this, a bibliometric study is performed by examining 2584 documents. The data were visualized using VOSviewer and Bibliometrix and showed that countries such as India, China and United States remain the undisputed leaders in the field. Chinese institutions maintain the expertise followed by India, but collaborate little with foreign researchers, unlike the United States, which is cooperative. They have developed some very interesting solutions, and it is important to learn from the experience of these countries and contextualize them for effective development in Africa. Technically, blockchain remains the most widely used technology for data protection, but the issues of security and protection of patient data remain a major challenge that involves several other parameters.

Keywords

Internet of Things, Data security, healthcare, Health system

1. Introduction

The Internet of Things (IoT) is a concept that reflects a connected set of devices, anywhere, anytime, with any service and any network. The IoT is a megatrend in next-generation technologies that can impact the entire commercial spectrum and can be seen as the interconnection of uniquely identifiable objects and intelligent devices within the current Internet infrastructure, with extended benefits. Benefits typically include advanced connectivity of these devices, systems, and services that goes beyond machine-to-machine (M2M) scenarios [1]. The Internet of Things (IoT) makes smart objects the ultimate building blocks for the development of intelligent and ubiquitous cyber-physical frameworks. IoT has a variety of application areas, including healthcare. The IoT revolution is redefining modern healthcare with promising technological, economic and social prospects [2]. By 2020, 40 % of the IoT-related technologies were related to healthcare, more than any other category, which will represent a market of $ 117 billion [3]. The projections for the impact of IoT on the internet and the economy are impressive, some predicting up to 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025 [4]. Behind all these wearable sensors lies the mega-data generated, the security of which is still a major challenge. Data are often exposed to attacks. Therefore, it is important to find appropriate technology and mechanisms to ensure data security. In this work, our aim is to carry out a

CITA 2025— Emerging Technologies and Sustainable Agriculture, 26-28 June 2025, Cotonou, Benin

*Corresponding author.

†These authors contributed equally.

ida.tognisse@imsp-uac.org (I. S. TOGNISSE); pelagie.houngue@imsp-uac.org/ (P. HOUNGUE); jules.degila@imsp-uac.org/ (J. DEGILA); hsoude@gmail.com/ (H. SOUDE); ife.dansou@imsp-uac.org/ (I. DANSOU); isaac.mbumba@imsp-uac.org/ (I. MBUMBA)

0000-0003-4688-9178 (J. DEGILA)

survey of what already exists in order to understand how to effectively secure IoT data used in health intelligence. Specifically, it involves:

- A systematic bibliometric analysis of the scientific literature on the security of IoT systems applied to healthcare;
- A critical qualitative analysis of the major contributions identified;
- A specific focus on African challenges and opportunities;
- Finally, the proposal of a model for adapting existing solutions to the technical, social and legal realities of African countries.

To meet these objectives, we address the understanding of trends and implications of research in terms of IoT data security in healthcare, to provide a comprehensive overview of the development of the field and future directions. In the remainder of this paper, in session 2 we present the work that has carried out a review of the existing literature, in particular a bibliometric study, on data security in medical IoT systems. In session 3, we present our methodological approach and in session 4 the results obtained in this bibliometric study, followed by a discussion.

2. Literature Review

A bibliometric study is a study that provides a summary of research reported in scientific publications, allowing researchers to generate quantitative information from existing data [5][6]. This study is of vital importance for researchers to situate themselves in relation to their investigations, given the range of research already covered in the field. Several bibliometric studies have been carried out on objects connected to the internet and health. In [7], Maysam et al. explore the transformative impact of the Internet of Things (IoT) on healthcare care, highlighting its potential to improve patient monitoring, optimize treatments, and reduce costs. The authors provide a systematic assessment of the scientific output in this rapidly evolving field, making it a valuable resource for understanding current trends and future directions in smart healthcare systems. The authors point out that research in this area is expanding rapidly, with a notable increase in publications and international collaborations. They also highlight the importance of continuing to explore IoT applications in healthcare to develop smart and efficient healthcare systems in the future. This systematic evaluation of scientific publications provides a solid basis for understanding current trends and future directions in IoT research in medicine. They analyzed articles indexed in the Web of Science database covering the period from 2013 to August 2024, while suggesting that future researchers explore other databases such as scopus to facilitate comparisons with the results of this study. Using bibliometric analysis to shed light on trends and developments in this rapidly evolving field over the period 2015 to 2022, Hoang et al argue that the fascinating integration of the Internet of Things (IoT) into the healthcare sector highlights its importance and impact on modern healthcare electronics [8]. In [9], a bibliometric analysis highlighted a comprehensive description of the Internet of Things (IoT) concept between 2009 and 2019. They reviewed the security aspect and the importance of understanding research trends and emerging areas to better respond to current technological challenges. The study focused on articles published in the Web of Science database, which may not represent all research and publications in the field of IoT. The authors recommended exploring the use of artificial intelligence (AI) and machine learning as promising technologies to improve the security of IoT devices. These technologies can potentially help detect and prevent security threats by analyzing data in real time and identifying patterns of anomalous behavior. Katarina et al in [10] worked on metavers security by conducting a bibliometric study. Thanks to this in-depth bibliometric analysis, the authors map the significant themes and prominent sources in this evolving field. The authors have taken a time frame of 2015-2024.

Despite the multitude of works that focus on a survey of IoT in healthcare, there is a gap in the literature in terms of studies that address the security of the generated data. Very few studies focus on the case of developing countries. In this sense, in [11], Sylverster et al explored the security and privacy implications of IoT devices in the healthcare system in a developing country like Zambia. The study identified that

vulnerabilities such as device authentication, data breaches, insufficient regulatory frameworks pose risks to patient data and overall system integrity. In addition, the context of developing countries is marked by a lack of communication and energy infrastructure, low technology adoption and healthcare workers who do not have the minimum skills to deal with the risk of cyber attacks. In [12] through a literature review, the authors demonstrated the advantages and disadvantages of IoT and connected healthcare by highlighting the security and privacy issues encountered on a global scale and on an African scale in particular by targeting a developing country such as South Africa. The study looked in more detail at the advantages and disadvantages of the proposed attack detection frameworks. The common disadvantages of the solutions are that the systems are unable to learn new patterns, new behaviours and define security measures. A systematic review has also been developed in [13] and provides a comprehensive framework that can be used to identify risks that affect authenticity, secure access, network availability and security planning in IoT systems developed for healthcare. Despite this work which focuses on developing countries, there is still a lack of information on how the experience of developing countries and existing new technologies could help to ensure safe deployment in developing countries.

3. Methodology

The methodology adopted for this research is divided into several phases. Firstly, the data for this research was collected from the Scopus database, which includes 2584 published between 2020 and 2025. The data extraction date is 25 April 2025 and the research string is: ((“Internet of Things” OR “Connected object” OR IoT OR “smart health”) AND (“Data security” OR “Data Protection” OR “Information security” OR “Data Integrity” OR “data confidentiality” OR “data privacy”) AND (health OR medical OR sick OR patient)). The data visualization and analysis phase enabled us to explore our database, obtained after standardizing the search terms on Scopus, and to extract the information needed to achieve our objectives for this study. The VOSviewer and RStudio software with the Bibliometrix library were used to view and analyses the data, producing the results presented in the next section.

4. Results and Discussions

Bibliometric analysis is a powerful tool that uses statistical approaches to detect descriptive and analytical variations in a research subject. It allows trends, productivity and future directions of research to be assessed in order to draw meaningful conclusions. In this section, we present the results of our bibliometric analysis in order to meet the research objectives presented in section 1.

4.1. Annual distribution of publications

Figure 1 illustrate annual distribution of scientific production on the data base collected.
From 2020 to 2025, we saw a steady increase in the number of articles published each year. The number of publications increased from 216 in 2020 to 833 in 2024, a nearly 4-fold increase in 4 years. Already 236 articles have been published for the first quarter of 2025.

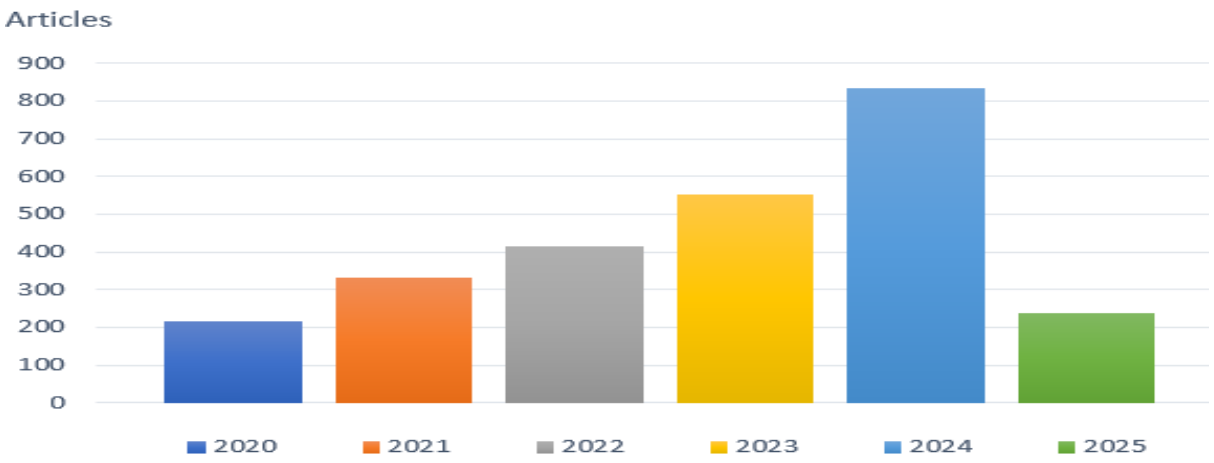

Figure 1: Breakdown of publications by year

4.2. Countries of Scientific contribution

Figure 2 shows the distribution of publications by country. This is a network visualisation, each circle represents a country, and the size of the circles is proportional to the number of publications from that country. The different colours of the nodes suggest the presence of clusters or groups of highly interconnected countries.

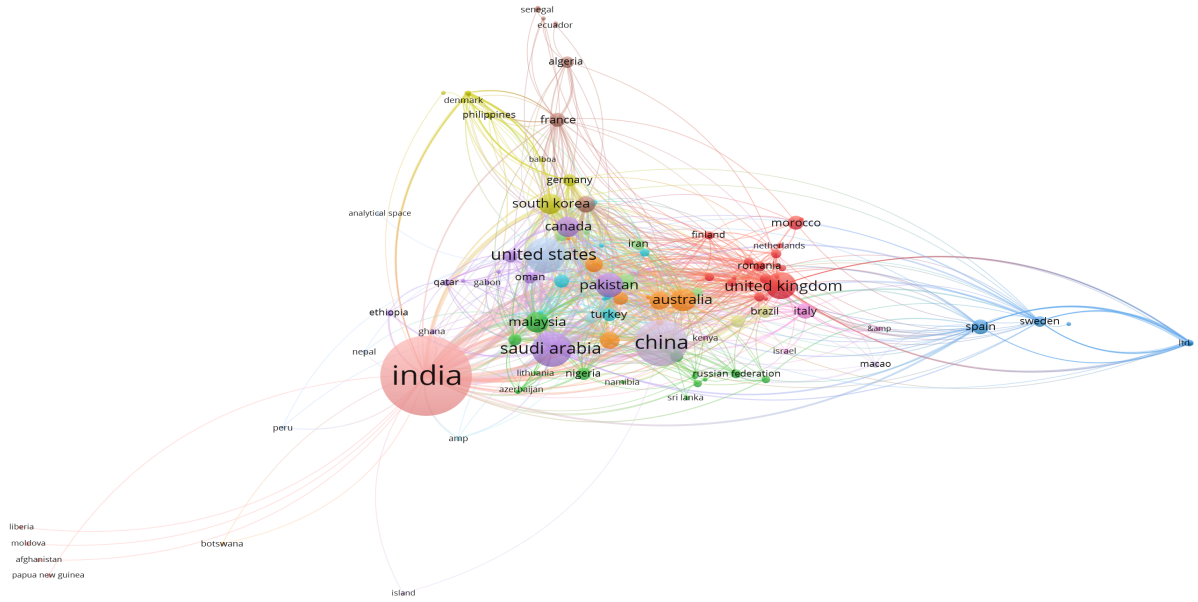

Figure 2: Cooperation network

In this figure, India, China, the United States and Saudi Arabia dominating in terms of total number of publications. However, very little contribution comes from countries such as the African countries. Only countries such as Nigeria, Ghana, Senegal, Algeria and Egypt are featured with a small contribution. We can also see that there appears to be fairly dense international collaboration in the field, with several groups of countries working more closely together. India, China and the United States are major centers, indicating their strong involvement in international projects; Europe forms a dense group, showing numerous regional collaborations; Africa tries to situate itself in relation to three countries, India, China and Saudi Arabia, with which collaborations are carried out.

4.3. Distribution of publications by journals

Figure 3 presente the 10 most relevant sources of collected data.

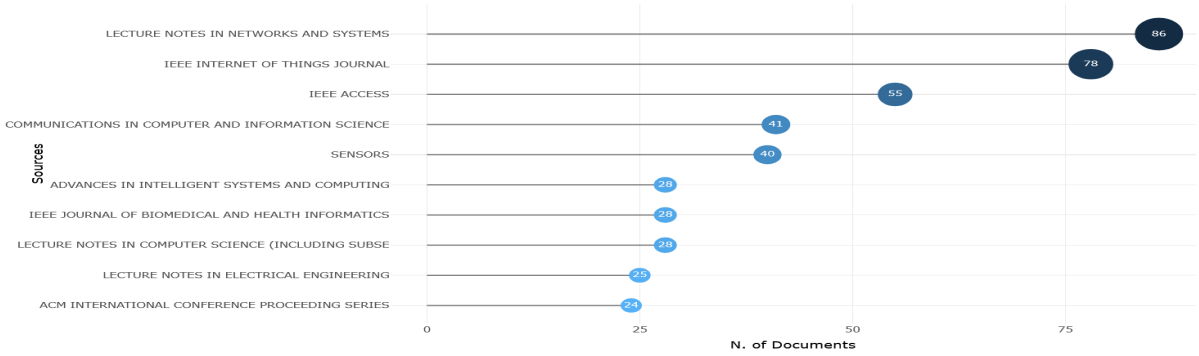

Figure 3: Most Relevant Sources

After going through the analyses found in the Scopus database, bibliometrix has identified the ten journals with the highest number of articles published in this field of research. Lecture Note in network system comes first with 86 articles. IEEE Internet Of Thing journal and IEEE Access follow with 78 and 55 papers respectively.

4.4. Keyword co-occurrence networks

Figure 4 shows the co-occurrence of terms in the field. We can see that the data security aspect has been taken seriously in this period, with an emphasis on blockchain technology, integrating artificial intelligence, machine learning, and deep learning...

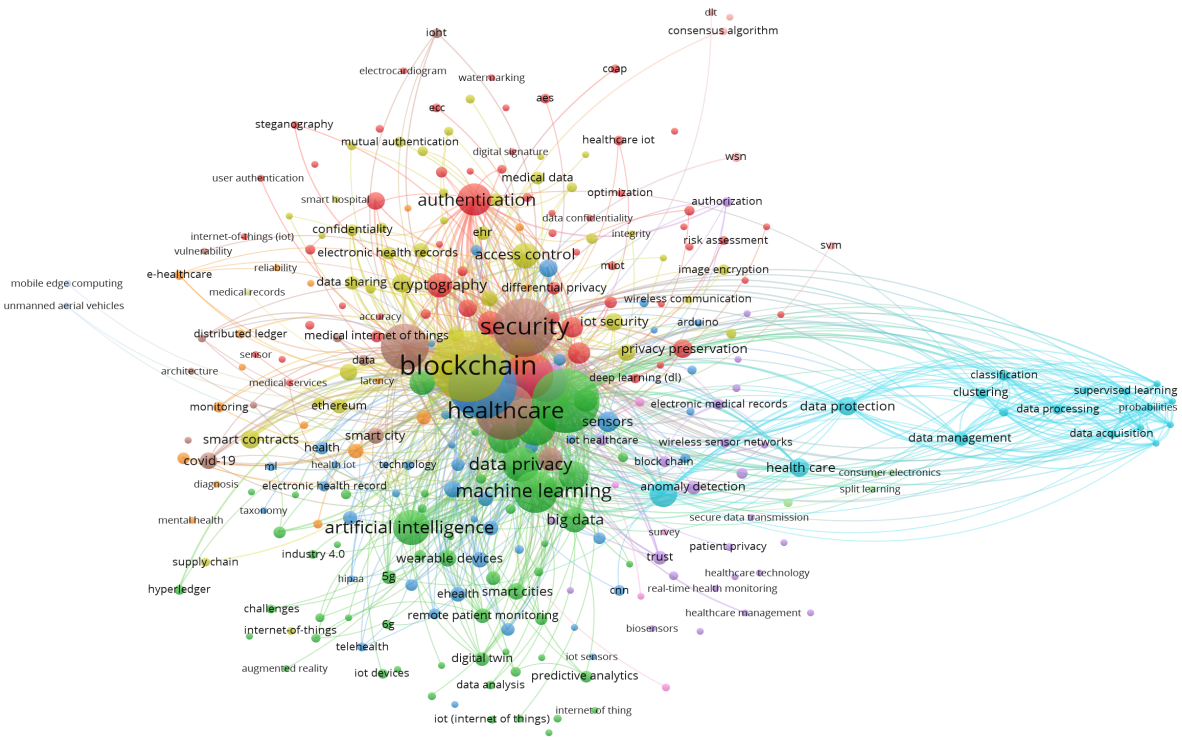

Figure 4: Co-occurrence networks of terms

clarifying that themes such as "Internet of Things", "network security", "data protection" and "blockchain" appear as moderately central and developed topics. This suggests that they are at the heart of the discussions in the corpus studied. These concepts form a structuring axis of the field but still require efforts to reach full maturity.

Several distinct color clusters can be identified in this figure:

- The red cluster centered on the theme "authentication", including terms such as "cryptography", "privacy prevention", "IoT security", "digital signature", highlights the security aspects of the systems. Authentication is a central term in the red security cluster, but it also has links with other clusters, notably healthcare.
- A blue cluster associated with "data privacy" and including terms such as "data protection", "privacy preservation", "differential privacy", "trust", etc., highlighting the challenges of data protection.
- A yellow cluster around "blockchain", with terms such as "smart contracts", "distributed ledger", "ethereum" etc, indicating the application of blockchain. Blockchain appears to be a bridge between security and specific applications such as smart contracts and potentially healthcare.
- A green cluster linked to "artificial intelligence" and "machine learning", with terms such as "big data" and "predictive analytics", presenting technologies commonly found in the system.
- A cluster associated with "data management", "data acquisition", "classification", "clustering", etc., representing aspects of data management and analysis.

4.5. Top ten authors

Figure 5 ranks the 10 most relevant authors in a field, with a strong contribution to the scientific literature.
KUMAR A is the author with the highest number of publications. No African author appears in this

Figure 5: Top Ten authors

list of the 10 best authors.

4.6. Ten best papers

Table 1 illustrates the most cited papers in the world, which would serve as a basis for researchers wishing to address topics in this direction, the most cited paper is that of STOYANOVA M published in 2020 in IEEE COMMUN SURV TUTOR, with 643 citations. The second paper is that of HASSAN MU, published also in 2020 in IEEE COMMUN SURV TUTOR.

In what follows, we will take an in-depth look at these best papers in order to draw out solutions and contributions to the development of these systems in Africa.

Table 1: Best Papers

Paper	Total Citations	Country based	Objectives	Methodology	Results	Limitations
STOYANOVA M, 2020, IEEE COMMUN SURV TUTOR [14]	643	Germany, Grrece	Identify and analyze the key issues involved in the complex process of IoT-based investigations, including legal, privacy and cloud security challenges.	Survey	This article demonstrates the importance of adapting and extending traditional forensic tools to the IoT domain, while maintaining forensic principles. There is a need for explicit IoT security regulations and generally accepted standards. Research institutions, companies and the law need to work together, as the expansion of IoT will bring increasing challenges.	Does not present a technical solution approach
HASSAN MU, 2020, IEEE COMMUN SURV TUTOR [15]	427	Australia	Presents a comprehensive survey of differential privacy techniques for modern cyber-physical systems.	Survey	An effective solution to overcome these privacy risks for cyber-physical systems is to preserve data by adding noise using differential privacy perturbation mechanisms. The authors propose that modern differential privacy algorithms combined with techniques such as machine learning and blockchain can eradicate the problem of privacy loss.	No case study, no implementation and simulation
HATHALIYA JJ, 2020, COMPUT COMMUN [16]	351	India	Explore the solution to provide information to researchers and practitioners on security and privacy in healthcare 4.0	literature review	The authors illustrate basic and advanced architectures, using traditional security methods and blockchain technology respectively. They also describe the taxonomy of security and privacy issues related to healthcare 4.0. It covers all aspects of healthcare, such as processing, data management, IoT, ML, telehealth, policies, network traffic and authentication schemes	No proposal for a global solution that takes into account all the security challenges presented in the paper.

BHUIYAN MN, 2021, IEEE INTERNET THINGS J [17]	323	Bangladesh	Analyse the security, privacy, and data protection functionalities, which face challenges in many IoT-based healthcare architectures	systematically reviewed	To ensure end-to-end security and privacy to guarantee data integrity and validity, the authors propose a Barebone Operating System for IoT medical devices/sensors that will contain only a minimal viable interface to the outside world by limiting network services. Also, blockchain should be included to enhance the handling of records such as creation, deletion and updates. Although IoT and blockchain have different operating principles and architecture, the integration of these two networks is possible using a software platform.	The solution is not tested
YU S, 2021, IEEE INTERNET THINGS J [18]	300	China	Minimise total offload delay and network resource utilisation for multi-acces perifery in an IoT network, 5 G	design and simulation	They propose a 2Ts-DRL algorithm based on federated learning for I-UDEC to guarantee device confidentiality. It should be noted that I-UDEC still faces security challenges, such as DDoS attacks and packet saturation. For this reason, they are proposing to integrate blockchain into I-UDEC, as integration can ensure effective monitoring of the control plane to prevent malicious behaviour.	The study focused on 5G network parameters, and the specific challenges of IoT in healthcare are not specifically taken into account.
SARKER IH, 2021, SN COMPUT SCI [19]	285	Australia	Present a comprehensive view of data science, including different types of advanced analytics methods that can be applied in areas such as healthcare	Literature review	Advanced analytics solutions based on data science and machine learning can be used to enhance security in systems such as IoT applied in healthcare	It is not developed in the article comments AI and machine learning could help enhance security
FAROUK A, 2020, COMPUT COMMUN [20]	280	Canada	Critically analyse the impact of blockchain and IoT on the healthcare sector.	Literature review	To ensure the security of IoT data in healthcare, it is essential to choose blockchain and ensure that access to the blockchain is properly developed to avoid any leakage of patients' personal information. For the implementation of these systems, two complementary technologies should be considered to accelerate adoption and profitability. The first is the use of AI, which aggregates and then extracts information by identifying patterns and correlations within large volumes of data. Hybrid clouds are the second key to a solid foundation for IoHT and blockchain.	No implementation, no deployment.

KUMAR A, 2021, COMPUT COMMUN [21]	267	India	Propose a secure and energy-efficient intelligent building architecture in which devices are installed and observe how to integrate the DTLS protocol with the secure hash algorithm (SHA256) using certificate authority (CA) optimisations to improve security.	Case study simulation	Each device is identified by its unique address, and one of the main Web transfer protocols is the Constrained Application Protocol (CoAP). This is an application-layer protocol that does not use protected channels for data transfer. Automatic key management, confidentiality, authentication and data integrity are features of Datagram Transport Layer Security (DTLS).	The IoT system is much more widely used for energy optimisation. Alsa, the study of does a typical case IoT in the field of health.
JAMIL F, 2020, SENSORS [22]	264	Korea	Propose a new platform for monitoring patient vital signs using blockchain-based smart contracts	Design and simulation	The system designed is based on a web paradigm with the development of web front-end technologies, including HTML5 and JavaScript, to improve resource management within the network. Similarly, blockchain provides product-centric services via representational state transfer application programming interfaces (REST APIs) to address inherent challenges such as data security, identity and scalability.	In-depth testing of the proposed system with different IoT frameworks.
MAKHDOOM I, 2020, COMPUT SECUR [23]	258	Australia	To propose an innovative framework that secures and preserves the confidentiality of IoT data in a smart city environment.	Design and simulation	PrivySharing, an innovative secure and privacy-preserving data sharing mechanism based on blockchain, has been proposed. For data security, access to user data is controlled by integrating access control rules into smart contracts. In addition, data is isolated and secured through private data collection and encryption, respectively. Similarly, the REST API enabling customers to interact with the blockchain network benefits from double security: an API key and OAuth 2.0	No mechanism for securely integrating IoT devices into the blockchain network

Most of the most cited works in our database are systematic literature reviews. This shows how important it is for the research community to have an in-depth view of the subject of IoT data security and protection in healthcare. In the healthcare system, medical information is sensitive by nature, and its security is a challenge. Whatever the use of IoT in the healthcare sector, the attack surface and vulnerabilities of the IoT infrastructure the security risks are inherent in any connected device. From these various studies, it is clear that for reliable and sustainable deployment in Africa, certain factors need to be taken into account.

4.7. Recommended model for adapting existing solutions to the realities of African countries

We propose a structured adaptation model based on certain criteria, including:

- Appropriate technological choices: low-cost devices, low energy consumption.
- Legal aspects: proposal for a minimum medical data protection framework adapted to the African context.
- Training and awareness: define training programmes for local users (healthcare professionals, technicians).
- Deployment strategy: giving priority to distributed architectures to reduce dependence on unstable networks.

Figure 6 shows a schematic diagram of our solution approach.

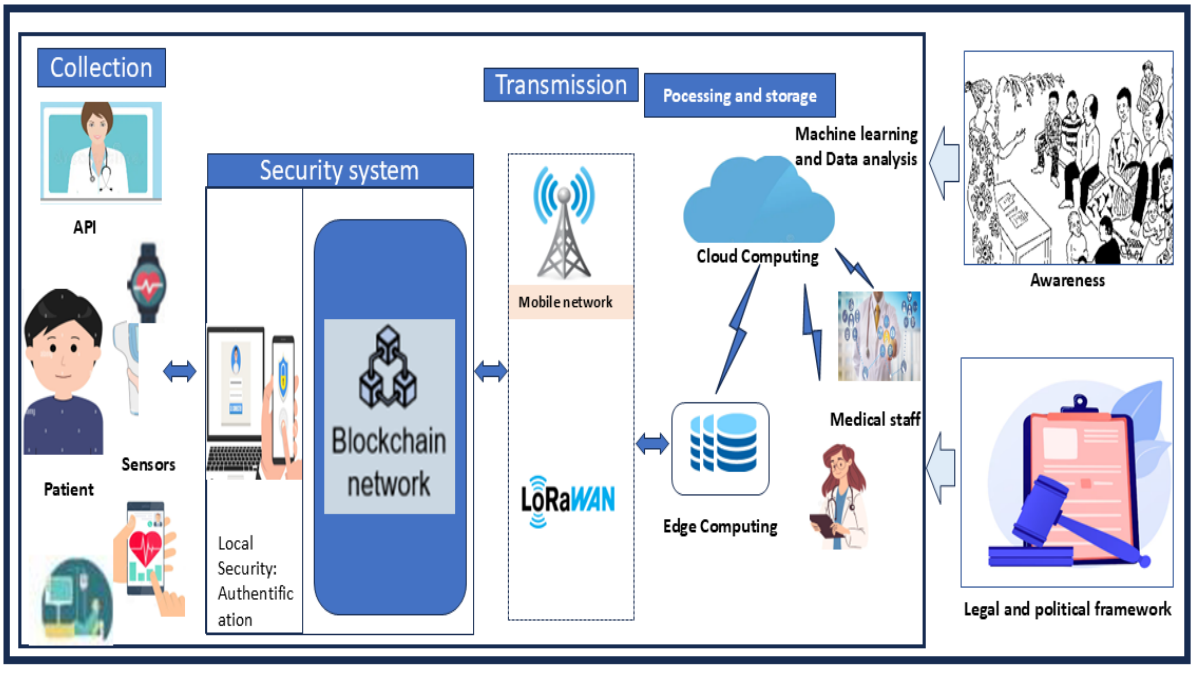

Figure 6: Proposal for the development of a secure IoT health system

Firstly, the IoT system must be based on reliable infrastructure and quality Internet connectivity (see wireless networks and move towards 5G). Secondly, to ensure data security, algorithms combining machine learning and blockchain must be implemented. In this system, each device must be identified by a unique address, using Web transfer protocols such as the Constrained Application Protocol (CoAP). REST APIs must also be used, enabling clients to interact with the blockchain network, which benefits from double security. For implementation in these systems, these complementary technologies need to be considered to accelerate adoption and profitability. Energy optimization must also be a priority.

Finally, a blockchain framework for IoT in healthcare needs to be considered. There is a need for explicit IoT security regulations and standards generally. The framework must take into account not only the techno-economic but also the legal realities of African countries.
Therefore, several aspects need to be taken into account to ensure the secure deployment of this technology. For each aspect, we need to:

Equipments :

- Biometric sensors adapted to users' needs.
- Wearable devices for remote monitoring of the patient's condition.
- Connected medical devices with simple, ergonomic interfaces.
- Secure transmission to the local IoT gateway via (LoRaWAN, NB-IoT, mobile phone networks).
- Edge processing: Maximise local data processing (IoT gateway) to reduce dependency on a stable internet connection and limit latency in the event of critical alerts.
- Local security: Manage device authentication and data encryption. o Redundancy: Provide mechanisms to keep devices and applications running in the event of temporary loss of connection to the central network.

Data analysis and security

- Tools for analyzing the data collected (big data, artificial intelligence), to identify trends, improve clinical decision-making, and support public health policies.
- Develop a blockchain to strengthen system security.

Legal and policy aspects

- Draw up clear principles relating to the quality of consent, purpose, minimisation of collection, limitation of storage periods, security and confidentiality.
- Establishment of a national authority to monitor compliance with the legal framework for the processing of personal data and penalise breaches.
- Inclusion of data protection modules in the training of health professionals and technicians.

5. Conclusion

In this article, we conduct a bibliometric study on the secure development of IoT in healthcare. The Internet of connected objects requires particular attention in terms of protecting user data, which is why researchers in recent years have focused on emerging technologies such as Bitcoin, artificial intelligence, machine learning and deep learning to guarantee the integrity of user data, It would be desirable for the major leaders (China, India, USA, Germany), who are at the heart of the collaborative networks, to strengthen their scientific cooperation in order to find solutions to the problems that remain unresolved in this field, and for these nations to try to encourage scientists from other countries who want to tackle this issue. The study revealed that the Internet of Things (IoT), data privacy, and blockchain occupy a central place, indicating that they constitute the pillars of the field. The study, based on Scopus data, suggests that similar studies in combination with several databases would provide additional in-depth information to understand the subject and compare it to produce more relevant analyzes. Analysis of the most cited articles has enabled us to understand that for secure deployment in Africa, it is necessary to opt for a combination of technologies such as machine learning and blockchain and well-determined protocols. There is an urgent need for explicit IoT security regulations and standards, as well as a comprehensive framework that takes into account all the challenges of IoT deployment in the specific context of Africa. Being a simple review of existing literature, the main limitation of this work is that it does not focus on the application of the proposed technologies, on testing and deployment. But it does provide a starting point for design, implementation and deployment work to establish an appropriate framework for the deployment of IoT systems in the specific case of Africa. Another limitation is that the data used for this study comes solely from Scopus. The inclusion of Web of Science and IEEE Xplore would increase coverage.

Declaration on Generative AI

During the preparation of this work, the author(s) used X-GPT-4 and Gramby in order to: Grammar and spelling check. Further, the author(s) used X-AI-IMG for figures 3 and 4 in order to: Generate images. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] I. Saleh, Issues and challenges of the internet of things (iot), Internet des objets 17 (2017) 1–19. doi:10.21494/iste.op.2017.0133.

[2] S. M. R. Islam, D. Kwak, M. H. K. UWB, M. Hossain, K.-S. Kwak, The internet of things for health care: A comprehensive survey, Electronic 3 (2015) 678–708. doi:10.1109/ACCESS.2015.2437951.

[3] D. V. Dimitrov, Medical internet of things and big data in healthcare, Healthc Inform Res 22 (2016+) 156–163. doi:10.4258/hir.2016.22.3.156.

[4] K. Rose, S. Eldridge, L. Chapin, The internet of things (iot): An overview – understanding the issues and challenges of a more connected world, Internet Society (2015).

[5] S. T. Konstantinidis, A. Billis, H. Wharrad, P. D. Bamidis, Internet of things in health trends through bibliometrics and text mining, Stud Health Technol Inform 235 (2024) 73–77. doi:10.3233/978-1-61499-753-5-73.

[6] K. H. Abdullah, N. Gazali, R. Muzawi, E. Syam, M. F. Roslan, D. Sofyan, Internet of things (iot) in education: A bibliometric review, International Journal of Information Science and Management 22 (2024) 183–202. doi:10.22034/ijism.2023.1977600.0.

[7] M. Alavi, M. Dehghan, Internet of things in medicine: a bibliometric review, International Journal of Web Research (2022). doi:10.22133/ijwr.2024.476672.1237.

[8] N. H-S, D. H.-C. M. Q-P, M. J, H. J, P. M, P. J. A, A bibliometrics analysis of medical internet of things for modern healthcare, Electronics 12 (2023). doi:10.3390/electronics12224586.

[9] M. I. Jaya, M. F. A. Razak, D. N. E. Phon, S. I. Hisham, A. Firdaus, Systematic description of the internet of things: a bibliometric analysis, J Theor Appl Inf Technol 100 (2022) 2835–2853.

[10] K. Kostelić, D. Etinger, Securing the metaverse: A bibliometric analysis of cybersecurity challenges and research trajectories, IEEE Engineering Management Review (2024) 1–21. doi:10.1109/emr.2024.3453974.

[11] S. Mugala, K. A. L. Sibanda, C. Mulenga, M. Hachamba, H. Mwiinga, Exploring security and privacy implications of iot devices in zambia's healthcare system, East African Journal of Information Technology (2025). doi:10.37284/eajit.8.1.2896.

[12] K. H. Naqvi, E. D. Markus, M. Muthoni, A. Abu-Mahfouz", A critical review of iot-connected healthcare and information security in south africa, Lecture Notes in Networks and Systems 286 (2021). doi:10.1007/978-981-16-4016-2_70.

[13] K. N, R. R", Iot medical device risks: Data security, privacy, confidentiality and compliance with hipaa and cobit 2019, South African Journal of Business Management 56 (2025). doi:10.4102/sajbm.v56i1.4796.

[14] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E. K. Markakis, A survey on the internet of things (iot) forensics: Challenges, approaches, and open issues, IEEE Communications Surveys and Tutorials 22 (2020) 1191–1221. doi:10.1109/COMST.2019.2962586.

[15] H. Muneeb, M. H. Rehmani, J. Chen, Differential privacy techniques for cyber physical systems: A survey, Commun. Surveys Tuts. 22 (2020) 746–789. doi:10.1109/COMST.2019.2944748.

[16] J. J., Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in healthcare 4.0, Computer Communications 153 (2020) 311–335. doi:10.1016/j.comcom.2020.02.018.

[17] M. N. Bhuiyan1, Internet of things (iot): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities, IEEE INTERNET OF THINGS JOURNAL (2021). doi:10.1109/JIOT.2021.3062630.

[18] S. Yu, X. Chen, Z. Zhou, X. Gong, D. Wu, When deep reinforcement learning meets federated learning: Intelligent multi-timescale resource management for multi-access edge computing in 5g ultra dense network, IEEE Internet of Things Journal 8 (2020) 1–19. doi:10.1109/JIOT.2020.3026589.

[19] I. H. Sarker, Data science and analytics: An overview from data-driven smart computing, decision-making and applications perspective, SN Computer Science (2021). doi:10.1007/s42979-021-00765-8.

[20] A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: Vision and future opportunities, Computer Communications (2020) 223–235. doi:10.1016/j.comcom.2020.02.058.

[21] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, P. Singh, Secure and energy-efficient smart building architecture with emerging technology iot, Computer Communications (2021) 207–217. doi:10.1016/j.comcom.2021.06.003.

[22] F. Jamil, S. Ahmad, N. Iqbal, D.-H. Kim, Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals, Sensors (2020). doi:10.3390/s20082195.

[23] M. Imran, Z. Ian, A. Mehran, L. Justin, N. Wei, Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, Computers security 88 (2020). doi:10.1016/j.cose.2019.101653.