A critical review of the state of computer security in the health sector

Raúl Jáuregui-Velarde[1], Domingo Hernández Celis[2], Cesar Yactayo Arias[3], Laberiano Andrade-Arenas[4]
[1]Facultad de Ingeniería y Negocios, Universidad Privada Norbert Wiener, Lima, Perú
[2]Facultad de Ciencias Financieras y Contables, Universidad Nacional Federico Villarreal, Lima, Perú
[3]Departamento de Estudios Generales, Universidad Continental, Lima, Perú
[4]Facultad de Ciencias e Ingeniería, Universidad de Ciencias y Humanidades, Lima, Perú

Article Info

Article history:

Received Dec 3, 2022
Revised May 12, 2023
Accepted Jul 14, 2023

Keywords:

Blockchain
Computer security
Health sector
Healthcare
Information security

ABSTRACT

There is growing concern about IT security in the healthcare sector due to the number of cyberattacks. The objective of the review is to analyze the state of adoption of computer security in the healthcare sector and provide valuable knowledge to researchers and health organizations interested in this field of study. An exhaustive search of international and regional articles on computer security in healthcare organizations was conducted using Scopus, Dimensions, and pubMed databases. Preferred reporting items for systematic reviews and meta-analysis (PRISMA) statement was used for the selection of articles published between 2018 and 2022. The final number of articles considered is 50. The review explored approaches related to computer security types, mechanisms, and technologies. The findings reveal that blockchain is the most widely used technology to protect medical information. In addition, network, software, and hardware security approaches are employed, using mechanisms such as data encryption, authentication, and access control. Based on these findings, a perimeter security model for the protection of medical information is proposed. In conclusion, these results highlight the importance of adopting robust security measures in terms of networks, software, and hardware, as well as adopting blockchain technology to improve data security in the healthcare sector.

Corresponding Author:

Laberiano Andrade-Arenas
Facultad de Ciencias e Ingeniería, Universidad de Ciencias y Humanidades
Lima, Perú
Email: landrade@uch.edu.pe

1. INTRODUCTION

Worldwide concern about computer security, or cybersecurity, in information technology has increased due to the growing number of cyberattacks on various organizations. The healthcare sector is not exempt from this problem, as sensitive data is currently handled on electronic devices. In this sense, Sönmez *et al*. [1] state that during the pandemic, health systems became the main targets of cybercriminals, which is a constant challenge in the search for optimal security for health organizations. It is important to note that the COVID-19 pandemic has forced healthcare organizations around the world to adopt telemedicine, or telehealth, as a form of care. However, the security standards implemented in the information systems are inadequate or low, making them vulnerable to computer attacks, especially in developing countries.

Likewise, the COVID-19 pandemic has underscored the necessity for Latin American nations to embrace information and communication technologies (ICT) in order to address the hurdles associated with advancing digital healthcare. In this context, Costa *et al.* [2] affirm that computer security has become essential due to the increase in the use of information technologies (IT), the growth of internet access, and the emergence of new technologies such as the internet of things (IoT). This has led to increased use, data transfer over internet networks, and storage of information on servers and in the cloud. However, the massive use of ICT has also exposed users and organizations to cyberattacks [3]. This means that once cybercriminals can infiltrate and gain access to patient data, they are able to sell it for identity theft purposes or demand a ransom to recover it. Therefore, there is a growing concern and need for information security in Latin America to ensure the availability, privacy, and integrity of information.

Healthcare organizations store private patient information, including diagnoses and medical records. However, with the use of ICT, networked systems and devices become vulnerable, and data is exposed. The need to ensure a secure and reliable healthcare system is a fundamental priority, highlighting the importance of protecting the privacy and confidentiality of patient’s medical information [4], [5]. To achieve optimal security, it is essential to know the forms or types of computer security. In addition, computer security is constantly evolving due to the increase in threats in the digital environment and is vital for many healthcare organizations that are increasingly dependent on computer systems. Therefore, the continuous development and adoption of security is a must for the healthcare sector.

Therefore, this systematic review of the literature (SRL) aims to provide useful knowledge to other researchers and health organizations interested in this field of study to help them gain a better understanding and perspective on the forms of computer security adaptations to improve the security and maintain the integrity of medical data. In addition, this review proposes improvements and added information security measures in information systems in the health sector based on different approaches to information security extracted from the review of international and regional articles. Because of the development of new IT, remote medical care and the storage of patient information in information systems are increasing, making health systems more vulnerable to computer attacks [6]. Therefore, improving and increasing computer security measures is of vital importance to maintaining the availability, privacy, and integrity of information stored in information systems.

2. METHOD

Explaining the research involves conducting a SRL specifically focused on computer security in the healthcare industry. The study aims to explore and analyze the existing literature related to this specific area. To ensure rigor and transparency in the review process, the preferred reporting items for systematic reviews and meta-analysis (PRISMA) methodology will be used. This systematic approach facilitates the identification and selection of the most relevant articles from various databases and allows for the inclusion of high-quality studies that contribute to the understanding of computer security in healthcare. By using the PRISMA methodology, the research provides a comprehensive, evidence-based analysis of the current state of healthcare IT security and contributes to the development of effective strategies for protecting the industry's sensitive information. In addition, a bibliometric analysis is carried out to identify the terms that have the greatest influence on the implementation of IT security in the healthcare sector. The research structure is described in detail below.

2.1. Definition of research questions

The SRL encompasses the scope of peer-reviewed research through extensive classification and analysis of already existing related publications. The first step is to define the research questions to understand the coverage of existing works accurately. By examining related works, insights are gained that can help researchers develop new insights or ideas [7]. Table 1 presents the research questions used in this SLR, each of which is identified with the acronym research questions (RQ).

Table 1. Research questions

Id	Questions
RQ1	What types of computer security are implemented for the protection of information in the health sector?
RQ2	What computer security mechanisms are most commonly implemented in the health sector?
RQ3	What are the technologies used to strengthen computer security in the health sector?

2.2. Holistic analysis

At this stage, both a generic and a specific analysis of the search for information was carried out. A combination of Boolean operators was used. To carry out this analysis, the use of a database was required, so the analysis of several databases to be used, such as Scopus, Dimensions, Science Direct, and pubMed, was performed. After the analysis process, the Scopus, Dimensions, and pubMed databases were selected. Scopus is recognized as one of the largest open-access databases in the world. Dimensions and pubMed are also open-access databases that contain bibliographic abstracts of international research. On the other hand, it was decided to discard Science Direct to avoid duplication of information, as this platform, like Scopus, is owned by Elsevier.

2.3. Search strategy

2.3.1. Generic search

First, an extensive search was conducted to collect a diverse selection of articles relevant to the topic. This bibliometric search provides a comprehensive assessment of the current state of computer security, the primary variable, at both international and regional levels. Additionally, it facilitates the identification of various characteristics, including the countries with the highest research productivity in the field, commonly used keywords, co-occurrence patterns, and other significant factors. To carry out this search, the Scopus database was used, which combines quality and a large amount of metadata. Keywords such as computer security and the health sector were used, which resulted in the obtaining of 2,730 articles. These were exported to tools such as VOSviewer and Bibliometrix using the R programming language and its RStudio development environment, which allowed for an exhaustive analysis.

2.3.2. Specific search

Once the research questions were formulated, a specific search was conducted using parameters to filter the results for information related to the topic. This search was carried out using Boolean equations. Searches were conducted in different databases: i) Scopus, where the search was performed by title, abstract, and keywords; ii) Dimensions, where the search was performed by title and abstract; and iii) pubMed, by title and abstract. The Boolean equation used was as follows: (("computer security" OR "cybersecurity" OR "privacy" OR "data security") AND ("health" OR "health sector" OR “hospital”)).

2.4. Inclusion and exclusion criteria

The inclusion and exclusion criteria in SRL are essential to ensuring rigor and consistency in the selection of studies to be analyzed. These criteria set clear limits on the types of studies and the interventions or phenomena of interest that are considered. They also help to establish a transparent and reproducible process that improves the quality and validity of the results obtained in the review. Table 2 shows the inclusion criteria used to select articles, while Table 3 shows the exclusion criteria used.

Table 2. Inclusion criteria

Id	Inclusion
IC1	Articles related to computer security in the health sector
IC2	Articles that consider at least cybersecurity, information security or data security parameters in the health sector
IC3	Articles published between 2018 and 2022
IC4	Open access articles
IC5	Articles written in English

Table 3. Exclusion criteria

Id	Exclusion
EC1	Articles that do not respond to the research question
EC2	Articles elaborated in contexts other than health
EC3	Articles due to lack of results of interest

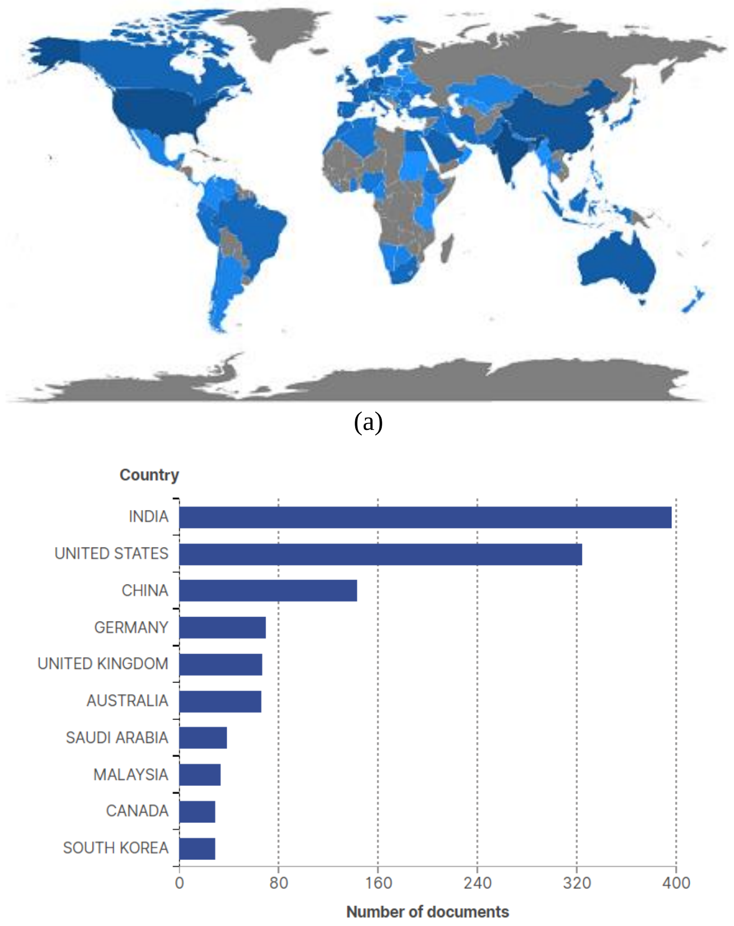
3. RESULTS AND DISCUSSION

This systematic review aims to provide valuable knowledge to researchers and health organizations interested in the area of study through a comprehensive analysis of the various contributions and results of the authors. To achieve this objective, an analysis is carried out at two levels: a general one, which covers a broad panorama of the existing literature, and a specific one, which delves into aspects relevant to the understanding of the subject. In this way, it aims to provide a complete and detailed vision that allows for a better understanding.

3.1. About the generic search

3.1.1. Scientific production

Figure 1(a) shows that, in terms of scientific production related to health computer security by continent, Europe is the continent with the highest number of publications. This means that there is a greater amount of research, scientific articles, or academic papers published on this continent compared to other continents. It is followed by the Americas and Asia, which implies that there is also a significant amount of research related to the field of health computer security. Meanwhile, Figure 1(b) shows the top 10 countries with the highest number of publications. The top three countries in terms of the number of publications are India, the United States, and China. India ranks first with more than 350 publications, indicating that this country has outstanding activity in research and publication of studies related to computer security in the health sector. The United States ranks second with more than 300 publications, and China ranks third with more than 100 publications, indicating a strong focus on health IT security in these countries. These results show that India, the United States, and China are leaders in the research and publication of studies on health computer security. This could be an indication that these nations are actively involved in creating IT security solutions to safeguard systems and data in healthcare.



(a)

(b)

Figure 1. Scientific production, (a) countries by continent and (b) 10 countries with the highest production

3.1.2. Generic search keyword analysis

Figure 2 shows the analysis of the bibliometric co-occurrence network carried out with the VOSviewer software on the subject of information security in the health sector. A minimum threshold of 5 occurrences was established for the keywords; of the 10,045 keywords and 837 meet this criterion. The analysis reveals several highlighted terms in the literature. These highlighted terms represent the areas of greatest interest and relevance in this field of study. The most salient terms identified in the analysis are healthcare, network security, cybersecurity, computer security, data privacy, cryptography, and confidentiality. These terms reflect critical and fundamental issues related to healthcare IT security. In addition, the terms highlighted in the bibliometric analysis reflect their importance in the context of computer security in the sector. These results may be useful to guide future research and actions focused on strengthening information security and protection in this area.

3.2. About the specific search

3.2.1. Study selection

During the identification phase, a total of 2,968 articles were retrieved from the Scopus, Dimensions, and pubMed databases. In the selection phase, eight duplicate records were eliminated, and the remaining articles were examined. Using the automated selection functions available in the three databases and considering the inclusion criteria, 2,850 articles that did not meet the established criteria were excluded. In the eligibility stage, a complete reading was carried out to evaluate the selection, excluding 60 articles using the exclusion criteria. Finally, 50 articles were selected for review (see Figure 3).

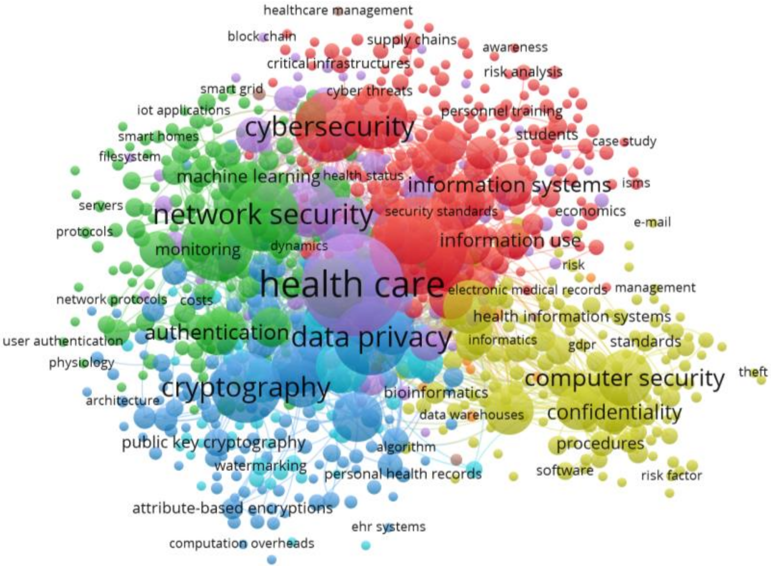


Figure 2. The network of co-occurrence of keywords

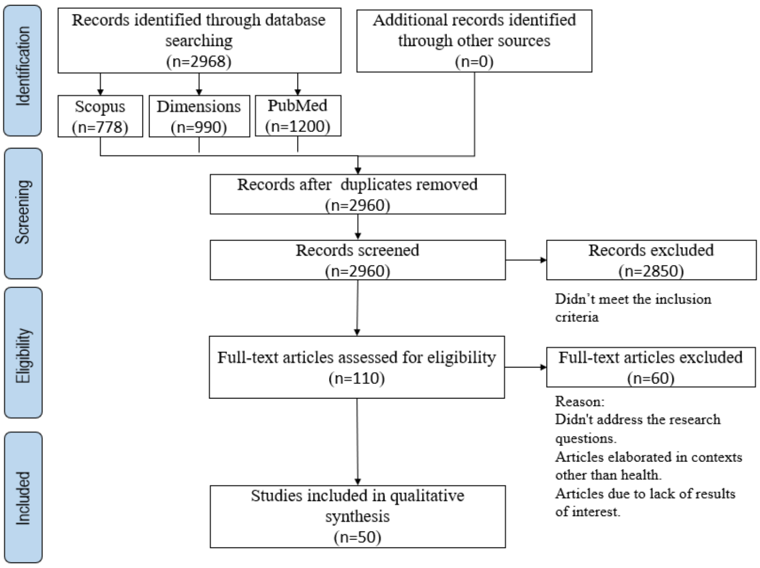

Identification
Screening
Eligibility
Included
Records identified through database searching (n=2968)
Additional records identified through other sources (n=0)
Scopus (n=778)
Dimensions (n=990)
PubMed (n=1200)
Records after duplicates removed (n=2960)
Records screened (n=2960)
Records excluded (n=2850)
Didn't meet the inclusion criteria
Full-text articles assessed for eligibility (n=110)
Full-text articles excluded (n=60)
Reason:
Didn't address the research questions.
Articles elaborated in contexts other than health.
Articles due to lack of results of interest.
Studies included in qualitative synthesis (n=50)

Figure 3. The PRISMA flow diagram of the literature search

3.2.2. Analysis of specific search keywords

A bibliometric analysis of the included articles was performed. Figure 4 shows an overlay display of trends in keywords used by authors over a specific period. The co-occurrence of keywords is used to represent the distribution of these words. The main concepts in each period are labeled with distinct colors [8]. The bibliometric analysis reveals that the articles published in recent years (represented by yellow) have focused on specific topics related to computer security, blockchain, medical devices, and technology in general, and all these topics are linked to the health sector. This suggests that there is growing interest in addressing computer security in healthcare as well as exploring the potential of emerging technologies such as blockchain to improve security and efficiency in this sector. The focus of research on these topics may be driven by the growing need to safeguard sensitive patient data, ensure system and data integrity, and explore innovative technological solutions to address these issues.

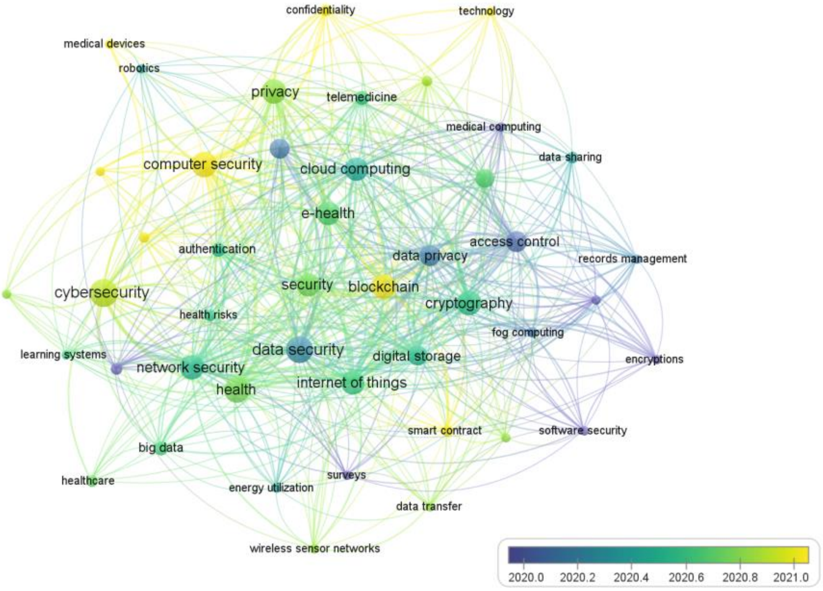


Figure 4. Distribution of the most used author keywords by year

3.2.3. Classification of studies by category

After SRL's comprehensive analysis, it was classified into three main categories: type of computer security (see Table 4), type of conventional computer security mechanisms (see Table 5), and emerging computer security technologies (see Table 6) in the sector of health. In this way, discuss the research questions.

Table 4. Classification by type of computer security

Types	Definition	Studies that consider the type of security
Network security	It is a type of security designed to protect the access, use, and integrity of the network and data.	[9]–[12]
Hardware security	It is a technical security measure to protect devices or computers from threats or interference.	[13], [14]
Software security	The technique that focuses on protecting programs and applications installed on computer equipment against cyberattacks and other risks.	[15]–[17]

Table 5. Classification by type of computer security mechanisms

Mechanisms	Definition	Studies that consider the mechanism
Data encryption	It is a method that encrypts the content of information to restrict access and ensure that only authorized parties can read or access said information	[18]–[24]
Authentication scheme	It is a method that determines the credentials of a user to access and obtain information	[25], [26]
Custom security checks	It is a method of stricter access controls that consists of customizing access for each user	[27]
Authentication	Verifies the identity of someone or something to allow access to a system and obtain information	[24], [28]–[30]
Access control	It is a method that determines who has permission to access certain data	[30], [31]

Table 6. Classification by type of emerging technology for computer security

Technologies	Definition	Studies that consider technology
Blockchain	It is a distributed and secure database that contains encrypted information about a transaction on the network, which prevents data manipulation.	[20], [28], [30], [32]–[54]
Cloud-based security	It is a discipline with the sole purpose of safeguarding data in the cloud.	[55]–[58]

3.3. Analysis of the research questions

Through a detailed analysis of each question, the soundness of the research is strengthened.

3.3.1. RQ1: what types of computer security are implemented for the protection of information in the health sector?

According to Angel [9], the security of patients' electronic health records (EHRs) is a major concern in medical information systems, which poses special challenges. For this, they consider that it is important to protect the computer network of a health center against attacks, and it is necessary to implement mobile guards in the network nodes, thus defending the network against malware attacks to guarantee the information. In addition, despite the challenges and contradictions in the management and maintenance of the security of computer networks, it is necessary to address them carefully [10]. Thus improving the security risk in the management and maintenance of computer networks through the implementation of countermeasures. Measures that focus on addressing pending problems and potential risks and actively promote reform and innovation in the management and security of computer networks in the health sector. Likewise, apply techniques to protect network computers [11]. In addition, to ensure the security of sectional medical image (SMI) transmission, it is critical to strengthen the hospital network infrastructure by implementing a four-tiered endpoint network penetration scheme [12]. This approach is based on leveraging the hospital's existing network facilities and information security policies to facilitate the secure and efficient exchange of SMIs over the internet. In this way, it seeks to establish a reliable environment that protects the privacy and integrity of medical images during their transmission.

Likewise, the authors mention that hardware security in wearable devices is critical for monitoring health data, as the growing popularity of wearable devices has led to their use in various fields, including health monitoring. However, the rapid commercialization of these devices has meant that some do not meet the necessary security standards. Strong hardware security measures are necessary to safeguard the device, the data, and the user [13], as these devices collect and transmit data in their roles of virtualization and connectivity. Similarly, the IoT and a variety of devices and sensors are being creatively combined in health 4.0, a promising new development in healthcare. However, its implementation can be complicated by security challenges. For this reason, it is crucial to use a lightweight security approach based on primitive cryptography and designed based on hardware [14], specifically to improve security.

On the other hand, the security of medical software is especially important. Therefore, it is crucial to apply techniques to design healthcare software that combines optimal security with preserved usability [15]. Similarly, Hydara *et al.* [16], mention that in the last decade, cross-site scripting vulnerabilities in web applications, including mobile versions, have been a significant problem affecting users, including healthcare users. The authors emphasize the importance of maintaining software security through vulnerability detection algorithms to protect user data. Similarly, healthcare organizations seek quality and secure software due to cyber risks to medical data [17], making software security a requirement for quality and reliable healthcare.

Therefore, computer security in the healthcare sector focuses on three aspects: network security, hardware security, and software security. Network security is the most widely used and recommended type of security by researchers. Software security is also considered important. However, it is observed that hardware security is used to a lesser extent compared to the other two aspects of security. This may indicate that more attention needs to be paid to hardware security in the healthcare sector to ensure comprehensive protection of systems and data.

3.3.2. RQ2: what computer security mechanisms are most commonly implemented in the health sector?

Research by Geetha *et al.* [18], point out that the creation of secure encryption algorithms is essential when transmitting medical images in a public environment. The use of encryption is presented as one of the effective solutions to ensuring security in this situation. Since the encryption technique protects the security of the transmitted health data, encrypted indexes must be included to allow queries on these data [19]. In addition, to maintain the security of health data, an effective encryption technique must be used [22]. The encryption technique protects electronic medical records (EMRs) efficiently and securely [20], [21]. Likewise, an iris-based biometric encryption system is efficient to ensure the security of patient health data on a smart card, a system that uses symmetric key cryptography for encryption and secure storage [23]. On the other hand, the integration of radio frequency identification (RFID) technology into healthcare systems aims to improve healthcare management. However, data security issues come to the fore, and to address security concerns in RFID-based systems, authentication and the advanced encryption standard (AES) encryption method are used to safeguard confidentiality and data integrity [24].

Similarly, Bahache *et al*. [25] it is highlighted that healthcare applications that make use of wireless medical sensor networks (WMSN) contribute to improving the quality of life, but there is a risk of manipulation due to the lack of security in the data transmitted. Therefore, they consider that security solutions and authentication schemes are effective ways to address this problem. On the other hand, cloud computing is widely used in the healthcare sector, so it is especially important to implement the mechanism of a remote authentication scheme for secure transfer of confidential files, especially patient health information [26]. Similarly, the adoption of a security verification mechanism for medical devices, along with verified data security parameters and appropriate custom controls, is crucial to preventing cyber-attacks [27].

On the other hand, Ramamurthy and Pushpa [28] raise the possibility of implementing a blockchain management system with three levels of security to protect health data. This approach involves the use of a user authentication mechanism that verifies identity through a unique combination of identification, password, and usage pattern. Moreover, by integrating supplementary layers of security, such as authentication and access control mechanisms, it becomes feasible to enhance the blockchain system for the decentralized and secure storage and retrieval of medical records [30]. Similarly, in an internet of health things (IoHT) environment, security needs to be enhanced with authentication protocols to protect patient data [29]. Similarly, the access control model is critical to protecting patient medical data from insider cybersecurity threats [31], a model that ensures that only authorized users, such as patients and physicians, can communicate with each other, beyond the established physical limits.

Therefore, it can be said that the most used information security mechanisms in the healthcare sector are data encryption, authentication schemes, personalized security checks, and authentication and access control. Among these mechanisms, data encryption is the most widely used and highly recommended by researchers. The authentication mechanism is also widely used in the industry. These findings underscore the importance of implementing strong security measures, such as data encryption, to protect sensitive health information.

3.3.3. RQ3: what are the technologies used to strengthen computer security in the health sector?

Research by Mohammed *et al*. [30], mention that the secure sharing of medical information to protect patient privacy is a major challenge. Therefore, they propose that a decentralized system that integrates blockchain and the interplanetary file system (IPFS) to store and retrieve medical records can be a solution to address security issues such as authentication, database leakage, and data integrity in different environments. On the other hand, the blockchain-based personal health record (PHR) application ensures the authenticity and security of patients' personal data through encrypted on-chain storage. Furthermore, it enables patients to track their consent records and actively store the consent mechanism for data exchange using blockchain technology [33]. Similarly, an exchange scheme for PHR that ensures security and protects privacy, based on blockchain, enhances diagnostics, and data security within eHealth systems [54].

Likewise, in the EMR, the blockchain system in healthcare not only facilitates the exchange of information between institutions but also provides adequate protection for EMRs [48]. Since the use of a blockchain framework to store the hash value of encrypted EMR and perform verification is considered a promising approach to ensure EMR integrity [20]. Also, to maintain security while sharing records, the method based on consortium blockchain technology supported by proxy encryption is a solution to the security problem [51]. Likewise, within the realm of the internet of medical things (IoMT), blockchain technology ensures security and privacy during the exchange of data [44], [50].

On the other hand, the authors highlight that the integration of blockchain technology in the healthcare sector emerges as a feasible and potent solution for facilitating patient-centric access and exchange of medical information. It effectively tackles challenges such as security, interoperability, and block storage [52], enabling cryptographic record storage [53]. As a revolutionary and decentralized technology, blockchain safeguards data against unauthorized access [34]. Likewise, this technology is suitable to protect and improve the security of the EHR [28], [40], [43], [45], [46] as it ensures the security, confidentiality, scalability, and integrity of electronic health data, thanks to its distinctive characteristics of decentralization, anonymity, integrity, and tamper-proof verification. In this sense, this technology offers significant potential to improve the security of EHRs [47]. It is also a promising solution for the reliable and secure exchange of health information between patients and physicians [41]. In addition, they suggest that the use of blockchain technology can increase the protection and confidentiality of data [32].

Kim *et al.* [55] mentioned that in the conventional management system of EHR, each medical center independently handles its own medical records, resulting in challenges when it comes to sharing across diverse platforms. Blockchain technology has emerged as a popular alternative, but full data storage is challenging due to size and cost. To address this, they see cloud computing as a promising option with storage and scalability benefits. However, cloud security has vulnerabilities to computer attacks; to address this, they recommend combining it with blockchain technology. Meanwhile, Bhatia and Malhotra [56], strengthen security in the cloud with mechanisms for secure storage of data in health systems, which replace the shortcomings of existing approaches to conventional cloud security. Moreover, Al-Zumia *et al.* [57], consider that cloud computing offers advantages in terms of having powerful computing capabilities and large storage resources. However, it needs to be strengthened to preserve data privacy through a novel approach in designing a private cloud-based data aggregation scheme that is resilient to mobile health network failures, Mittal *et al.* [58] strengthen cloud security with an innovative algorithm that allows the development of a secure and efficient e-health cloud model that is based on the use of identity-based cryptography to guarantee the protection of information.

Therefore, it can be affirmed that blockchain technology is the most widely adopted by researchers to strengthen the security of medical information. This indicates that blockchain technology is perceived as an effective solution to address security challenges in the healthcare sector. Additionally, a few researchers have embraced cloud-based security. However, there is a view that cloud-based security should be supported by blockchain to ensure greater privacy and integrity in the handling of medical and patient data. This suggests that some experts believe that the combination of both technologies could further strengthen data security in the healthcare sector.

4. COMPUTER SECURITY MODEL PROPOSAL

As a complement to the computer security measures proposed and implemented by the authors of the articles analyzed, this research proposes a perimeter security model that includes protection elements such as firewalls, virtual private networks (VPN), access and identity controls, honeypots, and distributed denial of service (anti-DDoS) systems, among others, as the first line of defense in a computer network. Figure 5 shows the model, where healthcare users access the system through a VPN, verifying their identity through authentication (username and password) and a digital token. Before reaching the perimeter security, a verification against DDoS attacks is performed. Perimeter security is controlled by a next-generation firewall (NGFW) that detects and prevents attacks through application-level security policies. In addition, a web application firewall (WAF) is used to monitor, filter, or block hypertext transfer protocol (HTTP) traffic to and from a secure web application. An anti-spam filter is also applied to the email servers. To access the health data server, NGFW verification is required, and finally, a database protection shield is in place.

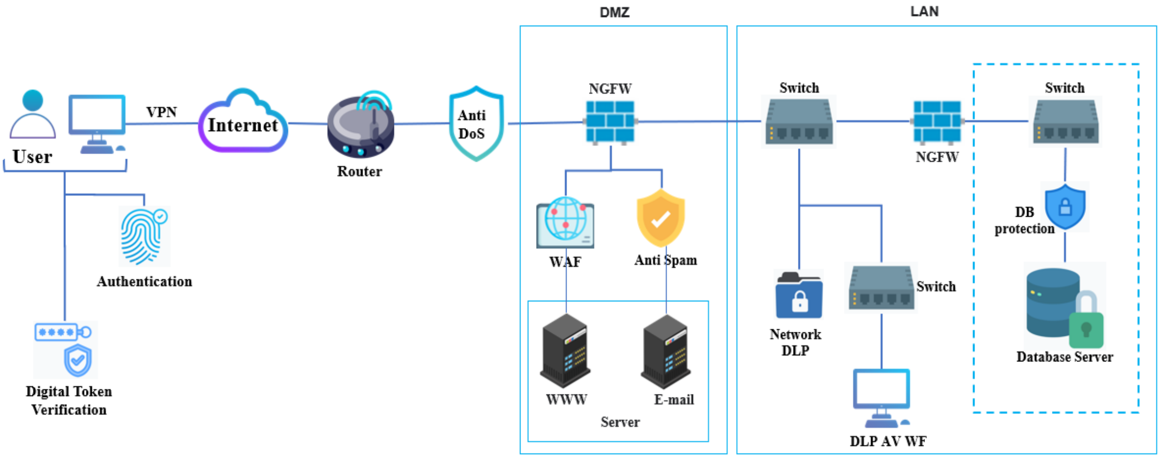


Figure 5. Proposed security model architecture

5. CONCLUSION

The objective of this study was to provide useful insights to other researchers about the state and adaptations of computer security to improve security and maintain data integrity in the healthcare sector. The research has concluded that, in the health sector, the most used security approaches are network, software, and hardware security, as well as data encryption mechanisms, authentication, and emerging technologies like blockchain and cloud-based security. Study observations suggest the importance of adopting strong security measures in terms of networks, software, and hardware, as well as harnessing the potential of blockchain technology and cloud-based security to improve data security in the healthcare sector. This work has opened several questions that require further investigation. Further work is needed to address emerging threats and challenges and to strengthen the technological infrastructure used to ensure the confidentiality, integrity, and availability of medical information.

REFERENCES

[1] F. Ö. Sönmez, C. Hankin, and P. Malacaria, "Decision support for healthcare cyber security," *Comput Secur*, vol. 122, pp. 1-20, Nov. 2022, doi: 10.1016/J.COSE.2022.102865.

[2] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, Mar. 2019, doi: 10.1016/J.COMNET.2019.01.023.

[3] J. Buzzio-Garcia, V. Salazar-Vilchez, J. Moreno-Torres, and O. Leon-Estofanero, "Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview," *ETCM 2021 - 5th Ecuador Technical Chapters Meeting*, Oct. 2021, pp. 1-5, doi: 10.1109/ETCM53643.2021.9590693.

[4] O. Said, "LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment," *Sensors*, vol. 22, no. 20, pp. 1-20, Oct. 2022, doi: 10.3390/S22207948.

[5] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," *Wireless Networks*, vol. 27, no. 8, pp. 1-20, 2021, doi: 10.1007/s11276-020-02340-0.

[6] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, Jul. 2022, doi: 10.1016/J.EIJ.2022.02.004.

[7] Z. Z. Zulkipli, R. Maskat, and N. H. I. Teo, "A systematic literature review of automatic ontology construction," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 2, pp. 878–889, Nov. 2022, doi: 10.11591/IJEECS.V28.I2.PP878-889.

[8] G. Wang and J. He, "A Bibliometric Analysis on Research Trends of Digital Literacy in Higher Education from 2012 to 2021," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 17, no. 16, pp. 43–58, Aug. 2022, doi: 10.3991/IJET.V17I16.31377.

[9] D. Angel, "Protection of Medical Information Systems Against Cyber Attacks: A Graph Theoretical Approach," *Wirel Pers Commun*, vol. 126, pp. 3455–3464, 2022, doi: 10.1007/S11277-022-09873-X.

[10] H. Tong, "Maintenance of Network Security in Hospital Information Construction Based on the Internet of Things," *International Transactions on Electrical Energy Systems*, vol. 2022, pp. 1-10, 2022, doi: 10.1155/2022/3175786.

[11] W. W. Widiyanto, "SIMRS Network Security Simulation Using Snort IDS and IPS Methods," *Indonesian of Health Information Management Journal (INOHIM)*, vol. 10, no. 1, pp. 10–17, Jun. 2022, doi: 10.47007/INOHIM.V10I1.396.

[12] L. Qiao *et al.*, "A Lightweight Internet Sharing Scheme for Sectional Medical Images according to Existing Hospital Network Facilities and Basic Information Security Rules," *J Healthc Eng*, vol. 2020, pp. 1-11, doi: 10.1155/2020/8838390.

[13] H. Tahir, R. Tahir, and K. McDonald-Maier, "On the security of consumer wearable devices in the Internet of Things," *PLoS One*, vol. 13, no. 4, pp. 1-21, Apr. 2018, doi: 10.1371/JOURNAL.PONE.0195487.

[14] V. Aivaliotis, K. Tsantikidou, and N. Sklavos, "IoT-Based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme," *Sensors*, vol. 22, no. 11, pp. 1-21, Jun. 2022, doi: 10.3390/S22114269.

[15] F. A. Al-Zahrani, "Evaluating the Usable-Security of Healthcare Software through Unified Technique of Fuzzy Logic, ANP and TOPSIS," *IEEE Access*, vol. 8, pp. 109905–109916, 2020, doi: 10.1109/ACCESS.2020.3001996.

[16] I. Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, "Towards cross-site scripting vulnerability detection in mobile web applications," *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 4, pp. 18–21, 2018, doi: 10.14419/ijet.v7i4.1.19484.

[17] M. T. J. Ansari, F. A. Al-Zahrani, D. Pandey, and A. Agrawal, "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development," *BMC Med Inform Decis Mak*, vol. 20, no. 1, pp. 1-13, Sep. 2020, doi: 10.1186/S12911-020-01209-8.

[18] B. T. Geetha, P. Mohan, A. V. R. Mayuri, T. Jackulin, J. L. A. Stalin, and V. Anitha, "Pigeon Inspired Optimization with Encryption Based Secure Medical Image Management System," *Comput Intell Neurosci*, vol. 2022, pp. 1-13, doi: 10.1155/2022/2243827.

[19] X. Yao, Y. Lin, Q. Liu, and J. Zhang, "Privacy-Preserving Search over Encrypted Personal Health Record in Multi-Source Cloud," *IEEE Access*, vol. 6, pp. 3809–3823, 2018, doi: 10.1109/ACCESS.2018.2793304.

[20] Y. L. Lee, H. A. Lee, C. Y. Hsu, H. H. Kung, and H. W. Chiu, "SEMRES - A Triple Security Protected Blockchain Based Medical Record Exchange Structure," *Comput Methods Programs Biomed*, vol. 215, pp. 1-12, Mar. 2022, doi: 10.1016/J.CMPB.2021.106595.

[21] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing," *J Med Life*, vol. 14, no. 4, pp. 448–461, 2021, doi: 10.25122/JML-2021-0100.

[22] M. S. Christo, V. E. Jesi, U. Priyadarsini, V. Anbarasu, H. Venugopal, and M. Karuppiah, "Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices," *Security and Communication Networks*, vol. 2021, pp. 1-13, 2021, doi: 10.1155/2021/6966206.

[23] F. Kausar, "Iris based cancelable biometric cryptosystem for secure healthcare smart card," *Egyptian Informatics Journal*, vol. 22, no. 4, pp. 447–453, 2021, doi: 10.1016/j.eij.2021.01.004.

[24] H. Xu, X. Chen, F. Zhu, and P. Li, "A Novel Security Authentication Protocol Based on Physical Unclonable Function for RFID Healthcare Systems," *Wirel Commun Mob Comput*, vol. 2021, pp. 1-14, 2021, doi: 10.1155/2021/8844178.

[25] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *SN Comput Sci*, vol. 3, no. 5, pp. 1-25, Sep. 2022, doi: 10.1007/S42979-022-01300-Z.

[26] S. Senthilkumar, K. Brindha, N. Kryvinska, S. Bhattacharya, and G. R. Bojja, "SCB-HC-ECC–Based Privacy Safeguard Protocol for Secure Cloud Storage of Smart Card–Based Health Care System," *Front Public Health*, vol. 9, pp. 1-15, Sep. 2021, doi: 10.3389/FPUBH.2021.688399/PDF.

[27] 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*, vol. 12, no. 16, pp. 1-20, Aug. 2022, doi: 10.3390/APP12168148.

[28] M. Ramamurthy and S. Pushpa, "Blockchain Management System with Three Layer of Security for E-Health Record using Improved 16-bit XOR Cryptography," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 5, pp. 386–394, 2021, doi: 10.22266/IJIES2021.1031.34.

[29] C. M. Chen, Z. Chen, S. Kumari, and M. C. Lin, "LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things," *Sensors*, vol. 22, no. 14, pp. 1-16, Jul. 2022, doi: 10.3390/S22145401.

[30] M. K. Mohammed, A. A. Abdullah, and Z. A. Abod, "Securing medical records based on inter-planetary file system and blockchain," *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 2, pp. 346–357, Apr. 2022, doi: 10.21533/PEN.V10I2.2855.

[31] M. A. Habib *et al.*, "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," *Int J Distrib Sens Netw*, vol. 15, no. 9, pp. 1-13, Sep. 2019, doi: 10.1177/1550147719875653.

[32] C. A. Hossain, M. A. Mohamed, M. S. R. Zishan, R. Ahasan, and S. M. Sharun, "Enhancing the security of E-Health services in Bangladesh using blockchain technology," *International Journal of Information Technology (Singapore)*, vol. 14, no. 3, pp. 1179–1185, May 2022, doi: 10.1007/S41870-021-00821-9.

[33] J. W. Kim, S. J. Kim, W. C. Cha, and T. Kim, "A Blockchain-Applied Personal Health Record Application: Development and User Experience," *Applied Sciences*, vol. 12, no. 4, pp. 1-13, Feb. 2022, doi: 10.3390/APP12041847.

[34] M. Gordan, P. Y. Siow, A. F. Deifalla, O. Z. Chao, Z. Ismail, and K. S. Yee, "Implementation of A Secure Storage Using Blockchain for PCA-FRF Sensor Data of Plate-Like Structures," *IEEE Access*, vol. 10, pp. 84837-84852, 2022, doi: 10.1109/ACCESS.2022.3197776.

[35] K. T. A. Md H. *et al.*, "Electronic Health Record Monitoring System and Data Security Using Blockchain Technology," *Security and Communication Networks*, vol. 2022, pp. 1-15, 2022, doi: 10.1155/2022/2366632.

[36] G. Ravikumar, K. Venkatachalam, M. Masud, and M. Abouhawwash, "Cost Efficient Scheduling Using Smart Contract Cognizant Ethereum for IoMT," *Intelligent Automation and Soft Computing*, vol. 33, no. 2, pp. 865–877, 2022, doi: 10.32604/IASC.2022.024278.

[37] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger healthchain: Patient-centric ipfs-based storage of health records," *Electronics*, vol. 10, no. 23, pp. 1-23, Dec. 2021, doi: 10.3390/ELECTRONICS10233003.

[38] D. Yonathan *et al.*, "Design of Decentralized Application for Telemedicine Image Record System with Smart Contract on Ethereum," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, pp. 272–281, 2021, doi: 10.14569/IJACSA.2021.0121030.

[39] H. Liu, R. G. Crespo, and O. S. Martínez, "Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts," *Healthcare*, vol. 8, no. 3, pp. 1-17, 2020, doi: 10.3390/HEALTHCARE8030243.

[40] D. Tith *et al.*, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthc Inform Res*, vol. 26, no. 1, pp. 3–12, Jan. 2020, doi: 10.4258/HIR.2020.26.1.3.

[41] A. Murugan, T. Chechare, B. Muruganantham, and S. G. Kumar, "Healthcare information exchange using blockchain technology," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 421–426, 2020, doi: 10.11591/IJECE.V10I1.PP421-426.

[42] N. Sharma and R. B. Joshi, "Enhancing the health care data security through blockchain," *Int J Eng Adv Technol*, vol. 8, no. 6, pp. 549–554, Aug. 2019, doi: 10.35940/IJEAT.F8057.088619.

[43] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019, doi: 10.1109/ACCESS.2019.2943153.

[44] Y. Chang, C. Fang, and W. Sun, "A blockchain-based federated learning method for smart healthcare," *Comput Intell Neurosci*, vol. 2021, pp. 1-12, 2021, doi: 10.1155/2021/4376418.

[45] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *PLoS One*, vol. 15, no. 12, pp. 1-6, Dec. 2020, doi: 10.1371/JOURNAL.PONE.0243043.

[46] J. Qu, "Security research of blockchain technology in electronic medical records," *Medicine*, vol. 101, no. 35, pp. 1-6, Sep. 2022, doi: 10.1097/MD.0000000000030507.

[47] J. H. Beinke, C. Fitte, and F. Teuteberg, "Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study," *J Med Internet Res*, vol. 21, no. 10, pp. 1-14, Oct. 2019, doi: 10.2196/13585.

[48] J. Fu, N. Wang, and Y. Cai, "Privacy-preserving in healthcare blockchain systems based on lightweight message sharing," *Sensors*, vol. 20, no. 7, pp. 1-16, Apr. 2020, doi: 10.3390/S20071898.

[49] 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, pp. 1-16, 2022, doi: 10.3390/s22155921.

[50] A. Mehbodniya, R. Neware, S. Vyas, M. R. Kumar, P. Ngulube, and S. Ray, "Blockchain and IPFS Integrated Framework in Bilevel Fog-Cloud Network for Security and Privacy of IoMT Devices," *Comput Math Methods Med*, vol. 2021, pp. 1-9, 2021, doi: 10.1155/2021/7727685.

[51] W. Chen, S. Zhu, J. Li, J. Wu, C. L. Chen, and Y. Y. Deng, "Authorized shared electronic medical record system with proxy re-encryption and blockchain technology," *Sensors*, vol. 21, no. 22, pp. 1-26, Nov. 2021, doi: 10.3390/S21227765.

[52] R. H. Hylock and X. Zeng, "A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study," *J Med Internet Res*, vol. 21, no. 8, pp. 1-30, Aug. 2019, doi: 10.2196/13592.

[53] P. Tagde *et al.*, "Blockchain and artificial intelligence technology in e-Health," *Environ Sci Pollut Res Int*, vol. 28, no. 38, pp. 52810–52831, Oct. 2021, doi: 10.1007/S11356-021-16223-0.

[54] A. Zhang and X. Lin, "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain," *J Med Syst*, vol. 42, no. 8, pp. 1-18, Aug. 2018, doi: 10.1007/S10916-018-0995-5.

[55] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain," *Sensors*, vol. 20, no. 10, pp. 1-21, May 2020, doi: 10.3390/S20102913.

[56] S. Bhatia and J. Malhotra, "Morton Filter-Based Security Mechanism for Healthcare System in Cloud Computing," *Healthcare*, vol. 9, no. 11, pp. 1-14, Nov. 2021, doi: 10.3390/HEALTHCARE9111551.

[57] F. A. Al-Zumia, Y. Tian, and M. Al-Rodhaan, "A novel fault-tolerant privacy-preserving cloud-based data aggregation scheme for lightweight health data," *Mathematical Biosciences and Engineering*, vol. 18, no. 6, pp. 7539–7560, 2021, doi: 10.3934/MBE.2021373.

[58] S. Mittal *et al.*, "Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health," *Comput Intell Neurosci*, vol. 2022, pp. 1-8, 2022, doi: 10.1155/2022/7016554.

BIOGRAPHIES OF AUTHORS

Raúl Jáuregui-Velarde systems and computer engineer. He has a background in database management and computer system design, with a focus on artificial intelligence applications, machine learning, and data science. His research interests are in the area of computer science. He can be contacted at email: jaureguivraul@gmail.com.

Domingo Hernandez Celis Doctor of Accounting; Doctor of Economics; Doctor of Administration; Master in Accounting and Financial Auditing; Certified Public Accountant; and Independent Auditor. General Manager of Microconsult-DHC Associates. Normal, remote and virtual undergraduate teacher; master's teacher; doctoral professor; financial advisor. In research, he is a teacher, advisor, reviewer, and jury. More than 30 years of professional practice and more than 20 years in teaching work. Teaching experience at Federico Villarreal National University (undergraduate and postgraduate); and University of San Mart´ın de Porres (undergraduate and postgraduate). He can be contacted at email: dhernandez@unfv.edu.pe.

Cesar Yactayo Arias Professional in administration and Master's in University Teaching. Extensive teaching experience in higher education. In addition, experience in educational management. Doctoral study in administration. He can be contacted at email: yactayo@uch.edu.pe.

Dr. Laberiano Andrade-Arenas Doctor in Systems and Computer Engineering. Master in Systems Engineering. Graduated with a Master's Degree in University Teaching. Graduated with a Master's degree in accreditation and evaluation of educational quality. Systems Engineer. ITILV3 Fundamentals International Course (Zonngo-Peru/IMLAD-Mexico). Scrum fundamentals certified, Research Professor with publications in Scopus indexed journals. He has extensive experience as the University Chair in face-to-face and blended classes at different undergraduate and postgraduate universities in Lima. He can be contacted at email: landrade@uch.edu.pe.