

Cybersecurity in health sector: a systematic review of the literature

Catherine Vanessa Peve Herrera¹, Jonathan Steve Mendoza Valcarcel¹, Mónica Díaz¹,
Jose Luis Herrera Salazar², Laberiano Andrade-Arenas³

¹Faculty of Engineering and Business, Universidad Privada Norbert Wiener, Lima, Perú

²Faculty of Engineering, Sciences and Administration, Universidad Autónoma de Ica, Lima, Perú

³Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima, Perú

Article Info

Article history:

Received Nov 3, 2022

Revised Mar 24, 2023

Accepted Apr 2, 2023

Keywords:

Cyberattacks

Cybersecurity

Health sector

Patients

Systematic review

ABSTRACT

Currently, health centers are being affected by various cyberattacks putting at risk the confidential information of their patients and the organization because they do not have a plan or tools to help them mitigate these cyberattacks, which is important to know what measures to take to protect the privacy of personal data. The present work was carried out under a systematic literature review, which aims to show the importance of cybersecurity in the health sector knowing which tools are the most used and efficient to prevent a cyberattack. A systematic review of 301 articles was carried out, 79 of which are aligned with the objective set, fulfilling the inclusion and exclusion criteria. The search for information was carried out in the Scopus and Dimensions databases. The analysis carried out has resulted in good information that was compiled for the development of this topic, being favorable thanks to the different research of different authors.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Laberiano Andrade-Arenas

Facultad de Ingeniería, Universidad Tecnológica del Perú

Jr. Natalio Sanchez 125-Lima, Perú

Email: landradearenas@gmail.com

1. INTRODUCTION

In recent years, cybersecurity has played an important role all over the world, for different types of companies and organizations. Because there is a large amount of data that is collected, processed, and stored on a computer, cybersecurity has become an important issue. In this regard, Olofinbiyi [1] mentions that during the pandemic, unauthorized medical information has had negative consequences, where hackers have taken advantage of the urgency of the situation to break into equipment, manipulate data, damage facilities, putting the health, and lives of patients at risk. Likewise, Wasserman and Wasserman [2] mentions that in general, hospitals should recognize that, in cyber incidents, the real victim is the patient, as they are physically and digitally at risk when medical devices or treatments are compromised. As mentioned by the authors we agree, but it is worth mentioning that these cyber-attacks have not only been executed with greater magnitude during the pandemic but also since several years ago.

Likewise, in Latin America, one of the sectors most vulnerable and affected by cyber-attacks are healthcare systems. Since they hold a large number of interconnected devices, from hospital devices to patients of the entity, they are the most vulnerable to cyberattacks. Subsequently, Buzzio-Garcia *et al.* [3] mentions that these hospital teams lack security policies and effective methods; these errors generate profound consequences in patient information, both in clinical results and in the breach of personal data, considerably affecting security. According to the above, the great risk posed by cyber-attacks is evident.

Regarding the local context, in Lima-Peru there is a trend of security deficiencies in hospital organizations. The leakage of personal data is manifested as the amount of digital information of a patient or employee that circulates in networks, equipment, and systems. It is that Rubio *et al.* [4] emphasizes that, for hackers, knowing and capturing this information constitutes a danger to society that must be prevented and combated. This involves the development of measures (such as the use of antivirus software, antimalware, intrusion detection, frameworks, and standards) as well as protocols to ensure computer security. Given the above, the present research is developed to analyze the importance of cybersecurity in the health sector. For most companies in the healthcare industry, information is considered the most important asset. In this sense, Quimiz-Moreira *et al.* [5] mentions that medical information is sensitive and critical because it contains detailed patient data on their socioeconomic situation, analysis, diagnosis, and treatment managed by the medical center, avoiding unauthorized changes or data theft, which is a potential problem affecting information systems and patients treated under these conditions.

In addition, Barnes and Daim [6] mentions that cybersecurity in hospitals must be formed with security policies, being clear to respond quickly and effectively to threats of all kinds that are becoming increasingly sophisticated. According to the insinuated, it is very important to take measures to protect the privacy of personal and public data. Therefore, the objective of the research is to know the importance of cybersecurity in the health sector, as well as to know the most frequent cyberattacks in this sector and in turn to know the technologies in the health sector to protect against cyberattacks, for a proper procedure of patient information as it is a main mechanism of data confidentiality. The document is composed as follows: in section 2 will be the methods, in the section 3 will be the results, in section 4 will be the discussions, and in section 5 the conclusions.

2. METHOD

The method used is the preferred reporting items for systematic reviews and meta-analyses (PRISMA) method [7]. Finally, we conducted an in-depth analysis of the identified articles to identify the most important statistical factors and methods used in teaching inclusive education and linked them to the results of the bibliometric analysis. This will allow the investigation to be better systematized.

2.1. Type of study

The present research work is carried out under a systematic literature review, with the purpose of learning more about the topic of “cybersecurity in the health sector”, in a more summarized and updated way. The type of investigation allows to have a clear idea in which the investigation is focused. In this way it will be a guide on the path to investigate.

2.2. Research questions

The proposed research questions are as follows: (4.1.1.) What are the emerging technologies that most influence the healthcare sector? Also, (4.1.2.) What are the most frequent cyberattacks in the healthcare sector? (4.1.3.) Finally, what technological tools are immersed in the healthcare sector to deal with cybersecurity?

2.3. Search strategy

2.3.1. Generic search strategy

As a first point, a generic search was carried out to perform the bibliometric analysis. In this way, it allows to have a broad perspective of how the main variable that is cybersecurity in the health sector is counted at an international and national level. Likewise, to know its characteristics such as the countries where most research is done, and the most frequent words used. The search was carried out with Scopus since it contains a large volume of metadata. For the search, we used words such as “cybersecurity” “cyberattacks” “health” and “hospital” obtaining 183 articles. Subsequently, these articles were exported to Vosviewer software and R programming language, allowing an in-depth analysis of the articles.

2.3.2. Specific search strategy

After formulating the questions, we continue to employ an information search strategy related to the topic, that is to say, a specific search. The search was performed using Boolean equations. The search was performed in databases such as Scopus (183 articles), and dimensions (112 articles) both by title and abstract. For this purpose, the following boolean equation was used (“cybersecurity” or “cyberattacks”) and (“health” or “hospital”), 2022, 2021, 2020, 2019, 2018, article, all open access.

2.4. Criteria for inclusion and exclusion

2.4.1. Inclusion criteria

Articles that have reference to cybersecurity in the health sector within the last 5 years (2018-2022) were included, and articles that raised proposals about the topic in the English language were included. To ensure the effectiveness of the search process, terms referring to the research question posed were established. Inclusion allows us to have a more limited panorama.

2.4.2. Exclusion criteria

Articles less than 5 years old and articles that were in Spanish were excluded, as well as articles that were not open access. On the other hand, articles referring to the three research questions that will allow the realization of this relevant research for the scientific entity are selected. In Figure 1, shows us the result of the number of articles included. After performing the search with the Booblean equation used, the results were obtained in dimensions (117 articles) and Scopus (183 articles). After employing the inclusion and exclusion criteria, the remaining articles were in dimensions (35 articles) and Scopus (44 articles), resulting in a total of 79 articles relevant to the systematic review.

3. RESULTS

As shown in Figure 1, 301 articles found in the databases related to the research topic were analyzed; duplicate articles and those that were not relevant to the present systematic review were eliminated. Subsequently, from the review of the articles, 71 articles were selected, excluding 230 articles according to the exclusion criteria and which did not help to answer the research question posed. Finally, as a result, 71 articles were obtained for the systematic review.

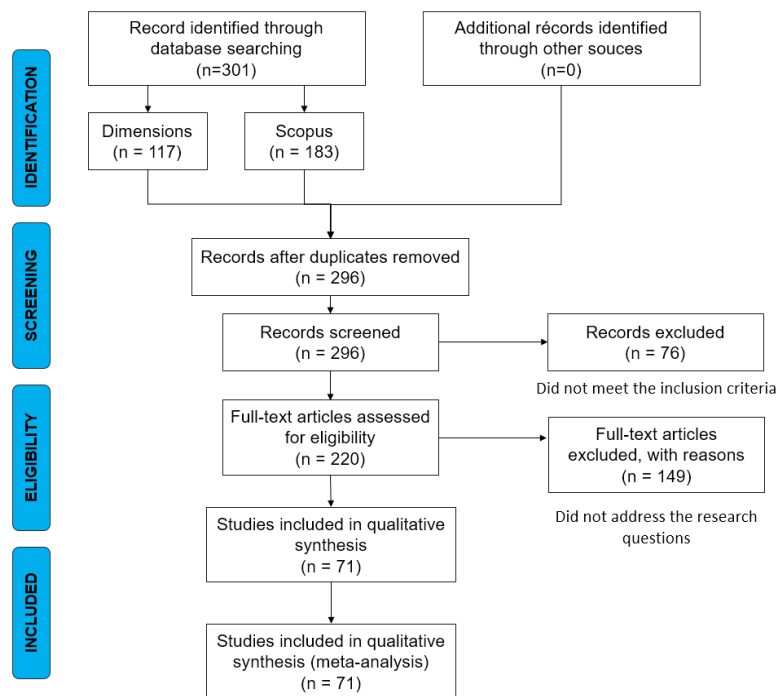


Figure 1. Inclusion and exclusion flowchart for articles

3.1. In a generic way

Figure 2, is analyzed using the co-occurrence and keyword visualization network; where the minimum number of occurrences of a word is 5. Of the 1,965 keywords, 141 meet the threshold. The keywords with the highest total link strength were selected. So, the number of selected keywords is 141 which is formed by 6 clusters; where the red color cluster is the most outstanding with the word cybersecurity. It has 133 links with a total link strength of 6,862. Likewise, the most relevant words are humans, health care, COVID-19, privacy, and the internet of things (IoT); this allows us to take into account this variable since cybersecurity cannot be without a study of the human and medical parts.

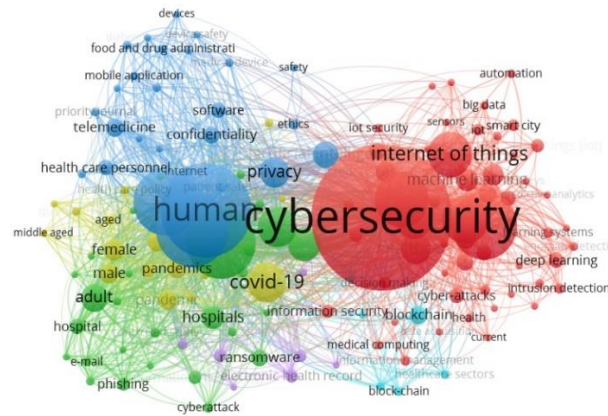


Figure 2. Network visualization

3.2. In a specific way

The bibliometric analysis was performed using the R language where the documents are analyzed with a specific search. In Figure 3, two thematic clusters can be distinguished, both well cohesive. In the red cluster, the central term is cyber security associated with terms such as deep learning, malware, artificial intelligence, or risk assessment. The articles in this cluster are focused on topics related to deep learning, malware (malicious programs), artificial intelligence and risk assessment. This cluster has the greatest impact of the two identified.

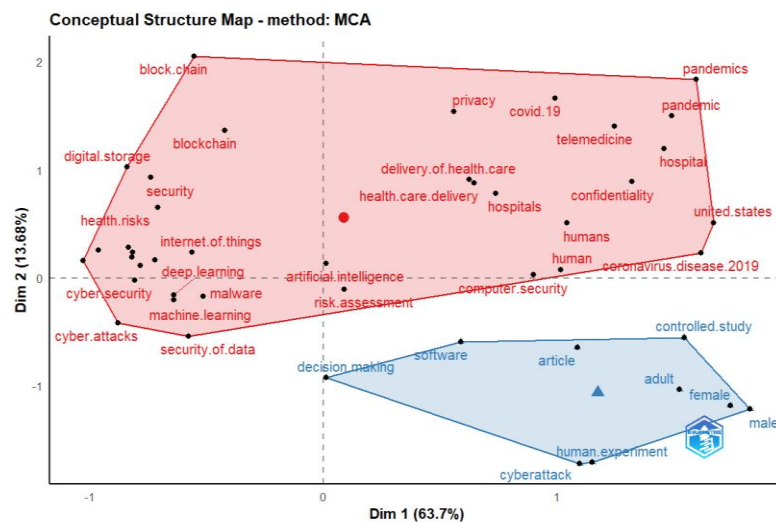


Figure 3. Factor analysis-multiple correspondence

4. DISCUSSIONS

This systematic literature review aims to answer the questions proposed under the different contributions and results of the authors. Question by question will be analyzed in depth. This makes the research more consolidated.

4.1. Analysis of the questions

4.1.1. What are the emerging technologies that most influence the healthcare sector?

Recent technological advances over the years have been transforming, the authors mention that they are becoming more personalized and based on the artificial intelligence applied in sensors [8], [9]. Likewise, the author mentions that artificial intelligence and the internet of medical things (IoMT) are one of the most promising technologies that help in the analysis of disease detection and results being of great help to medical professionals [10], [11]. On the other hand, the authors mention that there are a variety of technologies

emerging in the health sector, but few of them have protocols and efficient infrastructure. One of the technologies they emphasize the most is sensors based on artificial intelligence, which is the most used in clinical environments, since they reduce the need for routine measurements to be performed on patients [12]–[14]. On the other hand, the authors mention that medical device data sheets (MDIDS) document and characterize medical device data, highlighting it as an important technology that supports customer safety and innovation in the medical field, launching it as the next generation of the IoT [15].

The authors mention that artificial intelligence, wireless technology, cloud networking, and robotics are emerging technologies such as machine learning, the authors centralize these technologies to aid in symptom detection and quarantine tracking [16]–[18]. Among other technologies the authors mention NanoThing which are tiny bio-electrical devices that can be used in health monitoring and drug delivery [19]. The authors mention that the IoMT is the technology with the greatest impact as it systematically combines technologies such as augmented reality, and remote surgical that significantly improve these technologies that are influential in the health sector [20]. Well, in recent years, the authors mention that in the wake of the pandemic many people who were against and in favor of vaccines expressed their opinions through social networks, so the Pfizer-BioTech software was launched to assess social cyber behaviors so that through policies can reduce the size of anti-vaccine communities being a benefit to the health of people [21], [22]. According to the authors, a variety of technologies are presented in the health sector where most authors mention artificial intelligence as the main technology for the health sector as shown in Figure 3 demonstrating that cybersecurity is related to artificial intelligence.

4.1.2. What are the most frequent cyberattacks in the healthcare sector?

The authors mention that due to the COVID-19 pandemic, work had to be moved from face-to-face to remote, which generated an increase in cybercrime. The increase in the recession and the emission of e-mails was the cause of the phishing attack, which was a great threat to the data and infrastructure of the health sector [22]–[25]. On the other hand, the authors detail that most cyber-attacks are on medical equipment for which it is important to have a professional to manage security threats [23], [26]. They also mention that cyber-attacks increased due to poor electronic health record (HER) implementation and the COVID-19 pandemic as there was an increase in personal data breaches [27]. Therefore, the authors mention that one of the most frequent cyber-attacks are phishing attacks, to spread ransomware, where these criminals block the hospital servers and the measured infrastructure, as most of these hackers demand ransom for the stolen confidential data, which are not always successful [28]–[32].

To this day ransomware has been affecting considerably in the health sector, these cybercriminals block the communication of medical devices that are being used, and these medical equipment are the ones with more vulnerability to attacks despite their importance to save lives [22], [33]–[35], have also led to the interruption of different scenarios such as the radiotherapies of thousands of patients, mostly on the impact of COVID-19 [36]–[38]. Similarly, the authors mention that there are numerous security concerns, such as denial of service, spoofing, and remote hijacking, these cyber-attacks are associated with internet connectivity in medical things, and such devices mostly have security and privacy issues as they have very limited computing power [39], [40]. According to the authors, it is shown that cyber-attacks were carried out more frequently when COVID-19 emerged, taking advantage of the concern of citizens and the changes in working modalities, so the most frequent attacks are through phishing and ransomware, which most articles they mention.

4.1.3. What technologies are immersed in the healthcare sector to address cybersecurity?

Medical organizations face a battle in protecting their systems and digital equipment against a variety of cyber threats [41]–[43]. Because of this, the authors mention that blockchain technology preserves the security and privacy of data against cyber-attacks, this technology is based on a blockchain [44]–[51] this technology comprises several nodes which hide confidential information of the organization and prevents them from being disclosed to malicious nodes [52]–[56] advanced encryption and has a rapid response plan for such incidents [57]–[59], he blockchain alerts to any possible cyber-attack by preventing hackers from altering the stored information [60]–[65]. On the other hand, the authors recommend the ontology tool that is equipped with rules, classifying security threats and automatically recommending controls that can be applied in the face of a threat [66], [67]. Other authors mention a neural network with artificial intelligence to perform queries and transfers of medical data in a secure way [68]–[71]. On the other hand, the author mentions that the defender software is a health industry computer network that goes against attacks, these network topologies are attractive that protect the information in real-time [72]–[74].

The author mentions the attack occurrence probability (AOP) which are programs that guarantee the reliability and security of medical equipment, this tool works under the Fennigkoh and Smith model and performs a preventive maintenance calculation against cyber-attack threats [75]–[78]. On the other hand, the author proposes a light gradient boosting machine (LightGBM) model software that is trained with different knowledge of attacks that can affect the medical organization [79], [80]. We agree with the authors as all these

tools are useful to address cybersecurity, to be able to implement diagnostic evaluations and to safeguard confidential data and medical equipment that are of useful importance for human life [81]. As shown in Figure 4 blockchain is shown as the second most frequently mentioned topic by the authors after cybersecurity.

4.2. Information security model proposal

As shown in Figure 4, a blockchain-based information hiding techniques (IHT) framework architecture has been proposed which has been divided into four main layers: i) healthcare IoT device layer; ii) edge layer; iii) fog layer finally; and iv) cloud layer. According to Figure 4, the IoT layer focuses on providing greater security. Hospitals in general and medical laboratories in particular process a large amount of data on cloud servers to find the results they are looking for. This information is typically sent from the lab to the cloud server through traditional channels and using basic encryption methods. At the edge layer, a private blockchain ledger was placed for secure selection and authentication. The base station plays the role of the administrator of the blockchain and must verify the identity, authenticate the user, and register the user in the ledger to provide a faster authentication mechanism in the future. Device users and their respective cloud servers must also register with the blockchain and agree to a unique hash key that will be stored on the blockchain for further encryption. In the fog layer, which is where several high-performance servers are composed, smart contracts are generated between device users and servers in the cloud. Additionally, secret messages and helper bits are also encrypted to confuse an attacker in the event of a cyber attack. Multiple distributed servers are located in the cloud, where their role is to process the information received after decrypting it using a previously agreed hash key.

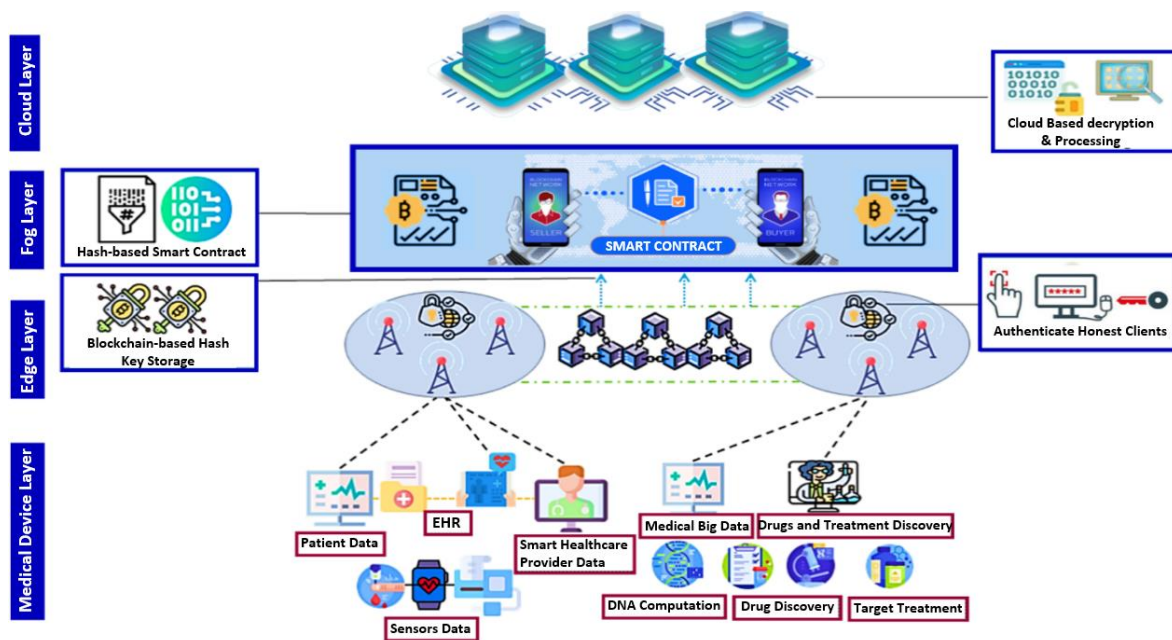


Figure 4. Proposed blockchain-based blockchain architecture

5. CONCLUSION

With the use of the systematic review of the literature with 71 articles related to the mentioned topic, it is concluded that the most emerging technologies in the health sector that help to protect human lives are artificial intelligence, IoMT and sensors since according to the articles found these technologies have a greater representation in those in medical devices. Likewise, most of the authors in their articles mention that the most used cyberattacks by cybercriminals are phishing and ransomware. These attacks, as mentioned by the authors, had a greater increase during the COVID-19 pandemic, experiencing a greater number of data breaches and interruptions in their medical equipment, which generated heavy expenses for the medical industry. Regarding the technological tools to face cybersecurity, the most mentioned and recommended by the authors is the blockchain since it allows good management of information, and increases the security and reliability of patient data and medical equipment. This tool is composed of nodes that through them travel linked and encrypted blocks whose objective is to increase the protection of data, as well as their privacy. It was also concluded that

the countries with more researchers in the last 5 years that are related to the topic of cybersecurity in the health sector are the United States of America (USA) followed by Canada.

Finally, a proposed model based on blockchain was proposed which promises greater security and privacy of data in the intelligent medical field and less time in the execution of procedures. Blockchain in turn creates a secure smart contract with its providers, as for information hiding techniques that have resulted in several advanced techniques to hide confidential information and prevent it from leaking to malicious nodes, IHT helps to protect the privacy and authenticity of communication messages, data files and even electronic contracts between companies.

REFERENCES




- [1] S. A. Olofinbiyi, "Cyber insecurity in the wake of COVID-19: a reappraisal of impacts and global experience within the context of routine activity theory," *ScienceRise: Juridical Science*, no. 1(19), pp. 37–45, Mar. 2022, doi: 10.15587/2523-4153.2022.253820.
- [2] L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," *Frontiers in Digital Health*, vol. 4, Aug. 2022, doi: 10.3389/fdgh.2022.862221.
- [3] J. Buzzio-García, V. Salazar-Vilchez, J. Moreno-Torres, and O. Leon-Estofanero, "Review of cybersecurity in Latin America during the Covid-19 pandemic. a brief overview," in *ETCM 2021 - 5th Ecuador Technical Chapters Meeting*, Oct. 2021, pp. 1–5, doi: 10.1109/ETCM53643.2021.9590693.
- [4] C. J. S. Rubio, G. G. Villacorta, J. O. Choque, and J. Armas-Aguirre, "Personal health data: a security capabilities model to prevent data leakage in big data environments," in *Iberian Conference on Information Systems and Technologies, CISTI*, Jun. 2022, vol. 2022-June, pp. 1–6, doi: 10.23919/CISTI54924.2022.9820432.
- [5] M. Quimiz-Moreira, W. Zambrano-Romero, C. Moreira-Zambrano, M. Mendoza-Zambrano, and E. Cedeño-Palma, "Cybersecurity mechanisms for information security in patients of public hospitals in Ecuador," in *Lecture Notes in Networks and Systems*, vol. 407 LNNS, 2022, pp. 211–224, doi: 10.1007/978-3-030-96147-3_17.
- [6] B. Barnes and T. Daim, "Information security maturity model for healthcare organizations in the United States," *IEEE Transactions on Engineering Management*, pp. 1–12, 2022, doi: 10.1109/TEM.2021.3139836.
- [7] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *Systematic Reviews*, vol. 10, no. 1, p. 89, 2021, doi: 10.1186/s13643-021-01626-4.
- [8] N. Taimoor and S. Rehman, "Reliable and resilient ai and IoT-based personalised healthcare services: a survey," *IEEE Access*, vol. 10, pp. 535–563, 2022, doi: 10.1109/ACCESS.2021.3137364.
- [9] M. Jofre *et al.*, "Cybersecurity and privacy risk assessment of point-of-care systems in healthcare—a use case approach," *Applied Sciences (Switzerland)*, vol. 11, no. 15, p. 6699, Jul. 2021, doi: 10.3390/app11156699.
- [10] K. S. Alqudaihi *et al.*, "Cough sound detection and diagnosis using artificial intelligence techniques: challenges and opportunities," *IEEE Access*, vol. 9, pp. 102327–102344, 2021, doi: 10.1109/ACCESS.2021.3097559.
- [11] D. Johansson, P. Jönsson, B. Ivarsson, and M. Christiansson, "Information technology and medical technology personnel's perception regarding segmentation of medical devices: A focus group study," *Healthcare (Switzerland)*, vol. 8, no. 1, p. 23, Jan. 2020, doi: 10.3390/healthcare8010023.
- [12] J. M. Goldman, S. Weininger, and M. B. Jaffe, "Applying medical device informatics to enable safe and secure interoperable systems: Medical device interface data sheets," *Anesthesia and Analgesia*, vol. 131, no. 3, pp. 969–976, Sep. 2020, doi: 10.1213/ANE.0000000000004251.
- [13] A. Al-Mawali, A. D. Pinto, and A. T. Al-Hinai, "Medical equipment and healthcare technology: Health Vision 2050," *Biomedical Instrumentation and Technology*, vol. 52, no. 6, pp. 442–450, Nov. 2018, doi: 10.2345/0899-8205-52.6.442.
- [14] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare internet of things (HIoT): a clinical perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 53–71, Jan. 2020, doi: 10.1109/JIOT.2019.2946359.
- [15] J. B. Lujan, K. E. Tume, M. G. Retuerto, and L. Andrade-Arenas, "Telemedicine prototype to improve medical care and patient and physician safety in Lima-Peru," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 83–96, Aug. 2022, doi: 10.14445/22315381/IJETT-V70I8P208.
- [16] C. T. Nguyen *et al.*, "A comprehensive survey of enabling and emerging technologies for social distancing-part ii: emerging technologies and open issues," *IEEE Access*, vol. 8, pp. 154209–154236, 2020, doi: 10.1109/ACCESS.2020.3018124.
- [17] M. Baz, H. Alhakami, A. Agrawal, A. Baz, and R. A. Khan, "Impact of covid-19 pandemic: A cybersecurity perspective," *Intelligent Automation and Soft Computing*, vol. 27, no. 3, pp. 641–652, 2021, doi: 10.32604/IASC.2021.015845.
- [18] L. Monoscalco, R. Simeoni, G. Maccioni, and D. Giansanti, "Information security in medical robotics: a survey on the level of training, awareness and use of the physiotherapist," *Healthcare (Switzerland)*, vol. 10, no. 1, p. 159, Jan. 2022, doi: 10.3390/healthcare10010159.
- [19] S. Zafar *et al.*, "A systematic review of bio-cyber interface technologies and security issues for internet of bio-nano things," *IEEE Access*, vol. 9, pp. 93529–93566, 2021, doi: 10.1109/ACCESS.2021.3093442.
- [20] Y. Tai, B. Gao, Q. Li, Z. Yu, C. Zhu, and V. Chang, "Trustworthy and intelligent COVID-19 diagnostic IoMT through XR and deep-learning-based clinic data access," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15965–15976, Nov. 2021, doi: 10.1109/JIOT.2021.3055804.
- [21] J. T. Blane, D. Bellutta, and K. M. Carley, "Social-cyber maneuvers during the COVID-19 vaccine initial rollout: content analysis of tweets," *Journal of Medical Internet Research*, vol. 24, no. 3, p. e34040, Mar. 2022, doi: 10.2196/34040.
- [22] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Digital healthcare-cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations," *IEEE Access*, vol. 10, pp. 12345–12364, 2022, doi: 10.1109/ACCESS.2022.3145372.
- [23] N. Lewis, Y. Connelly, G. Henkin, M. Leibovich, and A. Akavia, "Factors influencing the adoption of advanced cryptographic techniques for data protection of patient medical records," *Healthcare Informatics Research*, vol. 28, no. 2, pp. 132–142, Apr. 2022, doi: 10.4258/hir.2022.28.2.132.
- [24] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? survey, taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134–124144, 2020, doi: 10.1109/ACCESS.2020.3006172.

- [25] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, "Phishing simulation exercise in a large hospital: A case study," *Digital Health*, vol. 8, p. 205520762210817, Jan. 2022, doi: 10.1177/20552076221081716.
- [26] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, "Towards design and development of security assessment framework for internet of medical things," *Applied Sciences (Switzerland)*, vol. 12, no. 16, p. 8148, Aug. 2022, doi: 10.3390/app12168148.
- [27] I. C. A. Pilares, S. Azam, S. Akbulut, M. Jonkman, and B. Shanmugam, "Addressing the challenges of electronic health records using blockchain and IPFS," *Sensors*, vol. 22, no. 11, p. 4032, May 2022, doi: 10.3390/s22114032.
- [28] H. Ghayoomi, K. Laskey, E. Miller-Hooks, C. Hooks, and M. Tariverdi, "Assessing resilience of hospitals to cyberattack," *Digital Health*, vol. 7, p. 205520762110593, Jan. 2021, doi: 10.1177/20552076211059366.
- [29] S. Manghani, "Cybersecurity challenges in ensuring patient safety in global digital healthcare," *Nanotechnology Perceptions*, vol. 17, no. 1, pp. 19–22, Apr. 2021, doi: 10.4024/N24MA20A.ntp.17.01.
- [30] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.
- [31] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research problems," *Computers and Security*, vol. 111, p. 102490, Dec. 2021, doi: 10.1016/j.cose.2021.102490.
- [32] M. T. Jafar, M. Al-Fawareh, M. Barhoush, and M. H. Alshira'H, "Enhanced analysis approach to detect phishing attacks during COVID-19 crisis," *Cybernetics and Information Technologies*, vol. 22, no. 1, pp. 60–76, Mar. 2022, doi: 10.2478/cait-2022-0004.
- [33] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity protection for PACS and medical imaging: deployment considerations and practical problems," *Academic Radiology*, vol. 28, no. 12, pp. 1761–1774, Dec. 2021, doi: 10.1016/j.acra.2020.09.001.
- [34] A. Bobbio, L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "A cyber warfare perspective on risks related to health IoT devices and contact tracing," *Neural Computing and Applications*, Jan. 2022, doi: 10.1007/s00521-021-06720-1.
- [35] P. Radanliev and D. De Roure, "Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptive artificial intelligence (part 2)," *Health and Technology*, vol. 12, no. 5, pp. 923–929, Sep. 2022, doi: 10.1007/s12553-022-00691-6.
- [36] C. Joyce, F. L. Roman, B. Miller, J. Jeffries, and R. C. Miller, "Emerging cybersecurity threats in radiation oncology," *Advances in Radiation Oncology*, vol. 6, no. 6, p. 100796, Nov. 2021, doi: 10.1016/j.adro.2021.100796.
- [37] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers and Security*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.
- [38] D. Giansanti and L. Monoscalco, "The cyber-risk in cardiology: Towards an investigation on the self-perception among the cardiologists," *mHealth*, vol. 7, pp. 28–28, Apr. 2021, doi: 10.21037/mhealth.2020.01.08.
- [39] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021, doi: 10.1109/ACCESS.2021.3128837.
- [40] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: a survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
- [41] A. Agrawal *et al.*, "Evaluating the security impact of healthcare web applications through fuzzy based hybrid approach of multi-criteria decision-making analysis," *IEEE Access*, vol. 8, pp. 135770–135783, 2020, doi: 10.1109/ACCESS.2020.3010729.
- [42] G. Maccioni and D. Giansanti, "Medical apps and the gray zone in the covid-19 era: Between evidence and new needs for cybersecurity expansion," *Healthcare (Switzerland)*, vol. 9, no. 4, p. 430, Apr. 2021, doi: 10.3390/healthcare9040430.
- [43] F. Gioulekas *et al.*, "A cybersecurity culture survey targeting healthcare critical infrastructures," *Healthcare*, vol. 10, no. 2, p. 327, Feb. 2022, doi: 10.3390/healthcare10020327.
- [44] A. Kumar *et al.*, "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol. 22, no. 15, p. 5921, Aug. 2022, doi: 10.3390/s22155921.
- [45] D. Hawashin *et al.*, "Blockchain-based management of blood donation," *IEEE Access*, vol. 9, pp. 163016–163032, 2021, doi: 10.1109/ACCESS.2021.3133953.
- [46] C. Qin, L. Wu, W. Meng, Z. Xu, S. Li, and H. Wang, "A privacy-preserving blockchain-based tracing model for virus-infected people in cloud," *Expert Systems with Applications*, vol. 211, p. 118545, Jan. 2023, doi: 10.1016/j.eswa.2022.118545.
- [47] F. Firouzi *et al.*, "Fusion of IoT, AI, edge-fog-cloud, and blockchain: challenges, solutions, and a case study in healthcare and medicine," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 3686–3705, Mar. 2023, doi: 10.1109/JIOT.2022.3191881.
- [48] O. Filipec and D. Plášilb, "The cybersecurity of healthcare the case of the bešeňov hospital hit by ryuk ransomware, and lessons learned," *Obrana a Strategie*, vol. 21, no. 1, pp. 27–51, Jun. 2021, doi: 10.3849/1802-7199.21.2021.01.027-052.
- [49] F. Ö. Sönmez, C. Hankin, and P. Malacaria, "Decision support for healthcare cyber security," *Computers and Security*, vol. 122, p. 102865, Nov. 2022, doi: 10.1016/j.cose.2022.102865.
- [50] S. Barbaria, M. C. Mont, E. Ghadafi, H. M. Machraoui, and H. B. Rahmouni, "Leveraging patient information sharing using blockchain-based distributed networks," *IEEE Access*, vol. 10, pp. 106334–106351, 2022, doi: 10.1109/ACCESS.2022.3206046.
- [51] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq, and K. K. Wong, "Thinking out of the blocks: holochain for distributed security in iot healthcare," *IEEE Access*, vol. 10, pp. 37064–37081, 2022, doi: 10.1109/ACCESS.2022.3163580.
- [52] A. Al-Mamun, S. Azam, and C. Gritti, "Blockchain-based electronic health records management: a comprehensive review and future research direction," *IEEE Access*, vol. 10, pp. 5768–5789, 2022, doi: 10.1109/ACCESS.2022.3141079.
- [53] A. El-Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems," *Sensors*, vol. 22, no. 4, p. 1371, Feb. 2022, doi: 10.3390/s22041371.
- [54] F. Z. Hannou *et al.*, "Semantic-based approach for cyber-physical cascading effects within healthcare infrastructures," *IEEE Access*, vol. 10, pp. 53398–53417, 2022, doi: 10.1109/ACCESS.2022.3171252.
- [55] L. C. Ruiz, M. L. Amado, J. R. Carrasco, and L. Andrade-Arenas, "Implementation of information security audit for the sales system in a peruvian company," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, no. 3, p. 1189, Jun. 2022, doi: 10.18517/ijaseit.12.3.13969.
- [56] Y. Li, J. Yang, Z. Zhang, J. Wen, and P. Kumar, "Healthcare data quality assessment for cybersecurity intelligence," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 841–848, Jan. 2023, doi: 10.1109/TII.2022.3190405.
- [57] M. H. Chinaei, H. H. Gharakheili, and V. Sivaraman, "Optimal witnessing of healthcare IoT data using blockchain logging contract," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10117–10130, Jun. 2021, doi: 10.1109/JIOT.2021.3051433.
- [58] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019, doi: 10.1109/ACCESS.2019.2947613.
- [59] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating procurement contracts in the healthcare supply chain using blockchain smart contracts," *IEEE Access*, vol. 9, pp. 37397–37409, 2021, doi: 10.1109/ACCESS.2021.3062471.




- [60] I. A. Omar, M. Debe, R. Jayaraman, K. Salah, M. Omar, and J. Arshad, "Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment," *Computers and Industrial Engineering*, vol. 167, p. 107995, May 2022, doi: 10.1016/j.cie.2022.107995.
- [61] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Threat modeling and risk analysis for miniaturized wireless biomedical devices," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13338–13352, Aug. 2022, doi: 10.1109/IIOT.2022.3144130.
- [62] F. H. Semantha, S. Azam, B. Shanmugam, K. C. Yeo, and A. R. Beeravolu, "A conceptual framework to ensure privacy in patient record management system," *IEEE Access*, vol. 9, pp. 165667–165689, 2021, doi: 10.1109/ACCESS.2021.3134873.
- [63] L. A. Maggio, C. Dameff, S. L. Kanter, B. Woods, and J. Tully, "Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives," *Academic Medicine*, vol. 96, no. 6, pp. 850–853, Jun. 2021, doi: 10.1097/ACM.0000000000003859.
- [64] S. Y. Shea, J. L. Hick, S. Schwedhelm, and L. M. Sauer, "Opportunity among disaster: reflecting on 2 disaster scenarios during the COVID-19 pandemic," *Health Security*, vol. 20, no. S1, pp. S49–S53, Jun. 2022, doi: 10.1089/hs.2021.0192.
- [65] A. Georgiadou *et al.*, "Hospitals' cybersecurity culture during the COVID-19 crisis," *Healthcare (Switzerland)*, vol. 9, no. 10, p. 1335, Oct. 2021, doi: 10.3390/healthcare9101335.
- [66] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-based security recommendation for the internet of medical things," *IEEE Access*, vol. 7, pp. 48948–48960, 2019, doi: 10.1109/ACCESS.2019.2910087.
- [67] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law and Security Review*, vol. 41, p. 105528, Jul. 2021, doi: 10.1016/j.clsr.2021.105528.
- [68] K. Vijayakumar *et al.*, "Intelligence-based network security system to predict the possible threats in healthcare data," *Security and Communication Networks*, vol. 2022, pp. 1–12, May 2022, doi: 10.1155/2022/6716370.
- [69] C. Tselios *et al.*, "Melding fog computing and IoT for deploying secure, response-capable healthcare services in 5G and beyond," *Sensors*, vol. 22, no. 9, p. 3375, Apr. 2022, doi: 10.3390/s22093375.
- [70] Y. M. Dalmat, "Avec le coronavirus, alerte aux infox et aux cyberattaques," *Option/Bio*, vol. 32, no. 647–648, p. 13, Mar. 2022, doi: 10.1016/S0992-5945(22)00046-0.
- [71] B. I. I. Aljidi, S. Perumal, and S. A. Pitchay, "Securing data using deep hiding selected least significant bit and adaptive swarm algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 28, no. 3, pp. 1573–1581, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1573-1581.
- [72] D. Angel, "Application of graph domination to defend medical information networks against cyber threats," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 8, pp. 3765–3770, Aug. 2022, doi: 10.1007/s12652-022-03730-2.
- [73] J. M. Idme, J. L. V. Garcia, S. A. H. Morales, and L. Andrade-Arenas, "The implementation of information security for the inventory system in a municipality of Lima-Perú," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, no. 1, pp. 101–113, Jan. 2022, doi: 10.18517/ijaseit.12.1.13914.
- [74] A. Estepa, R. Estepa, G. Madinabeitia, and J. Vozmediano, "Designing cost-effective reliable networks from a risk analysis perspective: a case study for a Hospital Campus," *IEEE Access*, vol. 7, pp. 120411–120423, 2019, doi: 10.1109/ACCESS.2019.2937449.
- [75] D. W. Kim, J. Y. Choi, and K. H. Han, "Medical device safety management using cybersecurity risk analysis," *IEEE Access*, vol. 8, pp. 115370–115382, 2020, doi: 10.1109/ACCESS.2020.3003032.
- [76] H. Alhakami, A. Baz, W. Alhakami, A. K. Pandey, A. Agrawal, and R. A. Khan, "A usability management framework for securing healthcare information system," *Computer Systems Science and Engineering*, vol. 42, no. 3, pp. 1015–1030, 2022, doi: 10.32604/csse.2022.021564.
- [77] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, "Risk assessment methodologies for the internet of medical things: a survey and comparative appraisal," *IEEE Access*, vol. 9, pp. 40049–40075, 2021, doi: 10.1109/ACCESS.2021.3064682.
- [78] D. Markopoulou and V. Papakonstantinou, "The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular," *Computer Law and Security Review*, vol. 41, p. 105502, Jul. 2021, doi: 10.1016/j.clsr.2020.105502.
- [79] M. Azzeh, A. M. Altamimi, M. Albashayreh, and M. A. Al-Oudat, "Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 25, no. 3, pp. 1749–1758, Mar. 2022, doi: 10.11591/ijeecs.v25.i3.pp1749-1758.
- [80] A. K. Ahmed and A. A. Khorsheed, "Open network structure and smart network to sharing cybersecurity within the 5G network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 573–582, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp573-582.
- [81] T. Poleto *et al.*, "Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services," *Healthcare (Switzerland)*, vol. 9, no. 11, p. 1504, Nov. 2021, doi: 10.3390/healthcare9111504.

BIOGRAPHIES OF AUTHORS






Catherine Vanessa Peve Herrera    is graduated from the systems engineering and computer science career at Norbert Wiener University, systems practitioner as a professional development; great interest in current issues and research on them, obtaining knowledge for the writing of articles through method since it is of vital importance for the development of science. She can be contacted at email: catherin.99.pv@gmail.com.






Jonathan Steve Mendoza Valcarcel    is a student 10th cycle at the Norbert Wiener University, Born in Lima, Peru in 1998. He is currently a system engineering and computer science student interested in researching different topics such as cybersecurity among other topics related to the systems career. He can be contacted at email: jonamendo293@gmail.com.






Mónica Díaz    is Computer and Systems Engineer from USMP. She have completed studies of the master's degree in systems engineering at UNFV. She also have a master's degree in education with a mention in computer science and educational technology in USMP. She also have a Ph.D. in education from the USMP. She is currently in the fourth cycle of the Ph.D. in systems engineering at UNFV. She work as a teacher at various universities. She is also an undergraduate and postgraduate thesis advisor in education and systems engineering. She can be contacted at email: monica.diaz@uwiener.edu.pe.



Jose Luis Herrera Salazar    is a professional in systems engineering with experience in planning, analysis, design, and programming of computer systems and databases. Developed of equipment maintenance management systems, attendance control systems, warehouse control systems, production systems, and academic systems. He can be contacted at email luis.herrera@autonomadeica.edu.pe.



Laberiano Andrade-Arenas    is doctor in systems and computer engineering. Master in Systems Engineering. Graduated from the master's degree in University Teaching. Graduated from the master's degree in accreditation and evaluation of educational quality. Systems engineer ITILV3 fundamentals international course (Zonngo-Peru/IMLAD-Mexico) scrum fundamentals certified. He can be contacted at email: landradearenas@gmail.com.